International Journal For Technological Research In Engineering
Volume 2, Issue 9, May-2015 *ISSN (Online): 2347 - 4718*

DETECTION, ELIMINATION AND SIMULATION ANALYSIS OF BLACK AND GRAY HOLE ON AD-HOC NETWORK BY IMPROVED ZRP PROTOCOL

Priyanka[1], Professor Nasib Singh Gill[2]
[1]M. Tech (Cse), [2](HOD, Dept. of Computer Science and Application)
MDU Main Campus, Rohtak

ABSTRACT: MANETS can be used for facilitating the collection of sensor data for data mining for a variety of applications such as air pollution monitoring and different types of architectures can be used for such applications. It should be noted that a key characteristic of such applications is that nearby sensor nodes monitoring an environmental feature typically register similar values. This kind of data redundancy due to the spatial Correlation between sensor observations inspires the techniques for in-network data aggregation and mining. By measuring the spatial correlation between data sampled by different sensors, a wide class of specialized algorithms can be developed to develop more efficient spatial data mining algorithms as well as more efficient routing strategies. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes by mean of ZRP protocol.The result has been quite appreciable for detection algorithm and less time for operation.Removal process is also enhanced by the use of ZRP protocol due to its zonal feature of nodes.

Keywords: Mobile Ad-hoc Networks, Black Holes, Gray Holes, Routing, ZRP, Routing Table,ZRP protocol

I. INTRODUCTION

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes. The set of applications for MANETs is diverse, ranging from small, static networks that are constrained by power sources, to large-scale, mobile, highly dynamic networks. The design of network protocols for these networks is a complex issue. Regardless of the application, MANETs need efficient distributed algorithms to determine network organization, link scheduling, and routing. However, determining viable routing paths and delivering messages in a decentralized environment where network topology fluctuates is not a well-defined problem. While the shortest path (based on a given cost function) from a source to a destination in a static network is usually the optimal route, this idea is not easily extended to MANETs. Factors such as variable wireless link quality, propagation path loss, fading, multiuser interference, power expended, and topological changes, become relevant issues. The network should be able to adaptively alter the routing paths to alleviate any of these effects. Moreover, in a military environment, preservation of security, latency, reliability, intentional jamming, and recovery from failure are significant concerns. Military networks are designed to maintain a low probability of intercept and/or a low probability of detection. Hence, nodes prefer to radiate as little power as necessary and transmit as infrequently as possible, thus decreasing the probability of detection or interception. A lapse in any of these requirements may degrade the performance and dependability of the network. A mobile ad hoc network (MANET) is a collection of wireless mobile nodes which have the ability to communicate with each other without having fixed network infrastructure or any central base station. Since mobile nodes are not controlled by any other controlling entity, they have unrestricted mobility and connectivity to others. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks. ZRP is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbors, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. Each intermediate node receiving the RREQ, makes an entry in its routing table for the node that forwarded the RREQ message, and the source node. The destination node or the intermediate node with a fresh enough route to the destination node, unicasts the Route Response (RREP) message to the neighboring node from which it received the RREQ. An intermediate node makes an entry for the neighboring node from which it received the RREP, then forwards the RREP in the reverse

 Copyright 2015.All rights reserved.

direction. On receiving the RREP, the source node updates its routing table with an entry for the destination node, and the node from which it received the RREP. The source node starts routing the data packet to the destination node through the neighboring node that first responded with an RREP. A black hole is a malicious node that falsely replies for any Route Requests (RREQ) without having active route to specified destination and drops all the receiving packets. If these malicious nodes work together as a group then the damage will be very serious. This type of attack is called cooperative black hole attack. A gray hole attack is a variation of the black hole attack, where the malicious node is not initially malicious, it turns malicious sometime later. In this paper we present a mechanism to detect and remove the above two types of malicious nodes. ZRP (ZONE ROUTING PROTOCOL) ZRP is a framework by using it we can take advantage of both table driven and on demand driven protocol according to the application. In this separation of nodes, local neighborhood from the global topology of the entire network allows for applying different approaches and thus taking advantage of each technique's features for a given situation. These local neighborhoods are called zones (hence the name) each node may be within multiple overlapping zones, and each zone may be of a different size. The "size" of a zone is not determined by geographical measurement, as one might expect, but is given by a radius of length α where α is the number of hops to the perimeter of the zone.

