An Anonymous Location-Based Routing Protocol for SDR in MANET

[1]Rajeshri Byalalli , [2]Dhanjay M
[1]PG Scholar, [2]Professor & HOD
[1]Department of Computer Science and Engineering,
[1]Guru Nanak Dev Engineering collage, Bidar, Karnataka, India

***Abstract* - A mobile Ad Hoc network is an interconnection of group of nodes without fixed infrastructure. To provide a secure communication from outside observer several routing protocols have been proposed. Anonymous routing protocols provide a security by hiding nodes identities from outside observer. The existing anonymous routing protocols either generate high cost or cannot provide full anonymity protection to data sources, destination and routes. In this paper, we propose an Anonymous Location-based routing protocol for SDR (source, destination and route) at low cost. It hides the data initiator/receiver among many initiator/receiver by dynamically partitioning the network field into zones. The experimental results show that it achieves better route anonymity protection and lower cost compared to other anonymous routing protocols.**

***Index Terms* - Mobile ad hoc networks, Anonymity, Routing Protocols, geographical routing, GPSR**

I. INTRODUCTION

Mobile Ad Hoc Network is an interconnection of group of nodes without a fixed infrastructure. MANET can be used in scenarios in which no infrastructure exists, or in which the existing infrastructure does not meet application requirements for reasons such as security or cost. In Applications such as military exercises, disaster relief, secure and reliable communication is a necessary prerequisite for such applications.

Secure Ad Hoc network routing protocols are difficult to design, due to the generally highly dynamic nature of an Ad Hoc network and due to the need to operate efficiently with limited resources, including network bandwidth and the CPU processing capacity, memory, and battery power (energy) of each individual node in the network. Anonymous routing protocols are crucial in MANET to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers. Anonymity in MANET includes location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well 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. For route anonymity, adversaries, either en route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes en route.

Existing anonymity routing protocols in MANET can be mainly classified into two categories: hop-by-hop encryption [2] and redundant traffic [3], [4], [5]. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM [2] cannot protect the location anonymity of source and destination, SDDR [10] cannot provide route anonymity, and ZAP [5] only focuses on destination anonymity. Many anonymity routing algorithms [2], [4], [5] are based on the geographic routing protocol However; an Anonymous routing protocol generates a significantly high cost and exacerbates the resource constraint problem in MANET.

In order to provide high anonymity protection (for source, destination, and route) with low cost, we propose an Anonymous Location based routing protocol for SDR in MANET. Anonymous Location based routing protocol for SDR (SDR-RP) has a strategy to hide the data initiator/receiver among a number of initiators/receivers by dynamically partitioning the network field into zones to strengthen the anonymity protection of the source/destination.

II. LITERATURE REVIEW

Routing Protocol is mainly used to determine the optimal transmission path. Routing protocol of MANET adopts a uniform addressing and finds the path according to the nodes addressing. But in order to meet different application needs, choosing a suitable routing method which used to set up a path from data source to the destination based on saving the energy, implementing dynamic topology, high scalability and high stability. There are different criteria for designing and classifying routing protocols for wireless ad-hoc networks. For example, what routing information is exchanged; when and how the routing information is exchanged, when and how routes are computed and so on. The Routing protocols are mainly classified to two types, either Topology based routing protocol or Location-Aware routing protocol. Based on topology the routing protocol are further divided as proactive, reactive or table driven routing and hybrid routing protocol. The location-aware routing protocol or Position-Based routing protocol are further divided into Greedy forwarding like NFP,MFR or Restricted flooding type such as LAR, ARP, DREAM and etc .Most of the routing protocols have been implemented to provide anonymity protection to the network, but unable to provide all the anonymity protection such as source, destination and route anonymity. To provide all the anonymity protection at low cost we propose a routing protocol called Anonymous Location based routing protocol for SDR.

III. PROPOSED SYSTEM

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose An Anonymous Location based routing protocol for SDR (SDR-RP).SDR-RP uses dynamic hierarchical zone partition like in ALERT [9]. SDR-RP dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a no 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. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. The Fig. 1 presents the flow diagram for the proposed system.

