ISSN: 2321-7782 (Online)
Volume 3, Issue 5, May 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Implementation of an Anonymous Location-Based Efficient Routing Protocol in Mobile Ad-hoc Networks

Namrata R. Borkar[1]
G. H. R.C.E.M, Amravati
Amravati, Maharashtra - India

Avinash.P. Wadhe[2]
G. H. R.C.E.M, Amravati
Amravati, Maharashtra - India

Abstract: ***Mobile Ad-hoc Network is the branch of Ad-hoc Networks that deals with communication among the Mobile. Mobile Ad Hoc Networks use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications. To offer high anonymity protection at a low cost, we propose an Anonymous Location-based Efficient Routing protocol (ALERT). ALERT 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. ALERT provides better anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks. The ALERT algorithm is giving better performance in terms of Packet delivery ratio, Packet loss ratio and End to end delay.***

Keywords: MANET, Anonymity Routing Protocols, Zone Partitions, ALERT.

I. INTRODUCTION

Fast development of Mobile Ad Hoc Networks (MANETs) excited numerous wireless applications that can be used in a wide number of areas. It has self organizing and independent infrastructures, uses such as communication and information sharing. MANETs feature self-organizing and independent infrastructures that makes them an ideal alternative for uses such as information sharing and communication. Because of the decentralization and openness features of MANETs, usually it is not desirable to constrain the membership of the nodes in the network. Nodes in the Mobile Ad-hoc Networks are vulnerable to malicious entities which tamper and analyse data as well as traffic analysis by communication eavesdropping or attacking routing protocols. In civil oriented applications, anonymity may not be a basic requirement. But in military applications, it becomes critical for example a soldier communication Consider a Mobile Ad hoc network environment deployed in a battlefield arena in Militaries. In which enemies may intercept transmitted packets, their nodes may attacks to commander nodes, and also they can be block the data transmission by comprising relay nodes through traffic analysis.

So, to provide secure communication, Anonymous routing protocols plays vital role in MANETs which hides the node identities and also it by preventing traffic analysis attacks from outside observers. MANETs includes Anonymity in terms of identity and location of data, source, destination and route. For source and destination it's very difficult to obtain the real identities and exact location of other nodes. Likewise, 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. In order to dissociate the relationship between sender and recipient (i.e. relationship unobservability [1]), it is important to make an anonymous path between the two endpoints and make sure that nodes en route don't recognize where the endpoints are, particularly in MANETs where location devices might be equipped. In MANETs,

existing anonymous routing protocols can be divided into two categories: redundant traffic [8] and hop by hop encryption. Public key based encryption and high traffic causes to generate significantly high cost, many of approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources. Additionally, many of the approaches in MANETs cannot provide all of the aforementioned anonymity protections.

The term MANET (Mobile Ad hoc Network) refers to a multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. A mobile ad hoc network (MANET) is an autonomous system of mobile nodes, mobile hosts (MHs), or MSs (also serving as routers) connected by wireless Links, the union of which forms a network modelled in the form of an arbitrary communication graph. The routers are free to move at any speed in any direction and organize themselves randomly. There is no fixed infrastructure and information is forwarded in peer-to-peer (p2p) mode using multihop routing.

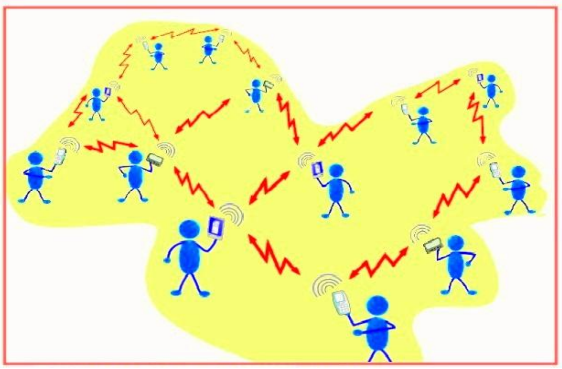

Figure 1.1: Structure of MANET

The purpose of the MANET working group is to standardize IP routing protocol functionality suitable for wireless routing application within both static and dynamic topologies with increased dynamics due to node motion and other factors. Approaches are intended to be relatively lightweight in nature, suitable for multiple hardware and wireless environments, and address scenarios where MANETs are deployed at the edges of an IP infrastructure. Hybrid mesh infrastructures (e.g., a mixture of fixed and mobile routers) should also be supported by MANET specifications and management features. Several routing protocols have been suggested and used for MANET. Routing is the most fundamental research issue in MANET and must deal with limitations such as high power consumption, low bandwidth, high error rates and unpredictable displacement of nodes. In General, current routing protocols for MANET can be categorized as:

A. Proactive (Table-Driven)

B. Reactive Routing Protocol

C. Hybrid Protocols

1.1 Characteristics of MANET's

1. In MANET, each node acts as both host and router. That is it is autonomous in behavior.

2. Multi-hop radio relaying- When a source node and destination node for a message is out of the radio range, the MANETs are capable of multi-hop routing.