II. LITERATURE SURVEY

1] A Study on Wormhole Attacks in MANET
Reshmi Maulik1 and Nabendu Chaki2

- In this paper, we have analyzed the performance of Mobile Ad-hoc Networks (MANET) under wormhole attack. Multiple QoS parameters have been considered here such as throughput, delay, packet delivery ratio, node energy and node density. The NS2 network simulator has been used and the reference point group mobility model (RPGM) is considered to study the effect of node density and the initial energy on the throughput.

2] Mobile Ad Hoc Networking: Imperatives and Challenges
Pravin Ghosekar, Girish Katkar , Dr. Pradip Ghorpade

- This paper attempts to provide a comprehensive overview of this dynamic field. It first explains the important role that mobile ad hoc networks play in the evolution of future wireless technologies. Then, it reviews the latest research activities in these areas of MANET_s characteristics, capabilities and applications.

3] A Framework for Reliable Routing in Mobile Ad Hoc Networks
Zhenqiang Ye, Srikanth V. Krishnamurthy, Satish K. Tripathi

- We show that the probability of establishing a reliable path between a random source and destination pair increases considerably even with a low percentage of reliable nodes when we control their positions and trajectories in accordance with our algorithm.

4] Analysis of TCP Performance over Mobile Ad Hoc Networks
GAVIN HOLLAND, NITIN VAIDYA

- In this paper, we investigate the effects that link breakage due to mobility has on TCP performance. Through simulation, we show that TCP throughput drops significantly when nodes move, due to TCP's inability to recognize the difference between link failure and congestion. We also analyze specific examples, such as a situation where throughput is zero for a particular connection. We introduce a new metric, expected throughput, for the comparison of throughput in multi-hop networks, and then use this metric to show how the use of explicit link failure notification (ELFN) techniques can significantly improve TCP performance.

5] MANET Routing Protocols and Wormhole Attack against ZRP
Rutvij H. Jhaveri1, Ashish D. Patel2, Jatin D. Parmar3

- In this paper we have discussed some basic routing protocols in MANET like Destination Sequenced Distance Vector, Dynamic Source Routing, Temporally-Ordered Routing Algorithm and Ad-hoc On Demand Distance Vector. Security is a big issue in MANETs as they are infrastructure-less and autonomous. Main objective of writing this paper is to address some basic security concerns in MANET, operation of wormhole attack and securing the well-known routing protocol Ad-hoc On Demand Distance Vector. This article would be a great help for the people conducting research on real world problems in MANET security.

6] An Efficient Wormhole Prevention in MANET Through Digital Signature
Anil Kumar Fatehpuria1, Sandeep Raghuwanshi2.

- In this paper we represent a mechanism which is helpful for prevention of wormhole attack, through observing the delay of different path to receiver and verification of digital signature. Our mechanisms detect pinpoint location of wormhole and prevent them. This method requires neither synchronized clocks nor special hardware equipped mobile nodes.

7] Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks
Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon and Kendall Nygard

- This generic characteristic of MANET has rendered it vulnerable to security attacks. In this paper, we address the problem of coordinated attack by multiple black holes acting in group. We present a technique to identify multiple black holes cooperating with each other and a solution to discover a safe route avoiding cooperative black hole attack.

