Design Enhancements in ZRP for Detecting Multiple Black Hole Nodes in Mobile Ad Hoc Networks

Raj Shree
Department of Information Technology, B. B. A. University, Raebareli Road, Lucknow

Sanjay Kr. Dwivedi
Department of Computer Science, B. B. A. University, Raebareli Road, Lucknow

Ravi Prakash Pandey
Institute of Engineering & Technology, Dr. R.M.L. Avadh University, Faizabad

ABSTRACT
Now a day, security in Mobile Ad hoc Network (MANET) is very important issue. Due to dynamic topology and mobility of nodes, Mobile Ad hoc Networks are more vulnerable to security attacks than conventional wired and wireless network. Nodes of Mobile Ad hoc Network communicate directly without any central base station. That means in ad hoc network, infrastructure is not required for establishing communication. Mobile ad hoc Network (MANET) is different than wireless sensor network (WSN). Mobile ad hoc network is more vulnerable than WSN. Therefore attacks in MANETs are very frequent than other networks. In this research paper we are describing black hole attacks which are easy to launch in wireless ad hoc network. Black hole attack is referred to as a node dropping all packets and sending forged routing packets to route packets over itself. In this paper, we are considering a zone with multiple black hole nodes that can work co-operatively and we are implementing Secure-ZRP protocol which can be used to prevent black hole attack in MANETs. We evaluated performance in Qualnet simulator. Our analysis indicates that S-ZRP is very suitable & efficient protocol to stop this attack.

General Terms
Mobile Ad Hoc Network, Security, Secure Routing in MANETs.

Keywords
ZRP, Secure ZRP protocol.

1. INTRODUCTION
Mobile Ad hoc Network is self forming network of mobile devices connected by wireless link. It is also called mobile mesh network or wireless ad hoc network. In MANET, every device works as a router and free to move in any direction. Using this property, we can send data over a long distance. Due to the dynamic topology and mobility of nodes, Mobile Ad hoc Networks are more vulnerable to security attacks than conventional wired and wireless network. In general, it is looking very simple processing. But in practical it is a complex procedure. Because, we have to care about many things that will be used during the communication process. Security constrain is one of them. Now a day, to send secure data is a very important and burning issue in the field of Mobile Ad hoc Network. Whenever we exchange message between mobile devises within an area (zone) or mobile devices from different areas (zone or ad hoc networks), it is necessary to send information securely over a medium. Due to the mobility of the nodes it is impossible to use static routing table maintained at fixed routers. Now a day, it is necessary to find out best or optimal path between nodes during the communication. When we talk about small networks, security considerations are not complex. But, when we take large network as a whole, we have to do many things related to security. For our convenience, we divide a large network into number of zones.

2. BLACK HOLE ATTACK- OVERVIEW
In black hole attack [1], black hole node acts like black hole in the universe. In this attack black hole node absorbs all the traffic towards itself and doesn't forward to other nodes. Whenever, source node wants to send packet to the destination node. To attract all the packet towards it, this malicious node advertise that it has shortest path through it to the destination node. There are two types of black hole attack-

2.1 Black hole attack with single malicious node -
In the Black hole attack with single malicious node [2, 3], only one node will act as malicious node in a zone. Other nodes of the zone will be authentic.

2.2 Black hole attack with multiple malicious node -
In the Black hole attack with multiple malicious node [4, 5], more than one node will act as malicious node in a zone. These malicious nodes can work with collaboration.

To understand the functioning of the black hole node and for more details see [6, 7].

3. PROTOCOLS USED IN MANETS
There are mainly three types of protocol categories used in the wireless sensor network for finding routes between nodes-

3.1 Proactive Protocol
Proactive MANET protocols [8] constantly update network topology information and ensure that it is available to all nodes. That means it ensures routes to all destination are up-to-date and ready for use when required. These protocols reduce network latency but increase data overhead by constantly updating routing information. This lead to consuming of large amount of bandwidth. Examples of proactive protocols are DSDV (Destination-Sequenced Distance Vector Routing) protocol and OLSR (Optimized Link State Routing) protocol.