3. Distributed nature of operation for security, routing and host configuration. A centralized firewall is absent here.

4. The nodes can join or leave the network anytime, making the network topology dynamic in nature.

5. Mobile nodes are characterized with less memory, power and light weight features.

6. The reliability, efficiency, stability and capacity of wireless links are often inferior when compared with wired links. This shows the fluctuating link bandwidth of wireless links.

7. Mobile and spontaneous behavior which demands minimum human intervention to configure the network.

8. All nodes have identical features with similar responsibilities and capabilities and hence it forms a completely symmetric environment.

9. High user density and large level of user mobility.

1.2 Advantages of MANET's

1. Wireless communication

1. Mobility

2. Do not need infrastructure

3. Small, light equipment

In existing protocol, ALARM cannot protect the location anonymity of source and destination [10], SDDR protects the location anonymity of source and destination but cannot provide route anonymity, and ZAP [11] only destination anonymity. Many anonymity routing algorithms [4] are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing GPSR that greedily forwards a packet to the node closest to the destination. However, the strict relay node selection of the protocol makes it easy to reveal the source and destination and to analyze traffic. MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. Also, the current increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency. However, existing anonymous routing protocols produces a significantly high cost that exacerbates the problem of resource constraint in MANETs. A low quality of service in voice and video data transmission may lead to disastrous delay in military operations. Mobile Ad hoc Networks employing a high cost anonymous routing in a battlefield area, to provide high anonymity protection for source, destination, data and route with low cost, we propose a new protocol as an Anonymous Location based and Efficient Routing protocol (ALERT). The idea of ALERT is to dynamically partition a network field into groups. Here we call it as a "Zones" and then it randomly chooses nodes in Zones as intermediate relay nodes that create a non traceable anonymous route. Particularly, in every routing step, the sender or forwarder of data partitions the network field in order to separate itself and the destination into two different zones. It then arbitrarily selects a node in the other zone as the next relay node and uses the GPSR [4] to send the data to the relay node. The final step, the data is broadcasted to k -nodes that are present in the destination zone, which provides k anonymity to the destination. In addition, ALERT (Anonymous Location based and Efficient Routing protocol) hides the data initiator among a number of initiators to strengthen the anonymity protection of the source node. ALERT also provides protection against intersection attacks and timing attacks [13]. In summary, the contribution of this work includes:

1. Anonymous routing. ALERT provides identity, route anonymity, location anonymity of source and destination.

2. Low cost. Rather than relying on hop by-hop encryption and redundant traffic, ALERT makes use of randomized routing of one message copy to provide anonymity protection.

3. Resilience to timing attacks and intersection attacks. ALERT has a strategy to effectively prevent the intersection attacks.

II. Literature Survey

In anonymizing geographic ad hoc routing for preserving location Zhi, Z. said "Due to the utilization of location information, geographic ad hoc routing present's superiority in scalability compared with traditional topology-based routing in mobile ad hoc networks". However, the consequent solicitation for location presence incurs severe concerns of location privacy, which has not

been properly studied. In this paper, location privacy based on the idea of dissociating user's location information with its identity. An anonymous geographic routing algorithm which includes three components to avoid the explicit exposure of identity and location in communication without compromising the efficiency guaranteed by geographic routing [3].

An Anonymous Location-Based Efficient Routing Protocol (ALERT) which explains anonymity protection for source, destination and route also. Route identity, source identity and destination identity are the main goals of anonymous routing protocols. The existing hop by hop encryption or redundant traffic concepts for providing anonymity results high cost. Hierarchical partition is the main technique used in ALERT [12]. The network is partitioned dynamically in to vertical and horizontal zones in ALERT. The algorithm used for data transmission is Greedy perimeter stateless routing (GPSR). Different mobility models such as random way point model and group mobility model can be used for ALERT. Communication latency is reduced to a great extend by using ALERT. ALERT restricting a node's visibility only to its neighbors. Here the same initial and forwarded messages are created. So an attacker cannot identify whether a node is a source or a forwarding node. All this factors contributes to the achievement of anonymity. Another mechanism used in ALERT to provide anonymity is the "notify and go". In this a number of nodes send information at the same time as the source sends packets. This hides the source among other nodes and provides high anonymity protection for the source. The number of nodes in the destination zone provides destination anonymity. The number of nodes in destination depends on the node density and destination zone size. ALERT is also providing protection from intersection attacks and timing attacks.

V. Pathak, D. Yao, and L. Iftode propose to secure location aware services over vehicular ad-hoc networks (VANET) with geographical secure path routing protocol (GSPR). GSPR is an infrastructure free geographic routing protocol, which is resilient to disruptions caused by malicious or faulty nodes. geographic locations of anonymous nodes are authenticated in order to provide location authentication and location privacy simultaneously. This protocol also authenticates the routing paths taken by individual messages. This paper presents the design of the GSPR secure gographic routing protocol [4].