8] Prevention of Co-operative Black Hole Attack in MANET
Latha Tamilselvan, Dr. V Sankaranarayanan

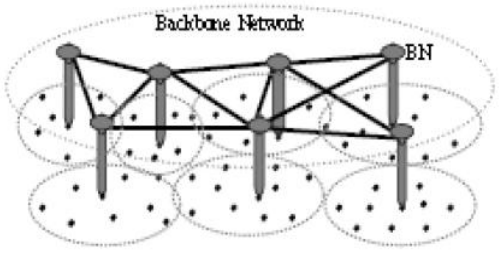
- Our approach to combat the Black hole attack is to

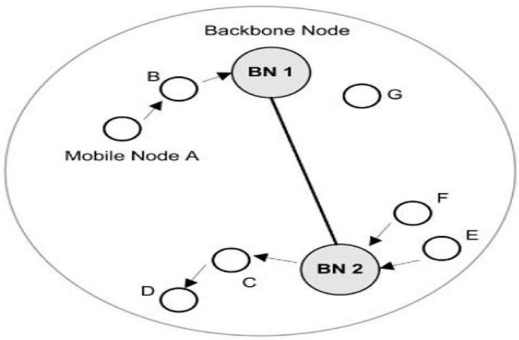
 Copyright 2015.All rights reserved.

make use of a 'Fidelity Table' wherein every participating node will be assigned a fidelity level that acts as a measure of reliability of that node. In case the level of any node drops to 0, it is considered to be a malicious node, termed as a 'Black hole' and is eliminated. Computer simulation using GLOMOSIM shows that our protocol provides better security and also better performance in terms of packet delivery than the conventional ZRP in the presence of Black holes with minimal additional delay and Overhead.

III. EXISTING METHOD TO DETECTION AND REMOVAL OF BLACK / GRAY HOLES

Initially when the source node wants to make a data transmission, it requests the nearest BBN for a restricted IP (RIP). The BBN on receiving the RIP answers to the source node with one of the unused IP addresses selected randomly out of the pool of unused IP addresses. The source node sends the RREQ for both the destination and the RIP simultaneously. Now if the Source Node (SN) gets the RREP only for the destination node(which is the normal case) and not the RIP, then the local network space is free from any of the black holes and currently free of any gray holes too. The source node reuses the RIP for a definite period of time for further data transmissions. Until that period of time the BBN does not assign any other node, this recently given out RIP. However in case the SN gets an RREP for the RIP, then it means that, there is a black hole in that route. In this case the SN initiates the process of Black Hole detection. The SN initially alerts the neighbours of the node from which it got the RREP to RIP, to enter into promiscous mode, so that they listen not only to the packet destined to them, but also to the packet destined to the specified Destination node. Now the SN sends a few dummy data packets to the destination, while the neighbouring nodes start monitoring the packet flow. These neighboring nodes further transmit the monitor message to the next hop of the dummy data packet & so on. At a point when the monitoring nodes finds out that the dummy data packet loss is way more than the normal expected loss in a network, it informs the SN about this particular Intermediate Node(IN). Now depending on the information received by the various monitoring nodes, the SN detects the location of the Black Hole. he SN detects the location of the Black Hole. This information is propagated throughout the network leading to its listing as black hole and revocation of their certificates. Further all nodes discards any further responses from this black hole and looks for a valid alternative route to the destination.





The above technique also works for gray holes also, as we are not using any trust based relationship between nodes i.e. even if a normal node turns into a black at any point of time, it is detected by normal Data transmission process by any of its neighboring normal nodes. Even in the case of cooperative black holes, the node that ultimately eats up the data packets, gets caught. Besides the Source Node decides the location of a black hole by the feed back of more than just one neighboring node. Hence it will lead to the detection and elimination of the malicious node.

Figure 1. Pictorial Representation of an Ad hoc network with a back bone network.