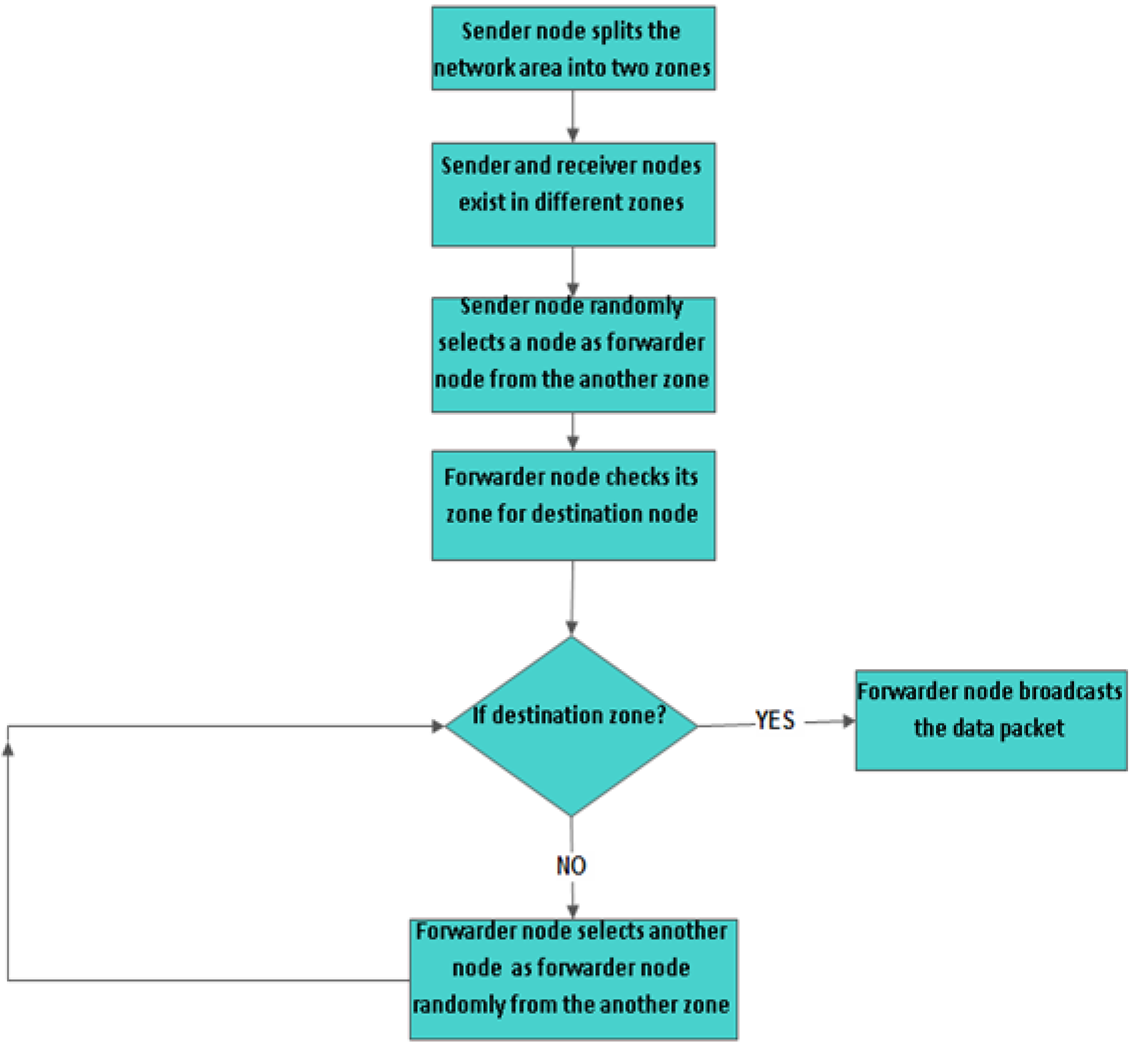
Sender node splits the network area into two zones
Sender and receiver nodes exist in different zones
Sender node randomly selects a node as forwarder node from the another zone
Forwarder node checks its zone for destination node
If destination zone?
YES
Forwarder node broadcasts the data packet
NO
Forwarder node selects another node as forwarder node randomly from the another zone

Fig 1 Flowchart of SDR-RP

3.1 Modules of the SDR-RP

In this section we will discuss the modules used for the implementation of SDR-RP, Which are specified as follows.

1. MANET creation and Routing

In this module, a Mobile ad-hoc network is created. All the nodes are configured and randomly deployed in the network area. Since our network is a mobile adhoc network, nodes are assigned with mobility (movement). A sample routing is performed to check the connectivity in the network.