In Privacy-friendly Routing in Suspicious MANETs, K.E. Defrawy and G. Tsudik said "Mobile Ad-Hoc Networks (MANETs) are particularly useful and well-suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery". When operating in hostile or suspicious settings, MANETs require communication security and privacy, especially, in underlying routing protocols. This paper focuses on privacy aspects of mobility. Unlike most networks, where communication is based on long-term identities (addresses), we argue that the location centric communication paradigm is better-suited for privacy in suspicious MANETs. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries [6].

AODV [19] is a reactive protocol in which the routes are created only when they are needed. It uses traditional routing tables. In AODV, when a source node sends data traffic to a destination node, firstly it initiates a route discovery process. In AODV, when a source node sends data traffic to a destination node, firstly it initiates a route discovery process. In this process, the source node broadcasts a Route Request (RREQ) packet. Neighbor nodes which do not know an active route for the requested destination node forward the packet to their neighbors until an active route is found or the maximum number of hops is reached. When an intermediate node gets the active route to the requested destination node, it sends a Route Reply (RREP) packet back to source node in unicast mode. Eventually, the source node receives the RREP packet and opens the route. [19].

The position based routing approach was designed for MANET routing protocol called Greedy Perimeter Stateless Routing (GPSR). In this greedy forwarding strategy is used to forward messages toward known destination. However if at one or multi hop, there are no nodes in direction of destination then it uses the perimeter mode [15]. In the case of greedy forwarding, the transmitter node chooses the optimal neighbor as the next hop which is the closest geographic node to the destination selected in a greedy manner. In other words, based on the neighbors' positions, the transmitter selects the closest neighbor as its local optimal choice. It will be considered as the next hop to the packet's destination. GPSR also uses a beaconing process to update its neighbors' data (such as positions, etc.). If there is no intersection between the transmitter node and the destination node, the

perimeter forwarding method is executed. It is based on the right hand rule in which, each node forwards packet through the perimeter to its first neighbor counterclockwise about itself. [18]

An Anonymous Location Aided Routing in Suspicious MANETs (ALARM) [5] uses proactive routing, where each node broadcasts its location information to its authenticated neighbors so that each node can build a map for later anonymous route discovery. However, this map construction leaks destination node locations and compromises the route anonymity. Thus, ALARM cannot protect the location anonymity of source and destination. In ALARM, each node at times disseminates its hold identity to its genuine neighbors and continually collects all other nodes' identities. Hence, nodes can assemble a secure map of other nodes for geological routing.

Zone based Anonymous Routing Protocol (ZAP) is a hybrid Wireless Networking routing protocol that combines the proactive and reactive routing protocols when sending the data over the network. ZAP [13] was designed to speed up the delivery rate and reduce the processing overhead by selecting the most efficient type of protocol to use throughout the entire route. ZAP uses a destination zone, and locally broadcasts to a destination zone in order to reach the destination without leaking the destination identity or position. A disadvantage of redundant traffic based methods is the very high overhead incurred by the redundant operations or packets, leading to high cost. Although some methods such as ZAP only perform local broadcast in a destination zone, these methods cannot provide source or routing anonymity [13].

In the AO2P [10] Ad Hoc On-Demand Position-Based Private Routing Protocol, pseudonyms are used to protect nodes real identities, and a node chooses the neighbor that can reduce the greatest distance from the destination. Since AO2P does not provide anonymity protection to destinations, the authors further improve it by avoiding the use of destination in deciding the classification of nodes. The improved AO2P selects a position on the line connecting the source and destination that is further to the source node than the destination and replaces the real destination with this position for distance calculation. SDDR [18] cannot provide route anonymity. Another anonymous routing protocol is Anonymous Secure Routing (ASR) protocol [12]. This protocol provides additional properties on anonymity, i.e. Identity Anonymity and Strong Location Privacy. As well as at the same time ensure the security of discovered routes against various passive and active attacks. But ASR protocol having route anonymity problem.

III. Problem Definition

Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide untraceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, 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 an intersection attack. Therefore, the destination node also needs the protection of anonymity. To provide secure communications, MANETs used Anonymous routing protocols. It hides a node identity and prevents traffic analysis attacks from outside observers. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. "Identity and 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 enroute or out of the route, cannot trace a packet flow back to its source or destination, and no node have information about the real identities and locations of intermediate nodes enroute. Also, in order to dissociate the relationship between source and destination (i.e., relationship unobservability, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are, especially in MANETs where location devices may be equipped.

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. Many approaches cannot provide all of the aforementioned anonymity protections ALARM cannot protect the location anonymity of source and destination, SDDR cannot provide route anonymity, and ZAP only focuses on destination anonymity. Existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing in a battlefield, a low quality of service in voice and video data transmission due to depleted resources may lead to disastrous delay in military operations.

