Multipoint Relay Selection using Trilateration Technique

Jeril Kuriakose[1], Sandeep Joshi[1], Amruth V[2], Sushanth K J[3], and Nithin[3]
[1] School of Computing and Information Technology, Manipal University Jaipur, India
[2] Department of Computer Science, Bearys Institute of Technology Mangalore, India
[3] Department of Electronics and Communication Engineering, Bearys Institute of Technology, Mangalore

***Abstract*— Mobile network had become the broad area in wireless network, because of its reduced deployment cost, easy to use, and relief from wires. Routing is carried out in a mobile network with the help of broadcasting. There are several broadcasting schemes among which multipoint relay (MPR) is found to be the effectual and uncomplicated scheme. The MPR broadcast scheme works with the help of selected MPR nodes. The selected node can be any node in the network, and provides no assurance about its honesty. In our paper, we have discussed a novel approach in MPR node selection, by adding a security feature before the node selection request is being sent to the neighboring node. Future events are also being discussed.**

***Keywords*— Multipoint relay; trilateration; attacks; security.**

I. INTRODUCTION

A large consideration is being given to the mobile network these days, due to their self-organizing and infrastructure less capabilities. In using a mobile network, a network can formed anywhere and at any time without any additional requirements; whereas this would not be possible in a cellular or wired network. Routing in a mobile network is carried out with the help of broadcasting, and a MPR broadcasting scheme [1] is considered as the effectual and uncomplicated scheme. As a mobile network is an infrastructure less network, the data is transferred with the help of neighboring nodes. During routing a broadcast message is sent from the sender node for identifying the destination node. During a broadcast message consumes energy and floods the network, and this can be overcome by using MPR broadcast scheme. MPR scheme broadcasts the message only to the selected MPR nodes, which in turn uses other MPR nodes to identify the destination nodes, thus reducing flooding and conserving energy.

Any of the neighboring nodes can be selected as the MPR node during MPR node selection, thus increasing the vulnerability during node selection. In this paper, we have added an additional security alternative during the node selection. Before the MPR node selection is carried out, the neighboring nodes are checked using trilateration technique to identify vulnerable node. Trilateration technique [2] uses location coordinates to identify the vulnerable node. In a mobile network, each mobile node is equipped with special hardware's to identify its location reference, and by using trilateration technique in our work, need for additional hardware for security is not required.

When a MPR node is under Sybil attack [3], the attacker can create various arbitrary identities or imitate other nodes identities in the network /MAC layer. A MPR node under black hole attack [4] makes the nodes to magnetize all the traffic in the network, it does that by publicity advertising that it has the shortest path to the destination. If a MPR node is under wormhole attack [5] it distracts the route from one section of network to a different section by using a wormhole link (tunnel) between two parts of the section.

The rest of the paper is organized as follows: section 2 demonstrates how a MPR node is selected, section 3 discusses the mathematical scheming of trilateration technique. Section 4 shows the results and section 5 concludes the paper.

II. MPR NODE SELECTION

The selection of MPR nodes is began by choosing a random node *r*. To select the MPR nodes for the node *r*, the set all one hop proximity nodes are taken as *P(r)*, and the set of all two hop neighboring nodes of the node *r* are taken as $P^2(r)$. All the two hop neighbors of the node r is represented with out-degree *O(s)*, where *s* is the one hop neighbor of *r*. Fig. 1 shows initial flooding problem. The selection of MPR node is carried out as follows: [1]