2. Destination Zone Position

GPSR uses D to indicate the destination node where as the SDR-RP use ZD rather than D, to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone. Finding the position of ZD is needed by each packet forwarder to check whether it is separated from the destination after a partition or it resides in ZD. Let H denote the total number of partitions in order to produce ZD. H is calculated by using eqn. (1). Where ρ represents node density and K is the number of nodes in ZD

$$H = \log(\rho.G/K) \qquad (1)$$

Using the number of patition H, the size G, the positions (0, 0) and (xG, yG) of the entire network area, the source S can calculate the zone position of ZD . Assume SDR-RP partitions zone vertically first. After the first vertical partition, the positions of the two generated zones are (0, 0), (0.5 xG, yG) and (0.5 xG, 0), (xG, yG). S then finds the zone where ZD is located and divides that zone horizontally. This recursive process continues until H partitions are completed. The final generated zone is the desired destination zone, and its position can be retrieved accordingly. Therefore, the size of the destination zone is G/2H .

3. Splitting the network area

The existing system is independent of the zone partition as there is no random forwarder node selection. In a Proposed system consider a zone partitioning to select a random forwarder. In our analysis scenario, we assume that the entire network area is a rectangle with side lengths lA and lB and the entire area is partitioned H times to produce a k-anonymity destination zone.

We first introduce two functions eq. 2 and eq. 3 to calculate the two side lengths of the hth partitioned zone:

$$a(h, lA) = lA/2^{[h/2]} \qquad (2)$$

$$b(h, lB) = lB/2^{[h/2]} \qquad (3)$$

4. Selection of Random forwarder

Given an S-D pair, depending on the partition pattern TDs selected randomly. The data source S first divides the area into two equal-size zones, A1 and A2, in order to separate S and ZD. S then randomly selects the first temporary destination TD1 in zone A1 where ZD resides. Then, S relies on GPSR to send pkt to TD1. The pkt is forwarded by several relays until reaching a node that cannot find a neighbor closer to TD1. This node is considered to be the first random-forwarder RF1. After RF1 receives pkt, it further divides the region A1 into regions B1 and B2 so that ZD and itself are separated in two different zones. Then, RF1 randomly selects the next temporary destination TD2 and uses GPSR to send pkt to TD2. This process is repeated until a packet receiver finds itself residing in ZD, i.e., a partitioned zone is ZD having k nodes. Then, the node broadcasts the pkt to the k nodes.

IV. RESULT ANALYSIS

The test was carried out on NS-2.33 simulator using 802.11 as the MAC protocol. Simulation model is implemented using TCL language. The test field in our experiment was set to 1500 m ×1500 m area with 50 nodes. The bandwidth used is 10MB, delay of 10ms and the Interface queue length is 1000. The packet size is set to 1000bytes and simulated for a period of 5sec. evaluated by varying the number of nodes and node mobility.

The simulation is carried out to compute the Throughput and Packet delivery ration.

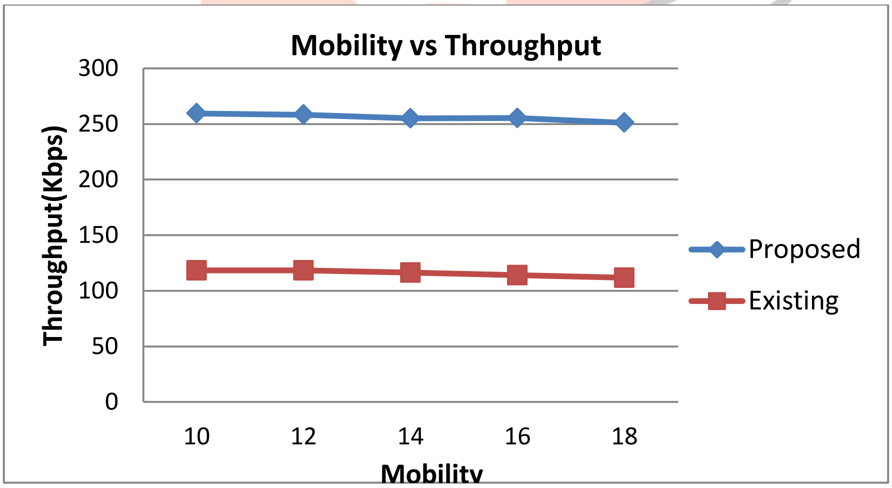

Fig 2 Throughput vs Mobility

Throughput is the percentage number of packets successfully reaching the destination over communication channel. The throughput is measured in terms of bits per second. Mobility of the node represents the change in position of the node. The frequent change in the node position will affect the routing table. Results that increase in mobility of the nodes decrease the throughput of the system as shown in Fig 2. Network Throughput by this work is enhanced up to 252kbps as compared to the earlier work as shown in Fig 3.