3.2 Reactive Protocol
Reactive MANAT protocols [9, 10] determine routing paths only when required. These protocols are associated with lower protocol overheads but longer packet delays. These protocols cause delays since the routes are not already available and flooding lead to additional control traffic again putting strain on the limited bandwidth. Examples of reactive protocols are AODV (Ad hoc Distance Vector Routing) protocol and DSR (Dynamic Source Routing) protocol.

3.4 Hybrid Protocol

This type of protocols combines the advantages of proactive and of reactive routing. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. The choice for one or the other method requires predetermination for typical cases. Advantage of these protocols depends on the amount of nodes activated. Reaction to traffic demand depends on gradient of traffic volume. Examples of hybrid protocols [11] are ZRP (Zone Routing Protocol) protocol and TORA (Temporally Ordered Routing) protocol.

In the simulation, security mechanism is associated with ZRP protocol

4. INTRODUCTION TO ZRP PROTOCOL-

ZRP [12-15] (Zone Routing Protocol) combines advantages of both proactive & reactive and makes hybrid approach. That means ZRP takes advantages of proactive within zone and use reactive approach when inter zone communication occurs. Here we assume that if nodes are in their vicinity, they can communicate securely with each other. But outer node can cause the attack and it may act as malicious node. There are some assumptions that we will take in this paper. Such as –

1. The radius of the zone will be r = 2

2. The nodes within the zone will be called as neighborhood nodes for each other.

3. It may be possible that a node belongs to multiple zones. That means overlapping of zones is possible.

In this paper we are categorizing nodes in four –

1. Inner nodes- within the zone (HC<r)

2. Boundary nodes- on the periphery and within the zone (HC=r)

3. Outer nodes- outside the zone. (HC>r)

4. Guard nodes- on the periphery with privilege (HC=r) and considered that it can never be compromised.

The node with hop count (HC) =1 will be direct neighbor node for each node. To provide security aspects in the small network is easy but to provide security in the very large network is much more complex. For our convenience we divide large network into number of zones. In this paper we are establishing secure ZRP which will be useful for large network. We know that ZRP takes the advantages of both proactive and reactive protocol. So ZRP is associated with no. of protocols. Associated protocols in the ZRP are as-

4.1 IARP (Intrazone Routing Protocol)

IARP [16] protocol is used inside routing zones. A route to a destination within the local zone can be established from the source's proactively cached routing table by IARP. Therefore, if the source and destination of a packet are in the same zone, the packet can be delivered. Most of the existing proactive routing algorithms like OLSR can be used as the IARP for ZRP.

4.2 IERP (Interzone Routing Protocol)

For routes beyond the local zone, route discovery happens reactively. Reactive routing protocol IERP [17] is used between routing zones. The source none sends a route request to the border nodes of its zone, containing its own address, the destination address and a unique sequence number. Border nodes are nodes which are exactly k hops away from the source. Each border node checks its local zone for the destination. If the destination is not a member of this local zone, the border node adds its own address to the route request packet and forwards the packet to its own border nodes. If the destination is a member of the local zone, it sends a route reply on the reverse path back to the source. The source node uses the path saved in the route reply packet to send data packets to the destination.
It takes reactive approach therefore it works like AODV.

4.3 BRP (Bordercasting Resolution Protocol)

The BRP [18] is responsible for forwarding IERP route queries to the peripheral nodes of the bordercasting node. To save network resources, a multicast tree is used. Although the receivers of a bordercast packet are the peripheral nodes, the BRP deliver the query to the IERP at every hop. BRP uses the intrazone routing information provided by IARP to construct a bordercast tree. The query packet from the source node is efficiently forwarded along the border cast tree to the regions of the network which haven't been queried before.

Because IARP is proactive protocol and IERP is reactive protocol, so because of the reactiveness of IERP, IERP is more vulnerable than IARP.

As we all know that ZRP provide framework for routing and maintain valid route tables without too much overhead. But there is no security providence in the ZRP. In this paper we are providing a secure mechanism in the ZRP protocol therefore we are implementing secure ZRP. Here, we are enhancing IERP protocol.

