High Anonymity Protection Routing Protocol in MANETs Using Neighbor Coverage Based Probabilistic Rebroadcast

V. Deepalakshmi[1], M. Rajeswari[2], V. Krishnaveni[3]

Student, M. Tech (CSE)
Dr. S.J.S Paul memorial college of Engineering and technology
Pondicherry University. Pondicherry.

***Abstract* - With the wide use of mobile devices in mobile ad hoc networks, maintaining anonymity is becoming an increasingly important issue. Existing routing algorithms either rely on hop-by-hop encryption or local broadcasting for anonymous routing, which lead to high overhead. An Anonymous Location-based Efficient Routing protocol (ALERT) was used to offer high anonymity protection at a low cost. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks and it will identify the attackers only. To prevent the occurrence of stronger and active attackers, we propose a new technique for reducing routing overhead in Mantes' using NCPR routing Protocol. The above protocol are on-demand routing protocols, and they could improve the scalability of MANETs by limiting the routing overhead when a new route is requested. A NCPR procedure must be deterministic—meaning that for a given input value it must always generate the same Address value. In other words, it must be a function of the data to be addressed, in the mathematical sense of the term.**

***Keywords* - Anonymity, ALERT, NCPR Routing protocol, Zone Partition.**

1. INTRODUCTION

A MANET is a type of ad hoc network self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. "Identity and Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as It as route anonymity. Location anonymity of sources and destinations" means it is hard if possible for other nodes to obtain the real identities and exact locations of the sources and destinations.

2. LITERATURE SURVEY

A light weight privacy-preserving on demand routing protocol to achieve source anonymity and routing privacy. ANODR [1] define source anonymity as a property guaranteeing that an adversary cannot find evidence that a node is the originator of an observed message or route request. Our definition of routing privacy corresponds to a property of hiding the identities of nodes on a path, from an adversary who may control one or more of these intermediaries.

ALARM: Anonymous Location Aided Routing in Suspicious MANETs [2] addresses a number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol (ALARM). It also offers protection against passive and active insider and outsider attacks. It also offers resistance to certain insider attacks.

An Anonymous Location-based Efficient Routing protocol (ALERT) [3] dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.

3. EXISTING METHOD

3.1 ALERT Routing Algorithm

ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node.

The ALERT Algorithm

Step1: Assume rectangle network area, nodes are disseminated.

Step2: Each data source or forwarder executes the hierarchical zone partition

Step3: First check whether itself and D are in same zone.

Step4: if so
Then divides the zone partition as Hierarchical zone partition

Step5: Repeat step 4 process until itself and ZD are not in zone

Step6: Source and ZD are not in the same zone.
Then, randomly choose a position in the other zone is called TD(Temporary Destination)

Step7: Using GPSR to send the data to the node closest to TD.
This node is defined as a RF(Random Forwarder)

Step8: Repeat step 6 and step 7 until a data receiver finds itself residing in ZD having k node

Step9: In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the D

Hierarchical zone partition

1. Horizontally partition it into two zone A1 and A2
2. Then vertically partition zone A1to B1 and B2
3. After that, Horizontally partition zone B2 into two zone
4. Alternatively splits the smallest zone in horizontal and vertical manner
5. This partition process is called Hierarchical Zone Partition

4. PROPOSED METHOD

Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks and it will identify the attackers only. Also, ALERT cannot be applied to all network models. In ALERT and ALARAM they are using Ad hoc On-demand Distance Vector Routing (AODV) Protocol this only verified node after identification.

In AODV (Ad Hoc On Demand Distance Vector) protocol Verify only node positions, but NCPR protocol Verify the Address of the data before Identification. A NCPR procedure must be deterministic meaning that for a given input value it must always generate the same Address value. In other words, it must be a function of the data to be addressed, in the mathematical sense of the term. This is the drawback of the AODV (Ad Hoc on Demand Distance Vector) protocol, so we are going to enhance the NCPR protocol.