So, for secure transmission here we implemented an Anonymous location- based routing protocol in MANETs. Basically, it partitions a whole network area into zones and randomly selects a relay forwarder and creates a non traceable anonymous route. Particularly, in every routing step, the sender or forwarder of data partitions the network field in order to separate itself and the destination into two different zones. It then arbitrarily selects a node in the other zone as the next relay node and uses the GPSR [15] to send the data to the relay node. The final step, the data is broadcasted to k -nodes that are present in the destination zone, which provides k anonymity to the destination. In addition, ALERT (Anonymous Location based and Efficient Routing protocol) hides the data initiator among a number of initiators to strengthen the anonymity protection of the source node.

IV. PROPOSED SYSTEM

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose preventing path tracing attack in MANETs by using Anonymous Location-based and Efficient Routing protocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable 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 [16] 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. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks.

4.1 ALERT Routing Algorithm

Assume the entire network area is a rectangle in which nodes are randomly disseminated. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT [12]. ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes.

As shown in the Fig. 4.1, given an area, we horizontally partition it into two zones A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. We call this partition process Hierarchical Zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node (i.e., data forwarder), thus dynamically generating an unpredictable routing path for a message.

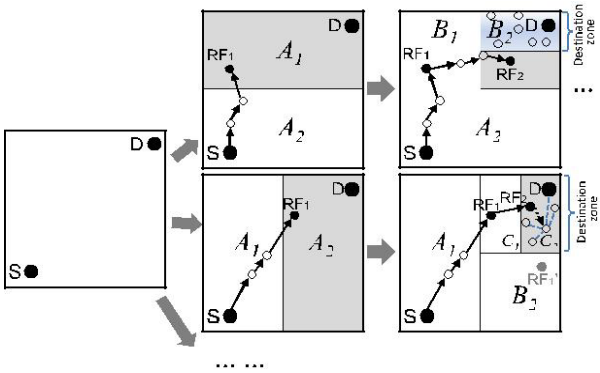

Figure 4.1: Different Zone Partitions

Fig. 4.2 shows an example of routing in ALERT. We call the zone having k nodes where D resides the destination zone, denoted as ZD. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 4.2 is the destination zone. Specifically, in the ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and *ZD* are not in the same zone. It then randomly chooses a position. Routing among zones in ALERT zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. This node is defined as a random forwarder (RF). Fig. 4.2 gives choosing a RF according to a given TD and fig. 4.3 shows an example where node N3 is the closest to TD, so it is selected as a RF.

ALERT aims at achieving k-anonymity for destination node D where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in ZD, providing k-anonymity to the destination. Given an S-D pair, the partition pattern in ALERT varies depending on the randomly selected TDs and the order of horizontal and vertical division, which provides a better anonymity protection.

In the fig. 4.1 upper routing flow, data source S first horizontally 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 neighbour closer to TD1.

This node is considered to be the first random-forwarder RF1. After RF1 receives pkt, it vertically 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.

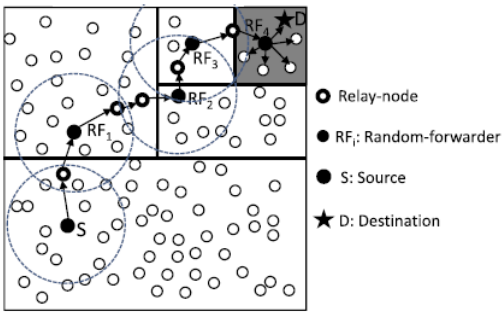

Figure 4.2: Routing among zones in ALERT

The lower part of Fig. 4.1 shows another routing path based on a different partition pattern. After S vertically partitions the whole area to separate itself from ZD, it randomly chooses TD1 and sends pkt to RF1. RF1 partitions zone A2 into B1 and B2 horizontally and then partitions B1 into C1 and C2 vertically, so that itself and ZD are separated. Note that RF1 could vertically

partition A2 to separate itself from ZD in two zones but may choose a TD further away from the destination than the TD that resulted from the horizontal partition. Therefore, ALERT sets the partition in the alternative horizontal and vertical manner in order to ensure that a pkt approaches D in each step. As GPSR, we assume that the destination node will not move far away from its position during the data transmission, so it can successfully receive the data. In this design, the tradeoff is the anonymity protection degree and transmission delay. A larger number of hierarchies generate more routing hops, which increases anonymity degree but also increases the delay. To ensure the delivery of packets, the destination sends a confirmation to the source upon receiving the packets. If the source has not received the confirmation during a predefined time period, it will resend the packets.