4.4 SECURE-ZRP (S-ZRP) PROTOCOL

The S-ZRP is based on the following algorithm-
Step1- Origin, L_0

Generate RREQ (NE) ^{IARP}

Pass RREQ (NE) $^{IERP/BRP}$

Step2-Intermediate Node $L_{1,2,\ldots\ldots n-2}$

Propagate RREQ (NE) $^{IERP/BRP}$

Step3- Previous Next Hop L_{n-1}

Deliver RREQ (NE) $^{IERP/BRP}$

Step4-Destination(Black hole node) L_n

RREP (NE) $^{IERP/BRP}$

Step5- Previous Next Hop Ln-1
$^{IERP/BRP}$
RREP (NE) Ln-1

Step6- Origin, L_0
$^{IERP/BRP}$
Receive RREP (NE) Ln-1,……2,1

Send BLOCK (Ln, NE) $^{IERP/BRP}$

Step7- Ln-1

Receive BLOCK (Ln, NE) $^{IERP/BRP}$

Delete RouteEntry (NE)

Update Neighbouring Node

In our algorithm we made changes in the IERP protocol. We added code for bluff probe packet and code for detecting and preventing black hole node. In our algorithm, we divided security in two parts (i) when local communication takes place that means communication within the zone. (ii) When inter zone communication takes place.

When local communication takes place at that time originator node broadcast the bluff probe packet. This contains the address of destination but in actual this is the address of nonexistent node. This massage is called bluff probe request packet. This message is received by the direct neighbour. They check their entries in the table if they are not black hole node than they will forward message to the next neighbour. If the malicious node present in the zone it will give immediate response to the source node through the intermediate node. As it will give response, the source node catches it as a black hole node and blocks the black hole node. After this, the source node sends information to the direct neighbour for updating their entries. Here we have implemented the security for inter zone communication. Suppose, L1, L2, L3, ……., Ln-1 are the nodes between the source L0 and the destination Ln (we are considering Ln as black hole node).

The algorithm works as-

To detect black hole node, Origin L0 sends bluff RREQ packet which contains the address of the nonexistent node, to the nearest guard node L2. It will check its table for entry of nonexistent node. If it is not in its table it will propagate this RREQ message to the intermediate nodes till Ln-1 node. Previous Next Hop Ln-1 delivers this RREQ message to the destination Ln. The destination black hole node replies and says that I have a shortest route for nonexistent node. The Ln node sends this RREP packet back to the nodes in the discovered route. Origin L0 Node Receive RREP(NE)Ln-1,……2,1 packet and send BLOCK (Ln, NE)IERP/BRP packet to Ln-1 node. This node deletes entry for Ln node. Now originator node or guard node broadcast this information to all the nodes.

Therefore we can see that this algorithm provide the efficient approach for detecting and preventing black hole node.

5. PERFORMANCE EVALUATION & CONCLUSION

To evaluate the performance of the S-ZRP (Secure Zone Routing Protocol), we used Qualnet simulator version 4.0. In our simulation we created three scenario first scenario contains 23 mobile nodes. This scenario has no malicious node. In the scenario, nodes are chosen randomly. Mobility model was random way point. We can set zone radius for each node but in this implementation we took zone radius for all as r = 2. We set routing protocol IERP. In the IERP, we set IERP radius size = 2 and IERP max message buffer size = 100. In this simulation IP forwarding is enabled. This simulation executed 99550 events in real time 13.1616 seconds with 2.9504 sec spent paused. Simulation time is kept 30 sec. in this scenario we are using original ZRP without enhancements and no black hole node. See the figures 1 & 2-