A. Neighbor Coverage Based Probabilistic Rebroadcast Protocol

The neighbor coverage based probabilistic rebroadcast protocol which combines both neighbor coverage and probabilistic methods. In order to successfully utilize the neighbor coverage knowledge and to determine the rebroadcast order we need

1. Rebroadcast Delay

Node pi has more neighbors uncovered by the RREQ packet from s. The meaning of that if node pi rebroadcasts the RREQ packet, then it can reach more neighbor nodes. To quantify of the Uncovered Neighbors (UCN) set U (pi) of node pi as follows:

$$U(pi) = N(pi) - [N(pi) \cap N(s)] - \{s\} \qquad \text{---- Eq. (1)}$$

The N(s) and N (pi) are the neighbor's sets of node. s is sends an RREQ packet to node pi. According to Eq. (1), In order to overcome the channel collision every node must be find the rebroadcast delay. When we find the rebroadcast delay the protocol affect the neighbor conformation knowledge. So any node will calculate the delay by RREQ packet. The node calculates by checking neighbor list of RREQ packet and itself neighbor list. The rebroadcast delay Td(pi) of node pi is defined as follows:

$$Tp(ni) = 1 - \frac{|N(s) \cap N(ni)|}{|N(s)|} \qquad \text{---- Eq. (2)}$$

$$T\,d(pi) = Max\ Delay \times Tp(pi) \qquad \text{----Eq.(3)}$$

Where Tp (pi) is the delay ratio of node pi, and Max Delay is a small constant delay. | · | is the number of elements in a set.

2. Rebroadcast Probability

The rebroadcast probability is collection of two factors:

- Additional coverage ratio: It is the ratio of the number of nodes that should be covered by a single broadcast to the total number of neighbors, and
- Connectivity factor: It is the relationship of network connectivity and the number of neighbors of a given node that are additionally covered by the node which has a more rebroadcast delay might listen to RREQ packets from the nodes.

5. PERFORMANCE METRICS

For improving the performance of routing protocol we are discussing the ad hoc on demand protocol and neighbor coverage based probabilistic rebroadcast protocol with their working methodology. We evaluate the performance of the protocol we calculate following performance metrics:

1. **End-to-End delay**
   End to End Delay: The packet end-to-end delay is the average time that packets take to traverse the whole network. This time is the generation of the packet by the sender up to their reception at the destination's application layer and is calculated in seconds. It therefore includes all the delays in the network such as transmission time, delay and buffer queues induced by routing activities and MAC control exchanges.
2. **Packet Delivery Ratio**
   Packet Delivery Ratio: Packet Delivery Ratio (PDR) is the ratio between the number of packets transmitted lines by a source node and the number of packets received by a destination node. This measures the loss rate by transport protocols. It characterizes the efficiency and correctness of ad hoc routing protocols. Always a high packet delivery ratio is required by a network.
3. **Compromised Vs Attacked Node**
   A malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable. A malicious observer may also try to detect destination nodes through traffic analysis by launching a Timing attack. Therefore, the destination node also needs the protection of anonymity.
4. **Location verification Vs Security**
   A number of systems for localization and ranging of wireless devices have already been proposed based on the propagation of RF, ultrasound, and infrared signals. Most of these systems can be adopted to work with MANETs. Here, we present a short overview of the precision and area sizes of existing localization and ranging systems, and we discuss how they can be integrated with secure localization based on NCPR.

A number of systems for localization and ranging of wireless devices have already been proposed based on the propagation of RF, ultrasound, and infrared signals. Most of these systems can be adopted to work with CBSs. Here, we present a short overview of the precision and area sizes of existing localization and ranging systems, and we discuss how they can be integrated with secure localization based.

6. SIMULATION RESULT

In order to evaluate the performance of the proposed Novel Rebroadcasting algorithm, we compare it with NCPR with AODV protocols using theNS-2 simulator. We evaluate the performance of routing protocols using the following performance metrics:

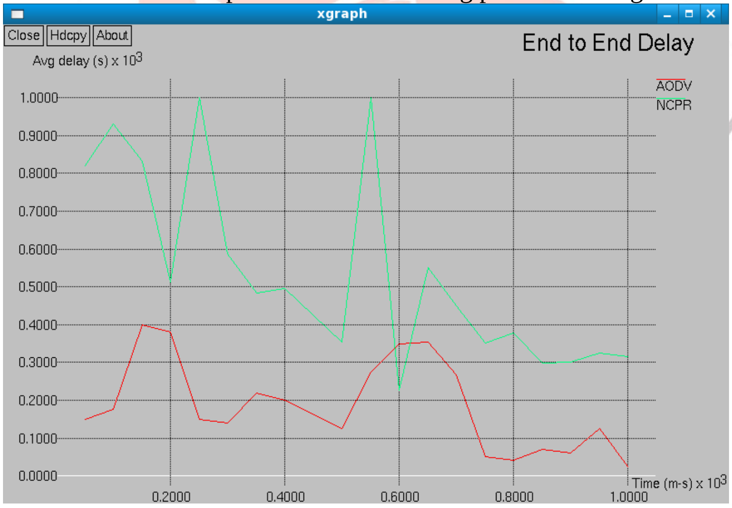

Figure 1 Graph of end to end delay

The simulated result shown in Figure 1 from this it is cleared that the end to end delay of NCPR is high at initial time interval but when time increases the end to end delay will not increases as compared to AODV. In average packet delay of NCPR protocol is more efficient than AODV protocol packet delay.

The simulated result shown in Figure 2 from this it is cleared that the location verification Vs security of AODV attack detection rate is increases but not in NCPR. So wormhole attack detection in NCPR is decreases when compare to AODV.

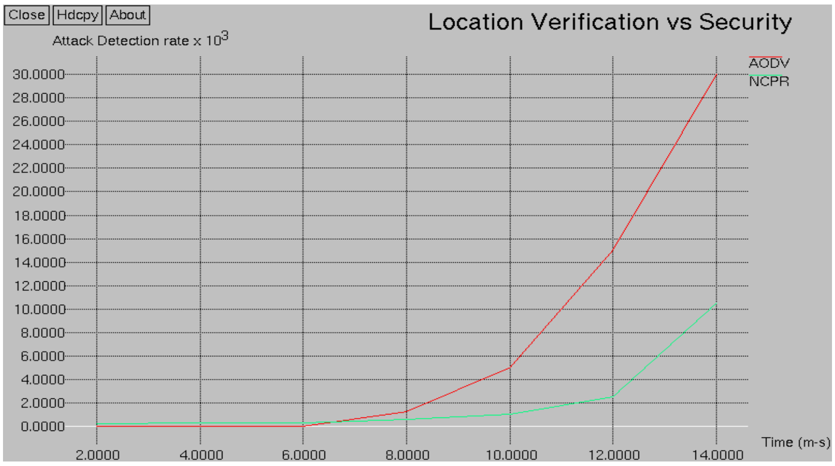

Figure 2 Graph of location verification Vs security

7. CONCLUSION

The concept of NCPR proposes which combines both neighbor coverage and probabilistic methods .The concept of NCPR proposes (neighbor coverage based probabilistic rebroadcast protocol) which combines both neighbor coverage and probabilistic methods. In existing AODV (Ad Hoc on Demand Distance Vector) protocol only verified node after identification. In AODV (Ad Hoc on Demand Distance Vector) protocol Verify only node positions, but NCPR protocol Verify the Address of the data before identification. In order to effectively exploit the neighbor coverage knowledge, we need a novel rebroadcast delay to determine the rebroadcast order, and then we can obtain a more accurate additional coverage ratio. In order to keep the network connectivity and reduce the redundant retransmissions, we need a metric named connectivity factor to determine how many neighbors should receive the RREQ packet.

REFERENCE

[1] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006

[2] Defrawy K. E. and Tsudik G. (2007), „ALARM: Anonymous Location- Aided Routing in Suspicious MANETs", Proc. IEEE Int"l Conf. Network Protocols (ICNP).

[3] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," Proc. Int'l Conf. Parallel Processing (ICPP), 2011.

[4] J.D. Abdulai, M. Ould-Khaoua, L.M. Mackenzie, and A. Mo-hammed, "Neighbour Coverage: A Dynamic Probabilistic Route Discovery for Mobile Ad Hoc Networks," Proc. Int'l Symp. Performance Evaluation of Computer and Telecomm. Systems (SPECTS '08), pp. 165-172, 2008.

[5] D. P. Agrawal, J. Kim and Q. Zhang, "Probabilistic broadcasting based on coverage area and neighbor confirmation in mobile ad hoc networks," GLOBECOM'04, 2004.