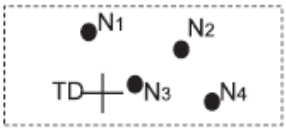

Figure 4.3: Choosing a temporary destination

4.1.1 ALERT Algorithm Steps

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: If source and ZD are not in the same zone then it randomly chooses 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.

4.1.2 Advantages

- To offers anonymity protection to sources, destinations, and routes.
- It also has strategies to effectively counter intersection and timing attacks.
- To offer high anonymity protection at a low cost.

4.2 Flowchart for Proposed System

Fig. 4.4 shows a flowchart for ALERT. This project is in MANET so first of all we have to create an MANET environment by using NS2. Following steps indicates a flowchart for ALERT.

1. In first step, ALERT uses the hierarchical zone partition.
2. It randomly chooses a node in the partitioned zone.
3. It checks each node as in same zone or different zone.
4. Again chooses a node in the partitioned zone as a relay node and choose the intermediate neighbor node as data forwarder.

5. It selects a node as temporary destination and performs broadcasting by using GPSR.
6. It checks this step until reach to the destination node.

Following fig. 4.5 shows a Data Flow Diagram for ALERT. In a first step we have to create MANET environment. Here, in this project we have taken 36 nodes and assume that the entire network area is a rectangle in shape and nodes in it are randomly scattered. It divides a network area into zones and chooses a random forwarder. Each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and zd are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node closest to TD. The zone having k nodes where D is present in the destination zone, which is denoted as Zd. The zone in which destination symbol resides is the destination zone. In the last step i.e. graph evaluation; we created an xgraph in NS2. We compare ALERT results with existing anonymous routing protocol ALARM and SDDR. For comparison, we have taken three parameters as below.

1. Packet Delivery Ratio
2. Packet Loss ratio
3. Latency

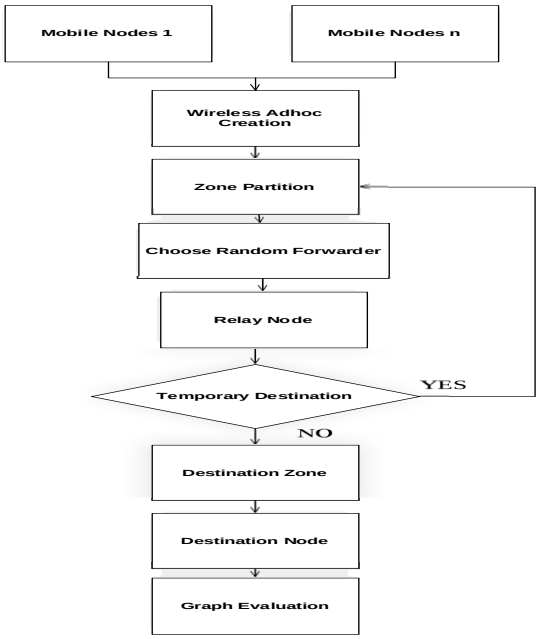

Figure 4.5: DFD for ALERT

4.3 Source Anonymity

ALERT contributes to the achievement of anonymity by restricting a node's view only to its neighbors and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source or a forwarding node. To strengthen the anonymity protection of the source nodes, we further propose a lightweight mechanism called "notify and go." Its basic idea is to let a number of nodes send out packets at the same time as S in order to hide the source packet among many other packets. "Notify and go" has two phases: "notify" and "go." In the first "notify" phase, S piggybacks its data transmission notification with periodical update packets to notify its neighbors that it will send out a packet. The packet includes two random back-off time periods, t and $t0$. In the "go" phase, S and its neighbors wait for a certain period of randomly chosen time $\in [t + t0]$ before sending out messages. Source neighbors generate only several bytes of random data just in order to cover the traffic of the source. T should be a small value that does not affect the transmission latency. A long $t0$ may lead to a long transmission delay while a short $t0$ may result in interference due to many packets being sent out simultaneously. Thus, $t0$

should be long enough to minimize interference and balance out the delay between S and S's farthest neighbor in order to prevent any intruder from discriminating S.

In ALERT, the transmission of each packet is based on a series of RFs who decide which region a packet should be sent to. Between any two RFs, the relays perform the GPSR routing. Each relay has no information on the S or D except the destination zone information. Its routing action is based on the coordinate of the next TD [12]. Therefore, relays can incorporate existing solutions to avoid the dead-end problem without exposing any direct information about the S or D.

4.4 Anonymity Protection and Strategies against Attacks

This section discusses the performance of ALERT in providing anonymity protection and its performance and strategies to deal with some attacks.