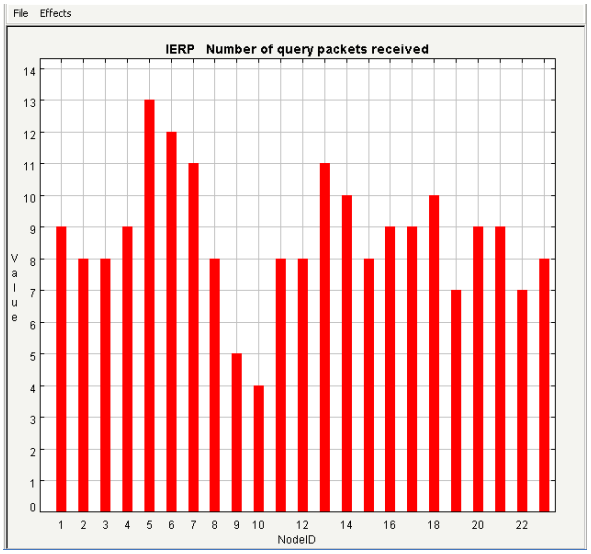

Fig1: Number of query packets received by legal nodes

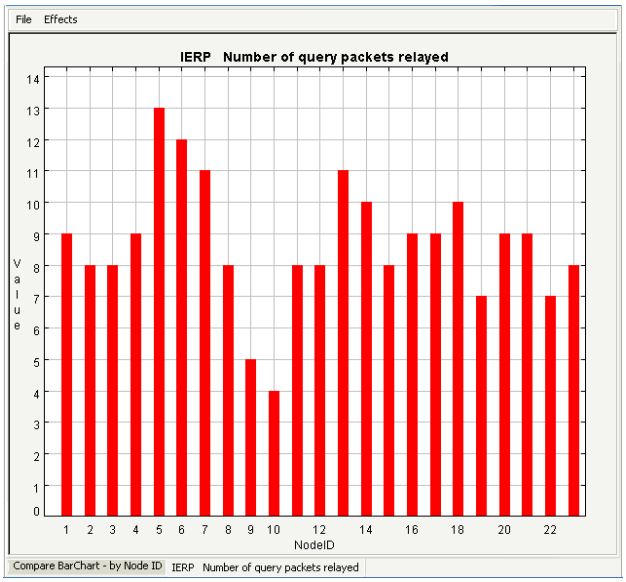

Fig2: Number of query packets relayed by legal nodes

In the second scenario, we took same settings as above. But difference is that there is single black hole node. In this, node 9 is malicious node. This simulation executed 114200 events in real time 12.5607 seconds with 0.5233 sec spent paused. Simulation time is kept 30 seconds. In this scenario we are using original ZRP without enhancements and one black hole node. The performance of algorithm can be seen in the fig 3 & 4. From the figure, it is clear that node 9 can only receive the packets. It cannot relay the packets.