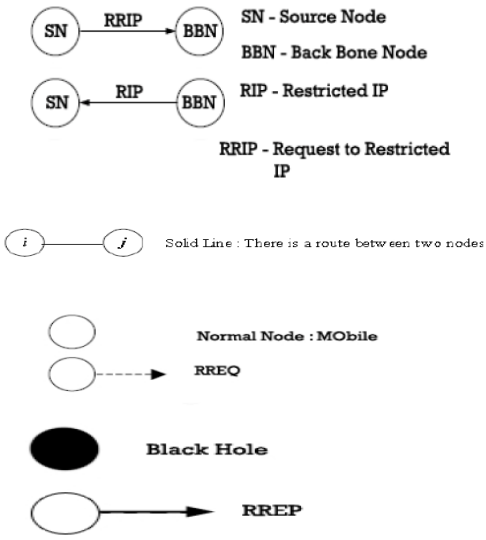
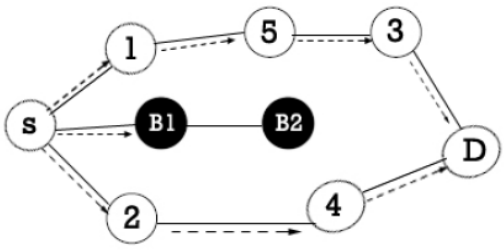


Figure 3. Nodes and their representation

RREQ - Route Request packet
RREP – Route Response packet



 Copyright 2015.All rights reserved.

Figure 4. Propagation of RREQ message

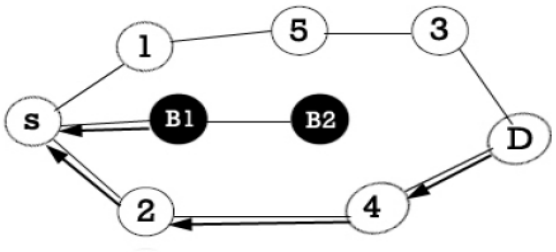


Figure 5. Propagation of RREP

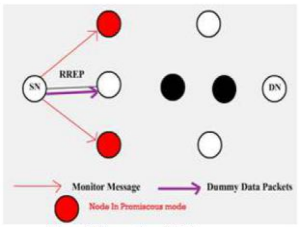


Figure 6. Propagation of Monitor message & dummy data packets

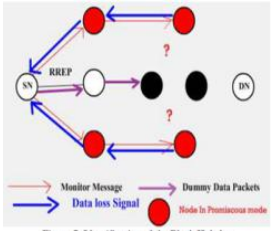


Figure 7. Identification of the Black Hole by promiscous nodes

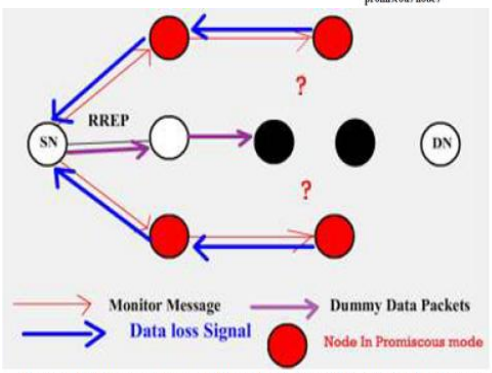


Figure 8. Propagation of Data loss Signal back to the Source Node

IV. OUR PROPOSED TECHNIQUE METHODOLOGY & ALGORITHM

Initially a backbone network of trusted nodes is established over the ad hoc network. The source node periodically requests one of the backbone nodes for a restricted (unused) IP address. Whenever the node wants to make a transmission, it not only sends a RREQ in search of destination node but also in search of the restricted IP simultaneously. As the Black/Gray holes send RREP for any RREQ, it replies with RREP for the Restricted IP (RIP) also. If any of the route responds positively with a RREP to any of the restricted IP then the source node initiates the detection procedure for these malicious nodes.

A. Network Model & Assumption

We approach this problem by selecting some nodes which are trustworthy and powerfull in terms of battery power and range. These nodes which are referred to as Back Bone Nodes(BBN) will form a Back Bone network and has special functions unlike normal nodes. For the co-ordination between the Back Bone Nodes (BBN) and the Normal Nodes, it is assumed that the network is divided into several grids. It is assumed that the nodes, when initially enters the network is capable of finding their respective grid locations. It is also assumed that the number of normal nodes are more then the number of black/gray nodes at any point of time.