4.4.1 Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing, which always takes the shortest path, ALERT makes the route between a S-D pair difficult to discover by randomly and dynamically selecting the relay nodes. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair. Additionally, since an RF is only aware of its proceeding node and succeeding node in route, the source and destination nodes cannot be differentiated from other nodes en route. Also, the anonymous path between S and D ensures that nodes on the path do not know where the endpoints are. ALERT strengthens the privacy protection for S and D by the unlinkability of the transmission endpoints and the transmitted data. That is, S and D cannot be associated with the packets in their communication by adversaries. ALERT incorporates the "notify and go" mechanism to prevent an intruder from identifying which node within the source neighborhood has initiated packets. ALERT also provides k-anonymity to destinations by hiding D among k receivers in ZD. Thus, an eavesdropper can only obtain information on ZD, rather than the destination position, from the packets and nodes en route. The route anonymity due to random relay node selection in ALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ALERT, the routes between two communicating nodes are constantly changing, so it is difficult for adversaries to predict the route of the next packet for packet interception. Similarly, the communication of two nodes in ALERT cannot be completely stopped by compromising certain nodes because the number of possible participating nodes in each packet transmission is very large due to the dynamic route changes.

4.4.2 Resistant to Timing Attacks

In timing attacks, through packet departure and arrival times, an unauthorized user can identify the packets transmitted between S and D, from which it can finally detect S and D. For example, two nodes A and B communicate with each other at an interval of 5 seconds. After a repeated observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, 20:01:38). Then, the intruder would suspect that A and B are communicating with each other. Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In ALERT, the "notify and go" mechanism and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to confuse the intruders. Mainly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D.

4.4.3 Strategy to Counter Intersection Attacks

In an intersection attack, an attacker with information about active users at a predefined time can determine the sources and destinations that communicate with each other through the repeated observations. Intersection attacks are the most common

problem and have not been well resolved. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in ZD during a transmission session. This is because as long as D is conducting communication, the attacker can monitor the change of the members in the destination zone containing D. As time elapses and nodes move, all other members may move out of the destination zone except D. As a result, D is identified as the destination because it always appears in the destination zone.

4.5 Packet Format of ALERT

For successful communication between S and D, S and each packet forwarder embeds the following information into the transmitted packet.

1. The zone position of ZD, i.e., the Hth partitioned zone.

2. The encrypted zone position of the Hth partitioned zone of S using D's public key, which is the destination for data response.

3. The current randomly selected TD for routing.

4. A bit (i.e., 0/1), which is flipped by each RF, indicating the partition direction (horizontal or vertical) of the next RF.

With the encrypted Hth partitioned zone in the information of (2), an attacker needs very high computation power to be able to launch attacks such as dictionary attack. Moreover, the Hth partitioned zone is the position of a zone rather than a position, which makes it even harder to locate the source S.

V. PERFORMANCE ANALYSIS

We created a network area with 36 nodes in NS2 and were successfully able to send data between the source and destination nodes by avoiding timing attacks and intersection attacks. Also providing the low cost and by using the optimal number of forwarders. Tests were conducted with data sent from a source node to a destination node in multiple attempts and the results were analyzed. We measured ALERT performance in comparison with existing anonymous routing protocol ALARM and SDDR. We use the following parameters to evaluation the routing performance in terms of effectiveness on anonymity protection and efficiency:

1. Packet Delivery Ratio

Packet delivery ratio is the ratio of the number of delivered data packet to the destination. The greater value of packet delivery ratio means the better performance of the protocol. Table 5.1 gives packet delivery ratio which compares ALARM, SDDR and ALERT. When ALERT executes, it asks for enter the source node and destination node.

Table 5.1 Packet Delivery Ratio

Transmission Range		**Existing System Anonymous Location-based Protocol**		**Proposed System**
Source	**Destination**	**ALARM[5]** (Anonymous Location-aided Routing in Suspicious MANETs)	**SDDR[18]** (Secure Dynamic Distributed Routing Algorithm)	**ALERT[12]** (Anonymous Location-based and Efficient Routing protocol)
2	28	59	63	68
3	15	66	71	76
7	30	51	56	61
9	35	50	55	64

For example, if we enter a source node as 2 and destination node as 28 then we found the packet delivery ratio of ALERT is too better than existing system. Table 7.1 gives such a various results for packet delivery ratio.

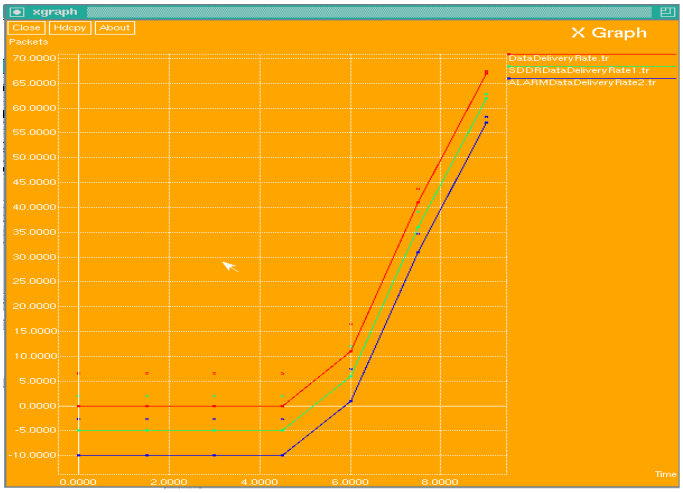

Figure 5.1: Xgraph for Packet Delivery Ratio

Fig. 5.1 shows a graph for packet delivery ratio. Here, we compared results of PDR between ALARM, SDDR and ALERT. ALARM result shown by blue color, SDDR result shown by green color and red color shows an ALERT result. For comparison of packet delivery ratio, here we have taken a various source node and destination node as per table 5.1. Here, red color indicates a PDR is more than ALARM and SDDR.