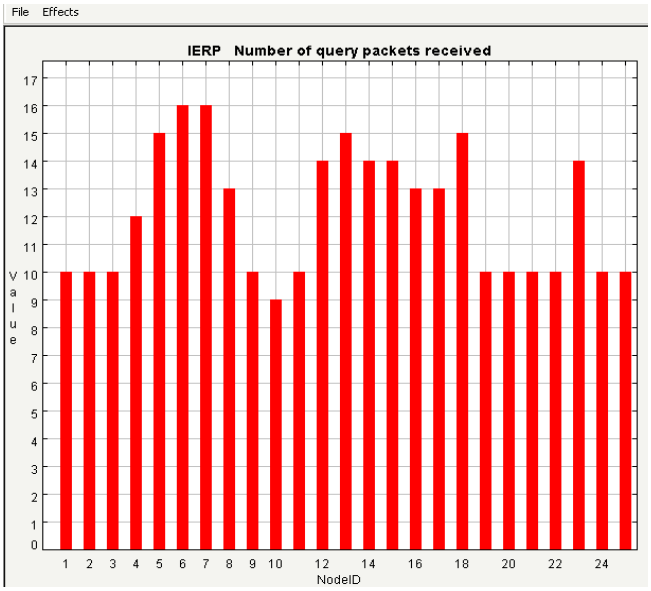

Fig3: Number of query packets received by nodes

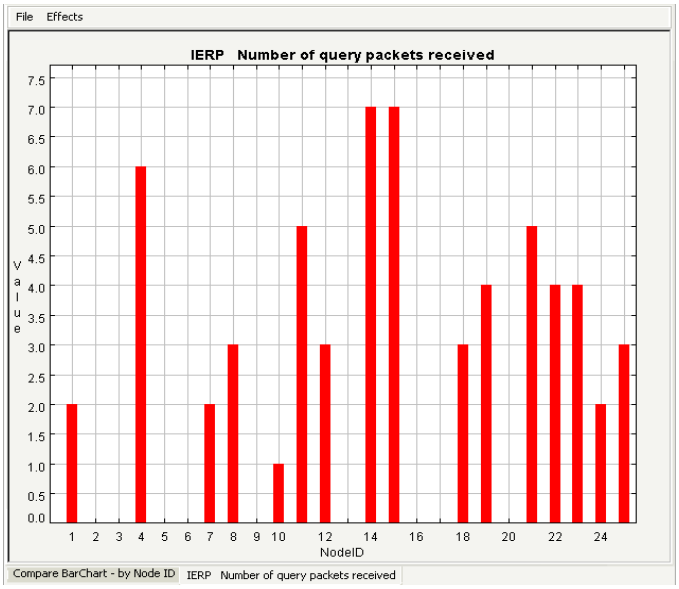

Fig5: Number of query packets received by legal nodes

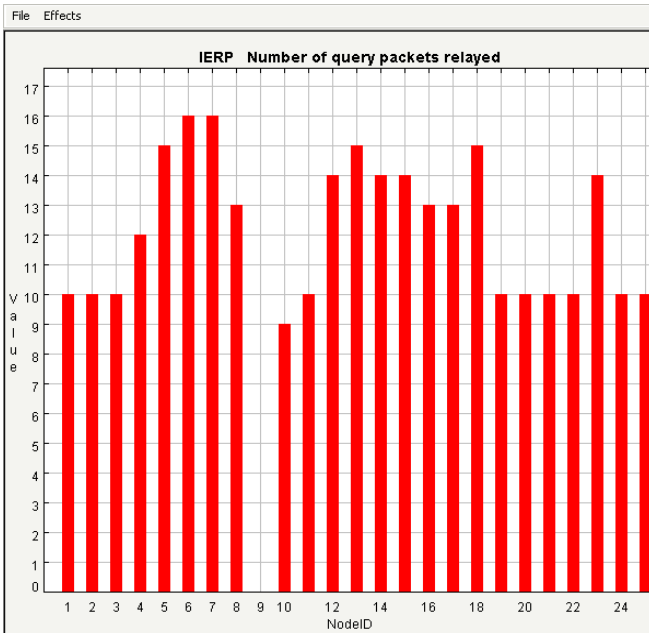

Fig4: Number of query packets relayed by nodes

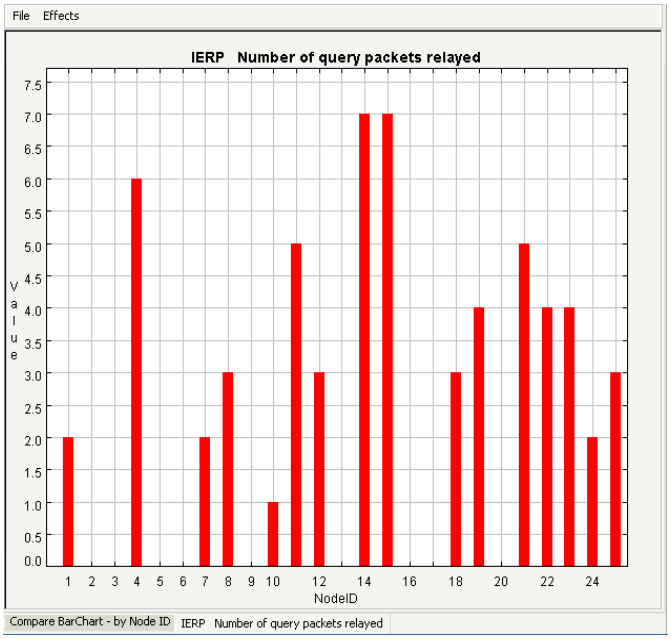

Fig6: Number of query packets relayed by legal nodes

In the third scenario, we took same settings as above. But difference is that there are multiple black hole nodes in a network. In this, nodes 2, 3, 5, 6, 9, 13, 16, 17, 20 are malicious nodes. This simulation executed 114200 events in real time 12.5607 seconds with 0.5233 sec spent paused. Simulation time is kept 30 seconds. In this scenario we are using original ZRP without enhancements and one black hole node. This simulation executed 125336 events in real time 18.8424 seconds with 3.3743 sec spent paused. Simulation time is kept 30 seconds. In this scenario we are using S-ZRP after enhancements in original ZRP and Multiple black hole nodes. The performance of algorithm can be seen in the fig 5 & 6. From the figure, it is clear that node 2, 3, 5, 6, 9, 13, 16, 17, 20 cannot receive the packets. They cannot relayed the packets

6. REFERENCES

[1] E. A .Mary Anita and V. Vasudevan, "Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining", International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12, pp. 21-28, 2010.