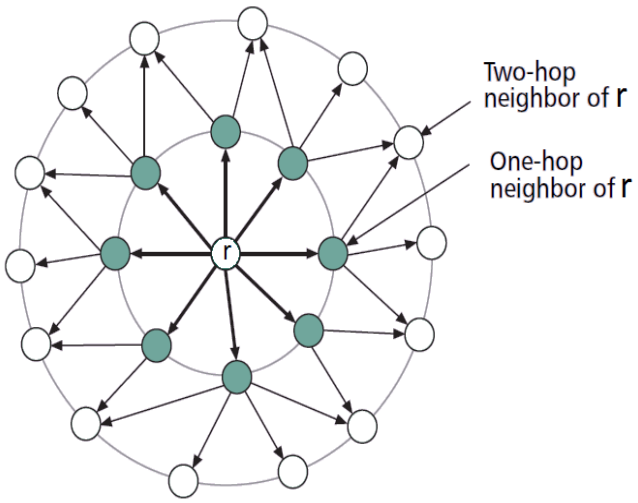


Fig. 1. Initial MPR selection

- Initially MPR is an empty set *MPR(r)*, where r is the random node.
- For each node in *P(r)*, the out-degree *O(s)* is calculated.
- The nodes in *P(r)* are added to the *MPR(r)* set, which are the only node by which the nodes in $P^2(r)$ can be reached to *r*.
- If some nodes are not covered in $P^2(r)$ through *P(r)*, in the set *MPR(r):*

- Select the unselected node in *P(r)*, through which the uncovered node in $P^2(r)$ can be reached.
- The node in *P(r)* which covers the maximum uncovered node in $P^2(r)$, is added to the *MPR(r)* set. If multiplicity occurs, out-degree is fetched into action to select the node.

- The nodes in *MPR(r)* are again checked with all the covered two hop neighbours, which can be covered by another node in *MPR(r)*. In case of multiple choices, one node is removed from *MPR(r)* using out-degree, thus optimizing the *MPR(r)* set. Fig. 2 shows the selected MPR nodes.

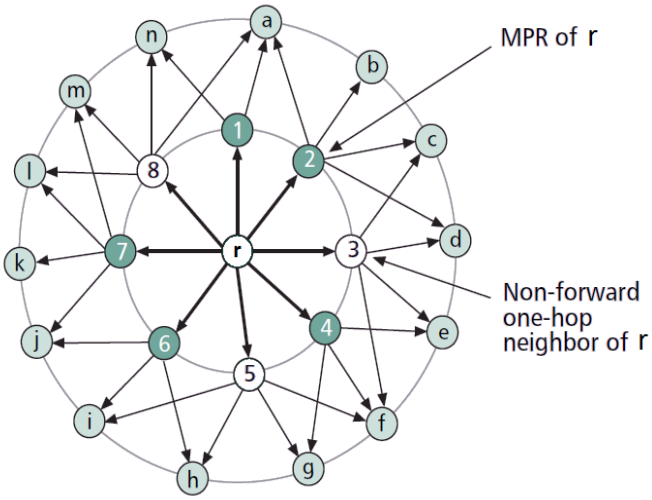


Fig. 2. Network after MPR node selection.

Determining out-degree

The calculation of out-degree *O(s)* for the one hop neighbors is carried out as follows:

A hello message is transmitted between the one hop neighbors on regular time intervals. A typical hello message in MPR scenario, contains informative data such as the selected MPR, node ID, and other information's relevant to the neighbors to update their information regarding MPR.

Three Step MPR Selection

A simplified three step MPR selection is as follows: [7]

i. The random node r selects a node as MPR that are the only neighbors of the two hop nodes of the node r.
ii. A node that covers the largest uncovered node is taken as the MPR. The MPR selection process is repeated until no uncovered nodes are left.
iii. In cases of multiple MPR nodes covering a node, only one MPR is selected. Fig. 3 shows the three step MPR node selection.

III. TRILATERATION TECHNIQUE

During the MPR selection there are several odds for an attacked node to get selected as the MPR node. So, in this paper we propose a new novel technique to carry-out the MPR selection. Whenever a node wants to find out its MPR nodes, first it searches for vulnerable neighboring nodes using trilateration technique [7, 8]. The nodes that are found to be vulnerable are not used in the MPR selection. Trilateration technique does not require any additional hardware or space apart from the typical MANET node. The mathematical computation of trilateration technique is as follows:

Consider three circles or spheres with center C_1, C_2 and C_3, radius L_1, L_2 and L_3 from points A_1, A_2 and A_3 (anchor node location), refer fig. 4.