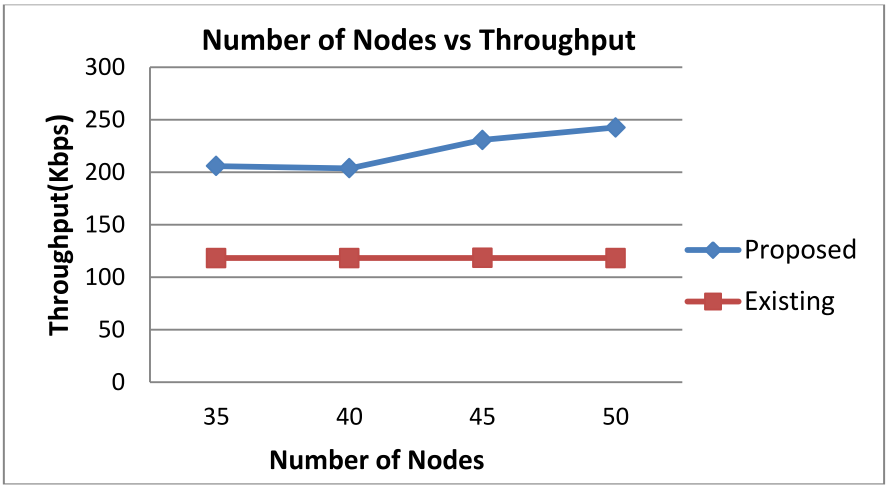

Fig 3 Number of Nodes vs Throughput

Packet Delivery ratio is measured by the fraction of packets that are successfully delivered to a destination. It shows the robustness of routing algorithms to adapt to mobile network environment. The below graph indicates the effect on packet delivery ration.

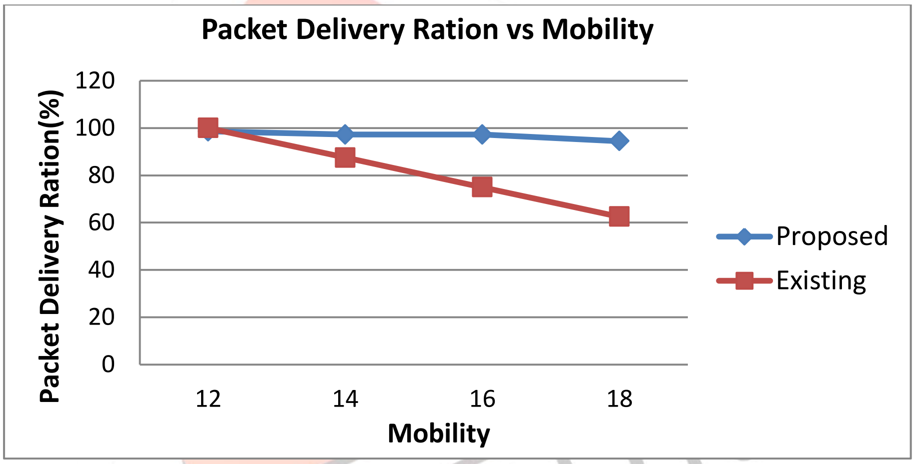

Fig 4 Packet Delivery Ration vs Mobility

Fig. 4 shows the performance of the Packet delivery ration against varying mobile speed. As shown in Fig 4, as the node moving speed increases the delivery rate decreases because of the mobility of destinations during data transmission. An interesting observation is that SDR-RP produces a higher delivery rate than GPSR. This is a benefit of the final local broadcast process in SDR-RP, which increases the possibility of packet delivery ration when the destination is not too far away.

V. V. CONCLUSION AND FUTURE WORK

In this paper, we proposed an overview of the existing techniques of different Anonymous Routing protocols for secure communication. These existing anonymous routing protocols are unable to provide complete source, destination and route anonymity and also generate high cost, hence proposed a new Anonymous Location-based Routing Protocol for SDR. The SDR-RP dynamically partitions the network area into destination zone, which provides high anonymity protection at low cast. An experimental result shows better routing efficiency than GPSR. Future work lies in reinforcing Anonymous Location-based Routing Protocol for SDR to the Clone detection attacks and outside attacks are solved as to the Security based Anonymous efficient routing protocol.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, “Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Man-agement a Consolidated Proposal for Terminology, Version 0.31,” technical report, 2005.

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

[3] Y.-C. Hu, A. Perrig, and D.B. Johnson, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Wireless Network,vol. 11, pp. 21-38, 2005.

[4] X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing protocol,” IEEE Trans. Mobile Computing, vol. 4,

no. 4, 335-348, July/Aug. 2005.

[5] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[6] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[7] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.

[8] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.

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

[10] K. El-Khatib, L. Korba, R. Song, and G. Yee, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. Int'l Conf. Parallel Processing Workshops (ICPPW), 2003.