B. Allocation of IP address

The IP address configuration in case of MANETs can broadly be classified into- i.Stateless approach ii. State full approach In the stateless approach an unconfigured host must obtain its own IP address by self assignment. This stateless approach adopts random address assignment and is followed by duplicate address detection mechanism to achieve address uniqueness. Stateless approaches do not keep any allocation table. In the statefull approach an unconfigured host asks its neighbouring MANET to work as proxies to obtain an ip address. We have devised a new type of state-full approach viz. Core Maintenance of the Allocation Core Maintenance of the Allocation. In this approach only the backbone network in MANET is permitted to select the IP addresses for unconfigured hosts. The mechanism is based on allocating a conflict free address to all newly arrived nodes by using multiple disjoint address spaces[6]. Each BBN in MANET is responsible for allocating a range of addresses disjoint from the ranges of all other BBN. In other words each BBN generates numbers that are unique for that host. Every hosts in the MANET must have the possibility to reach one of the Backbone Nodes (BBN) all the time. Algo for Detection and Removal of Backhole and Grayhole Atttacks in Manet Roles assigned: Backbone (BBN) node: Its main responsibility is to carry on the actual detection of black/grayhole attack and coordinate with the neighbors of the nodes present in the RREP for black and grayhole node detection. It also provides RIP(Restricted IP) if requested by the sender. Sender Node: Sends RRIP(Request for Restricted IP) to the BBN and the RREQ to the destination node D. Other nodes in the network: Maintain a MaliciousNode table and Blacklist table and work in coordination with the BBN for black and grayhole detection. Abbreviations: BBN: Backbone Node RIP : restricted IP RRIP: Request for Restricted IP Nrrep : id of the node sending route reply message to S

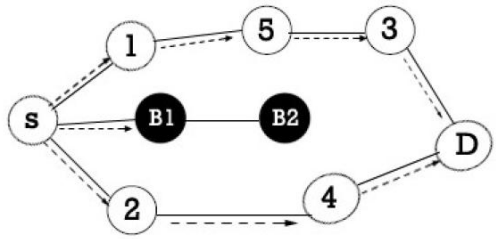
C. Detection Algo

Step 1: Source Node(SN) sends a Request to Restricted IP(RRIP) to the Back Bone Node(BBN).
Step 2: On receiving the Restricted IP(RIP), from the BBN it sends the RREQ for the Destination as well as for the RIP simultaneously and awaits for reply (RREP)
Step 3: On receiving the RREP , each node forwarding the RREP to the sender matches the RREP nodes with the node entries present in the MaliciousNode and Blacklist table maintained at each node in the network. If the nodes in the RREP does not match with the entries in the two tables then the RREP is forwarded towards the sender node S.
Removal process: Step 1: If the RREP is received only to the Destination & not to the Restricted IP (RIP), the node carries out the normal functioning by transmitting the data through

 Copyright 2015.All rights reserved.

the route.
Step 2: If the RREP is received for the RIP, it initiates the process of black hole/grayhole detection, by sending a request to the BBN to enter into promiscous mode.
Step 3: The BBN now starts the monitoring of the nodes in the RREP path and sends a PMODE_ON message to the sender node to notify that the promiscuous mode is ON for the BBN.
Step 4: On receiving the PMODE_ON message from BBN the sender node S sends a dummy packet through the same route reply(RREP) for the destination D.
Step 5: The BBN Instruct all neighbors of Nrrep (of the node sending route reply message to S) to vote for the next node to which Nrrep is forwarding packets originating from S and destined to D.
Step 6 :On receiving node ids from neighbors of Nrrep, BBN elects the next node to which Nrrep is forwarding the packets based on reported reference counts.
Step 7: If dummy packet is sent to the next node in the path which is the same node as the elected node then we replace the elected node as the Nrrep node and we verify the next node for the new Nrrep node with the help of neighbours of new Nrrep.
Step 8: If the elected node is a null node, Nrrep is itself dropping all the packets. We cross verify the malicious behavior of the elected node with the simultaneous dropping of dummy packet by the same node in the network.
Step 9: On detection of the malicious node, its node ID is broadcasted to the remaining nodes in the network including the sender node. The other nodes in the network then append this malicious node entry in the MaliciousNode table which is maintained at each node in the network and its count is set to 1.