The general equation of the sphere is

$$\sum_{k=1}^{3}(A_k - C_k)^2 = L^2$$

The three circles or spheres equation can be modified as follows,

$$L_1^2 = A_1^2 + A_2^2 + A_3^2 \quad (1)$$

$$L_2^2 = (A_1 - D)^2 + A_2^2 + A_3^2 \quad (2)$$

$$L_3^2 = (A_1 - i)^2 + (A_2 - j)^2 + A_3^2 \quad (3)$$

Subtracting equation (2) from equation (1), we get

$$L_2^2 - L_1^2 = (A_1 - D)^2 + A_2^2 + A_3^2 - A_1^2 - A_2^2 - A_3^2 \quad (4)$$

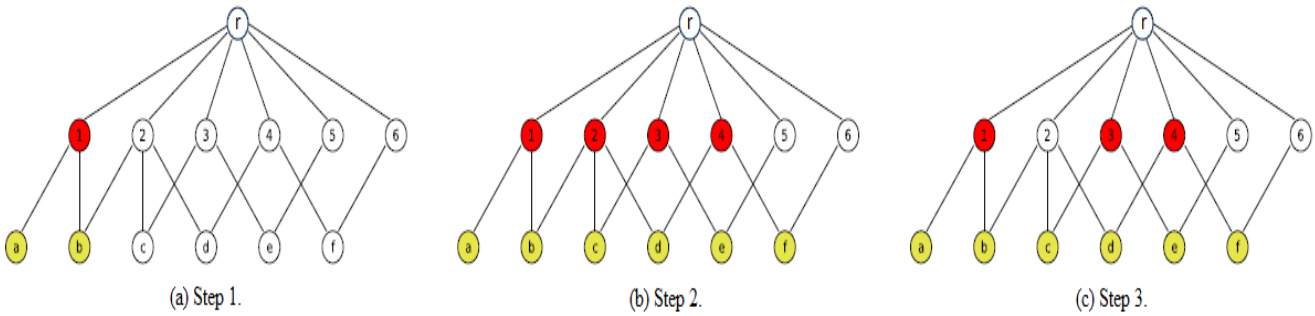
Substituting we get,

$$A_1 = \frac{L_1^2 - L_2^2 + D^2}{2D} \quad (5)$$

From the first two circles (C_1 and C_2) we can find out that the two circles intersect at two different points, that is

$$D - A_1 < A_2 < D + A_1 \quad (6)$$

Substituting equation (5) in equation (1), we can procure



(a) Step 1. (b) Step 2. (c) Step 3.

Fig. 3. Three step MPR selection.

$$L_1^2 = \left(\frac{L_1^2 - L_2^2 + D^2}{2D}\right)^2 + A_2^2 + A_3^2 \quad (7)$$

Substituting we get the solution of the intersection of two circles

$$A_2^2 + A_3^2 = L_1^2 - \frac{(L_1^2 - L_2^2 + D^2)^2}{4D^2} \quad (8)$$

Substituting equation (1) with equation (3), we get

$$L_3^2 = (A_1 - i)^2 + (A_2 - j)^2 + L_1^2 - A_1^2 - A_2^2 \quad (9)$$

$$A_2 = \frac{L_1^2 - L_2^2 - A_1^2 + (A_1^2 - i)^2 + j^2}{2j} = \frac{L_1^2 - L_2^2 + i^2 + j^2}{2j}$$

$$A_2 = \frac{i}{j} L_1 \quad (10)$$

From equation (5) and equation (10) we get the values of B_1 and B_2 respectively. From that we can find out the value of A_3 from equation (1),

$$A_3 = \pm\sqrt{L_1^2 - A_1^2 - A_2^2}$$

From the above equation we can say that, A_3 can have either positive or negative value. If any circles intersect any other two circles precisely at one point, then A_3 will get a value zero. If it intersects at two or more points, outside or inside it can get either a positive or a negative value.