[2] N. Bhalaji and A. Shanmugam, "A Trust Based Model to Mitigate Black Hole Attacks in DSR Based Manet", European Journal of Scientific Research ISSN 1450-216X Vol.50 No.1, pp.6-15, 2011.

[3] Latha Tamilselvan and Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on Wireless Broadband and

Ultra Wideband Communications, 0-7695-2842-2/07, 2007.

[4] Chang Wu Yu, Tung-Kuang Wu, Rei Heng Cheng, and Shun Chao Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, LNAI 4819, pp. 538–549, 2007.

[5] Santhosh Krishna B.V, Mrs.Vallikannu A.L, "Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism" International Journal of Scientific & Engineering Research, Volume 1, Issue 3, ISSN 2229-5518, December-2010.

[6] Hongmei Deng, Wei Li and Dharma P. Agrawal, " Routing Security inWireless Ad Hoc Network", IEEE Communications Magzine, vol. 40, no. 10, October 2002.

[7] Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks", International Conference on Wireless Networks (ICWN' 03), Las Vegas, Nevada, USA, 2003.

[8] M.Saravana karthikeyan, K.Angayarkanni , and Dr.S.Sujatha, " Throughput Enhancement in Scalable MANETs using Proactive and Reactive Routing Protocols", Proceedings of International Multiconference of engineers and computer scientists, Vol2, Hong Kong, March17-19, 2010.

[9] S. R. Biradar, Hiren H D Sarma, Kalpana Sharma, Subir Kumar Sarkar , Puttamadappa C, "Performance Comparison of Reactive Routing Protocols of MANETs using Group Mobility Model", Proceedings of International Conference on Signal Processing Systems, 2009.

[10] Shima Mohseni, Rosilah Hassan, Ahmed Patel, and Rozilawati Razali, "Comparative Review Study of Reactive and Proactive Routing Protocols in MANETs",Proceedings of 4th IEEE International Conference on Digital Ecosystems and Technologies (IEEE DEST 2010), 2010.

[11] Yasser Gadallah and Hadeel El-Kassabi, "A WSN/MANET Hybrid Protocol for Routing Data in Heterogeneous Wireless Sensor Networks", study supported under the UAE University individual research grant number 01-03-9-11/07, 2008.

[12] Amit Kumar Jaiswal and Pardeep Singh, "New Scheme of Adaptive Zone Routing Protocol", International Journal of Computer Science & Communication, Vol. 1, No. 2, pp. 207-210, July-December 2010.

[13] Mr. Kamaljit I. Lakhtaria and Mr. Paresh Patel, "Analyzing Zone Routing Protocol in MANET Applying Authentic Parameter", Global Journal of Computer Science and Technology, Vol. 10, Issue 4, Ver. 1.0, pp. 114-118, June 2010.

[14] Akio Koyama, Yoshitaka Honma, Junpei Arai, Leonard Barolli, " An Enhanced Zone-Based Routing Protocol for Mobile Ad-Hoc Networks Based on Route Reliability", IEEE proceedings, 2006.

[15] Haas, Z.J., Pearlman, M.R., Samar, P., "The Zone Routing Protocol(ZRP)", IETF Internet Draft, draft-ietf-manet-zone-zrp-04.txt, July 2002.

[16] Haas, Z.J., Pearlman, M.R., Samar, P., "Intrazone Routing Protocol (IARP)", IETF Internet Draft, draft-ietf-manet-iarp-02.txt, July 2002.

[17] Haas, Z.J., Pearlman, M.R., Samar, P., "Interzone Routing Protocol (IERP)", IETF Internet Draft, draft-ietf-manet-ierp-02.txt, July 2002.

[18] Haas, Z.J., Pearlman, M.R., Samar, P., "Bordercasting Resolution Protocol (BRP)", IETF Internet Draft, draft-brp-manet-iarp-02.txt, July 2002.