EXAMPLE:



MaliciousNode Table

Malicious Node Entry	Count
4	5
5	2

Blacklist table

Blackhole/Grayhole Node
4

Step 10: If the node entry already exist in the Malicious Node table we increase its count by count+1.
Step 11: If at any point of time the count of any node in the Malicious Node table for any node increases the threshold value then that node is detected as Blackhole/Grayhole Node and its node ID is sent to the BBN.
Step12: The BBN then broadcasts the grayhole/blackhole node ID to all the other nodes in the network and the node ID is appended in the Blacklist table maintained at each node.
Step 13: This Blacklist table is used by all the nodes in the network for all the future RREQ requests. If any node receives a RREP from a node present in the Blacklist table then that RREP is discarded and it is not forwarded to the sender node S.

V. SECURITY AND CONCERN

We take 4 most reliable nodes (based on packet dropping ratio and high battery power) out of which one node is selected as the Backbone Node (BBN) and the other nodes are candidate nodes. If the battery power of BBN node is down then it transfers the control to the second candidate node and that node becomes the new BBN node. The MALICIOUS NODE table and BLACKLIST table are commonly shared between all the candidate nodes. The read/write access is available only with the active node, i.e. the BBN node.

VI. CONCLUSION

The main idea behind this method is to list out the set of malicious nodes locally at each node whenever they act as a source node. As mentioned in the Assumption our protocol uses the concept of Core Maintenance of the Allocation Table ie, whenever a new node joins the network, it sends a broadcast message as a request for IP address. The backbone node on receiving this message randomly selects one of the free IP addresses. The new node on receiving the allotted IP address sends an acknowledgement to the BBN. Now since the allocation is only under the control of the Back Bone Nodes (BBN) the dynamic pool of unused/restricted IPs of the network at any point of time is known only to the BBN.As after the whole process we can get better result.

REFERENCES

[1] “Security Issues in Mobile Ad Hoc Networks- A Survey” Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.
[2] Hongmei Deng, Wei Li, and Dharma P. Agrawal, ”Routing Security in Wireless Ad Hoc Network”, IEEE Communications Magzine, vol. 40, pp. 70-75, 2002.
[3] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, ”Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”. In Proceedings of 2003 International Conference on Wireless Networks (ICWN’03), Las Vegas, Nevada, USA, pp. 570-575.
[4] Sukla Banerjee “Detection/Removal of Cooperative

 Copyright 2015.All rights reserved.

Black and Gray Hole Attack in Mobile Ad-Hoc Networks" Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA

[5] Piyush Agrawal, R. K. Ghosh, Sajal K. Das, Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks In Proceedings of the 2nd international conference on Ubiquitous information management and communication, Pages 310-314, Suwon, Korea, 2008.

[6] Sudath Indrasinghe, Rubem Pereira, John Haggerty, "Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)

[7] Mansoor Mohsin and Ravi Prakash,"IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016

[8] P. Agrawal, R. K. Ghosh, and S. K. Das. Localization of wireless sensor nodes using proximity information. In Proceedings of IEEE ICCCN07, pages 485–490, 2007.

[9] N. Bulusu, J. Heidemann, and D. Estrin. Gps-less low cost outdoor localization for very small devices. IEEE Personal Communications Magazine, 7(5):28–34, 2000.

[10] H. Deng, W. Li, and D. P. Agrawal. Routing security in wireless ad hoc network. IEEE Communications Magzine, pages 70–75, 2002.

[11] S. Ramaswamy, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard. Prevention of cooperative black hole attack in wireless ad hoc networks. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), pages 570–575. Las Vegas, Nevada, USA, 2003.

[12] I. Rubin, A. Behzad, R. Zhang, H. Luo, and E. Caballero. Tbone: A mobile-backbone protocol for ad hoc wireless networks. In Proceedings of IEEE Aerospace Conference, volume 6, pages 2727–2740, 2002.

 Copyright 2015.All rights reserved.