During deployment each node carries out the trilateration process with all of its neighboring nodes and every node is authorized with two or more trilateration points for security reasons. Every node reveals the information about its trilateration point to its immediate or one hop neighbors. Care is taken that no node reveals the trilateration information about its neighbors.

The algorithm for setting up the anchor nodes according to trilateration are as follows:

1. Start
2. {
3. Deploy the anchor nodes
4. {
5. Set the initial coordinates (latitude & longitude) for each anchor node
6. Cluster anchor nodes into a set of three or more
7. }
8. Trilaterate a group of anchor nodes to a centre point (or trilateration point) and save the location reference in M_1*
9. Individually trilaterate all the anchor nodes with the neighbouring group and save the location references in M_2*, M_3*, etc.
10. Pass trilateration information to its immediate neighbours
11. Repeat the above steps for all the anchor nodes
12. }
13. End

(* M_1, M_2, M_3, etc., are different memory with different location reference)

The algorithm for finding out the malicious anchor nodes are as follows:

1. Start
2. {
3. Trilaterate each group of anchor nodes to a centre point and save that location
4. {
5. Compare the obtained location with location reference (M_1)
6. If comparison not satisfied
7. {
8. Trilaterate all anchor nodes (individually) of the particular group (which does not satisfy the above comparison) with the neighbouring group (using the trilateration information obtained during deployment)
9. Compare the obtained results with the location references (M_2, M_3, etc.)
10. {
11. Separate the mismatched anchors node location and save the new location in M_n
12. }
13. }
14. If comparison satisfied, no cheating nodes occur
15. }
16. End

After the comparison, the anchor nodes that does not have the same location reference or the anchor node that tends to be vulnerable is considered to be malicious or cheating node.

IV. RESULTS

Whenever a node wants to find its MPR nodes, it broadcasts a trilateration request message. The nodes that are found to be safe are considered for MPR selection. The time taken for trilateration technique to identify the malicious node is shown in fig. 5.

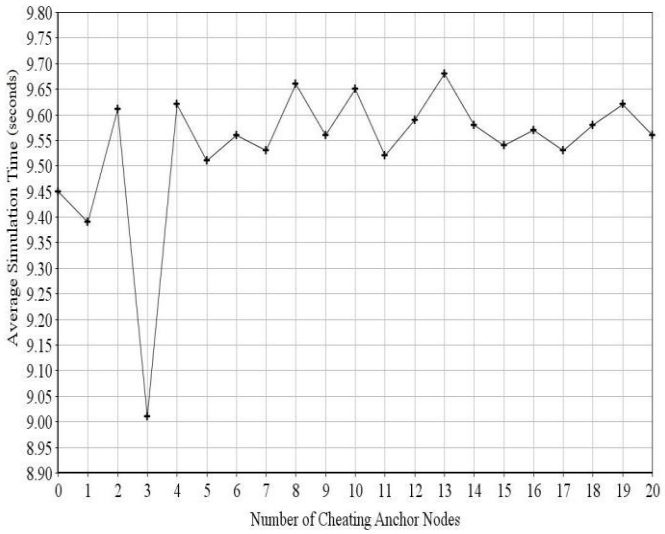


Fig. 5. Time taken for trilateration technique.

During the trilateration technique we came across few errors due to noise. Fig. 6 shows the error observed during trilateration technique.

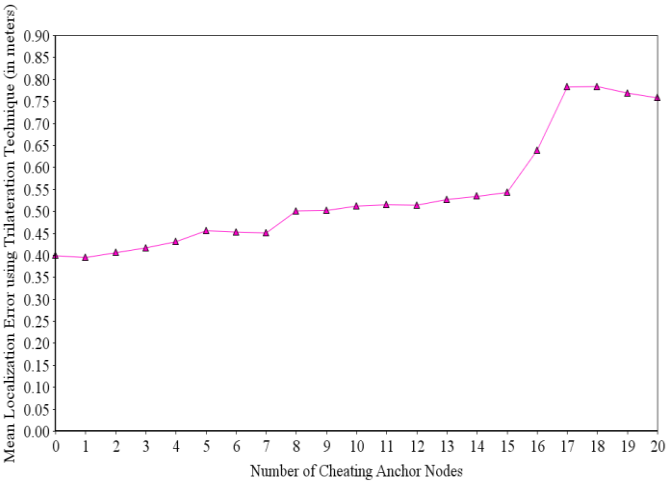


Fig. 6. Mean error observed.