2. Packet Loss Ratio

Packet Loss Ratio is the ratio of total number of packets dropped during the simulation. The lower value of the packet lost means the better performance of the protocol.

Table 5.2 Packet Loss Ratio

Transmission Range		**Existing System Anonymous Location-based Protocol**		**Proposed System**
Source	**Destination**	**ALARM[5]** (Anonymous Location-aided Routing in Suspicious MANETs)	**SDDR[18]** (Secure Dynamic Distributed Routing Algorithm)	**ALERT[12]** (Anonymous Location-based and Efficient Routing protocol)
2	28	10.2	5.3	0.3
3	15	10	5	0.1
7	30	17.1	12.0	7.1
9	35	14.2	10	6.3

Table 5.2 gives packet loss ratio which compares existing anonymous routing protocols ALARM, SDDR with proposed system ALERT protocol. In experimental results we found the very lower value for proposed system as compare to existing system.

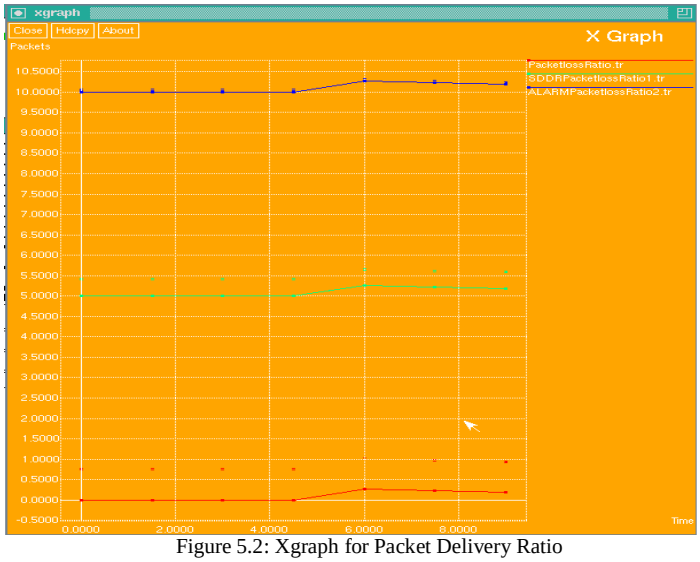

Figure 5.2: Xgraph for Packet Delivery Ratio

When we execute our project, you can enter any number of source and destination node from 0 to 36. Above table shows the some of the results. For example, if we enter source node as a 3 and destination node as 15 then as per system module it executes the ALERT algorithm. First of all, it partitions a network area into zones. Then randomly selects a relay node and forwards packets to it. Then it selects nontraceble route and apply broadcasting. So, by this way, we performed anonymity protection to source node, destination node and route also. And also avoid timing and intersection attacks. Here, for source node 3 and destination node 15 a packet loss ratio is 0.1 and hence it's a better performance than existing anonymous routing protocol. Figure 5.2 depicts network simulation result for packet loss ratio.

5.3 Latency

Latency is the average time taken by a data packet to arrive in the destination. It includes the delay caused by route discovery process and the queue in data packet transmission.

Table 5.3Latency

Transmission Range		**Existing System Anonymous Location-based Protocol**		**Proposed System**
Source	**Destination**	**ALARM[5]** (Anonymous Location-aided Routing in Suspicious MANETs)	**SDDR[18]** (Secure Dynamic Distributed Routing Algorithm)	**ALERT[12]** (Anonymous Location-based and Efficient Routing protocol)
2	28	12	10.6	9
3	15	11.6	10	8
7	30	10.5	9	7
9	35	9	8.5	6

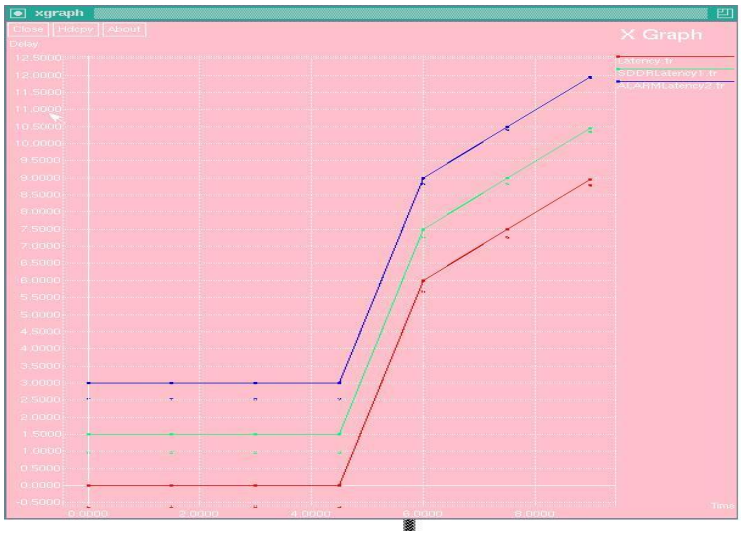

Figure 5.2: Xgraph for latency

Only the data packets that successfully delivered to destinations that counted. The lower value of end to end delay means the better performance of the protocol. Table 5.3 gives latency which compares existing system anonymous protocols ALARM and SDDR with proposed system ALERT protocol. In experimental results we found the very lower value for proposed system as compare to existing system. Above figure 5.3 reprents a xgraph for latency.

VI. CONCLUSION

Existing anonymous routing protocols depend on either hop-by-hop encryption or redundant traffic which generates high cost. And some protocols are not provides complete destination, source and route anonymity protection. ALERT is differentiated by its anonymity protection for source, destinations, and routes. The ALERT makes use of dynamic hierarchical zone partitions and random relay node selections to make it difficult for an intruder to detect the two endpoints and nodes en route. Every packet in ALERT involves the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT also has a capability for anonymity protection of source and destination by hiding the data initiator/receiver.

ACKNOWLEDGEMENT

This would not have been possible without the guidance and help of many people. This is the only section where I have the opportunity of expressing my emotions and gratitude from the core of my heart to them. This paper would not have been successful without enlightened ideas timely suggestion and keen interest of my respected Guide Prof. Avinash P. Wadhe without his best guidance this would have been an impossible task to complete. Also, I would like to express my thankfulness to teaching and non-teaching staff, my friends and all my well-wishers.

References

1. A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, “Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management a Consolidated Proposal for Terminology, Version 0.31,” technical report, 2005.
2. 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.
3. Z. Zhi and Y.K. Choong, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,” Proc. Third Int’l Workshop Mobile Distributed Computing (ICDCSW), 2005.
4. V. Pathak, D. Yao, and L. Iftode, “Securing Location Aware Services over VANET Using Geographical Secure Path Routing,” Proc. IEEE Int’l Conf. Vehicular Electronics and safety (ICVES), 2008.
5. K.E. Defrawy and G. Tsudik, “ALARM: Anonymous Location- Aided Routing in Suspicious MANETs,” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2007.
6. K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.

7. Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.
8. I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.
9. C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.
10. X. Wu, "AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol," IEEE Trans. Mobile Computing, vol. 4, no. 4, pp. 335-348, July/Aug. 2005.
11. B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.
12. Haiying Shen and Lianyu Zhao "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE Transaction on Mobile Computing, vol. 12, no. 6, June 2013.
13. A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm. Workshops (PERCOMW), 2004.
14. 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.
15. 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.
16. S. Ratnasamy, B. Karp, S. Shenker, D. Estrin, R. Govindan, L. Yin, and F. Yu, "Data-Centric Storage in Sensornets with GHT, a Geographic Hash Table," Mobile Network Applications, vol. 8, no. 4, pp. 427-442, 2003.
17. T. Camp, J. Boleng, and V. Davies, "A Survey of Mobility Models for Ad Hoc Network Research," Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
18. Khalil El-Khatib, Larry Korba, Ronggong Song, and George Yee, "Secure Dynamic Distributed Routing Algorithm for Ad Hoc Wireless Networks," published in First International Workshop on Wireless Security and Privacy, Kaohsiung, Taiwan. October 6, 2003.
19. C. Perkins, S. DasnRFC, "Ad hoc On-Demand Distance Vector (AODV) Routing," July 2003,7

AUTHOR(S) PROFILE

Ms. Namrata Ravindra Borkar is a Student of Master of Engineering in Computer Science & Engineering Department from G. H. Raisoni College of Engineering & Management, Amravati, Sant Gadge Baba Amravati University. I completed B.E. in Computer Science & Engineering from SGBAU, Amravati, MS, India. My research interests are Computer Networks and Network Security, etc.

Prof. Avinash P. Wadhe received the B.E from SGBAU Amravati University and M-Tech (CSE) From G.H Raisoni College of Engineering, Nagpur (an Autonomous Institute). He is currently an Assistant Professor with the G.H. Raisoni College of Engineering and Management, Amravati SGBAU Amravati University. His research interest includes Digital Forensics, Network Security, Data mining and Cloud Computing. He has contributed to more than 20 research paper. He had awarded with young investigator award in international conference.