The total number of transmissions taken to select the MPR node is listed in fig. 7.

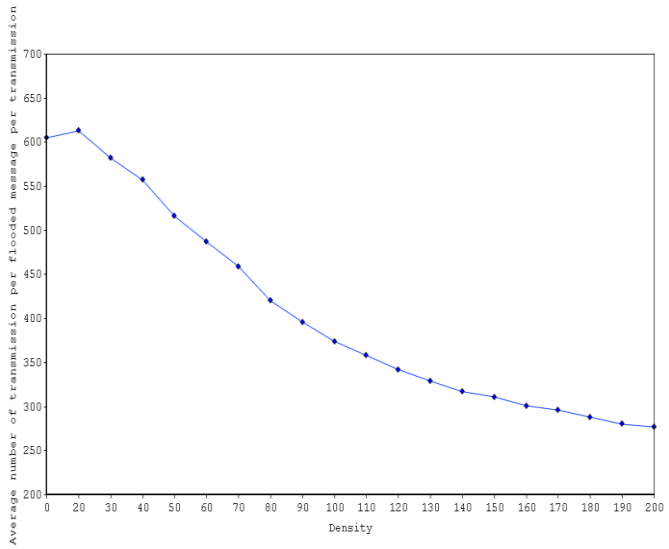


Fig. 7. Transmissions during MPR selection.

V. CONCLUSION

In this paper we have discussed how MPR node selection is carried out, and listed out some of the attacks during node selection. We came up with a novel idea to reduce the attacks faced during MPR node selection. Although there is a trade-off in the time taken, we were able to achieve reasonable results in terms of security. We would be considering other alternate techniques for trilateration in our future work.

REFERENCES

[1] Liang, Ou, Y. Ahmet Sekercioglu, and Nallasamy Mani. "A survey of multipoint relay based broadcast schemes in wireless ad hoc networks." *Communications Surveys & Tutorials, IEEE* 8.4 (2006): 30-46.

[2] Kuriakose, Jeril, et al. "A review on localization in wireless sensor networks."*Advances in signal processing and intelligent recognition systems*. Springer International Publishing, 2014. 599-610.

[3] Douceur, John R. "The sybil attack." *Peer-to-peer Systems*. Springer Berlin Heidelberg, 2002. 251-260.

[4] Al-Shurman, Mohammad, Seong-Moo Yoo, and Seungjin Park. "Black hole attack in mobile ad hoc networks." *Proceedings of the 42nd annual Southeast regional conference*. ACM, 2004.

[5] Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "MOBIWORP: Mitigation of the wormhole attack in mobile multihop wireless networks." *Ad Hoc Networks*6.3 (2008): 344-362.

[6] Nguyen, Dang Quan, and Pascale Minet. "Analysis of Multipoint relays Selection in the OLSR Routing Protocol with and without QoS Support." (2006): 15.

[7] Kuriakose, Jeril, et al. "A Review on Mobile Sensor Localization." *Security in Computing and Communications*. Springer Berlin Heidelberg, 2014. 30-44.

[8] Kuriakose, Jeril, et al. "A Comparative Analysis of Mobile Localization and its Attacks." *Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies. ACM*, 2014.

[9] Syed, Zeba, et al. "A novel approach to naval architecture using 1G VLAN with RSTP." *Wireless and Optical Communications Networks (WOCN), 2014 Eleventh International Conference on*. IEEE, 2014.

[10] Raju, R., et al. "A review on host vs. Network Mobility (NEMO) handoff techniques in heterogeneous network." *Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on. IEEE*, 2014.