IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.
PP 13-23
www.iosrjournals.org

EALERT-Enhanced Anonymous Location-based Efficient Routing Protocol

[1]Anjaly Mathai, [2]Deepu S
[1] *PG Scholar,Department of ECE,University College of Engineering,Muttom,India*
[2] *Lecturer,Department of ECE,University College of Engineering,Muttom,India*

Abstract: *The nodes of a Mobile Ad Hoc Network cannot be trusted for the correct execution of critical network functions and therefore security in MANETs is an essential component for maintaining data secrecy. At present MANETs do not have perfect security policy, but it is important to establish secure communication between parties in MANETs. So it is necessary to provide anonymities in networks. Previous anonymous routing protocols are unable to provide complete source,destination and route anonymities. Inorder to provide high anonymity protection with less cost, An Enhanced Anonymous Location based Efficient Routing Protocol (EALERT) can be employed. EALERT dynamically partitions a network into zones,chooses the high energy random forwarder nodes in each zones and randomly chooses intermediate nodes to transmit data,which forms a non traceable anonymous route.and thus reduces the source node load. It also employs hash key randomization to ensure data protection. Extensive simulations are also performed using NS-2 simulation tool to ensure the superior performance of EALERT over existing routing protocols.*

Keywords: *ALERT,Anonymity,GPSR,Hashkey,MANETs,Zone partition*

I. Introduction

The novel technology developments in wireless network such as Bluetooth introduce MANETs. The growth of mobile phones in MANETs a popular research topic since the mid-1990s. It has self organizing capabilities, so that mobile nodes can join and leave the network dynamically. In the recent years, MANETs have attracted a lot of attention in the research community. Still, there are very few real application scenarios where the wide deployment of MANETs is really foreseeable in the near future. It describes the summary of knowledge for security issues in MANETs though there are papers that approach certain aspects of the security field, risks and threats are still there[1].We propose solutions to the current state in respect to the network security.

The mobile ad hoc network has the following typical features;
1. Unreliability of wireless links between nodes: Because of the limited energy supply for the wireless nodes and the mobility of the nodes, the wireless links between mobile nodes in the ad hoc network are not consistent for the communication participants.
2. Constantly changing topology. Due to the continuous motion of nodes, the topology of the mobile ad hoc network changes constantly: the nodes can continuously move into and out of the radio range of the other nodes in the ad hoc network, and the routing information will be changing all the time because of the movement of the nodes.
3. Lack of incorporation of security features in statically configured wireless routing protocol not meant for ad hoc environments. Because the topology of the ad hoc networks is changing constantly, it is necessary for each pair of adjacent nodes to incorporate in the routing issue so as to prevent some kind of potential attacks that try to make use of vulnerabilities in the statically configured routing protocol.

Because of the features listed above, the mobile ad hoc networks are more prone to suffer from the malicious behaviors than the traditional wired networks[12]. Therefore,it is necessary to provide high data protection for MANETs.

Anonymous routing protocols are crucial in MANETs to provide secure communications by hiding node identities and preventing traffic analysis attacks from outside observers[1]. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders), destinations (i.e., recipients), and 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 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. Also, in order to dissociate the relationship between source and destination 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 limited resource is an inherent problem in MANETs, in which each node labours under an energy constraint[10]. MANETs' complex routing and stringent channel resource constraints impose strict limits on the system capacity.The recent increasing growth of multimedia applications(e.g,video transmission) imposes higher requirement of routing efficiency. However, 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 and thus a reliable anonymity needs to be established.

To provide the MANETs with high data secrecy and reliability,An Enhanced Anonymous Location based Efficient Routing Protocol can be suggested in this aspect..It relies on selecting the high energy node among all the nodes in each zone and transmitting the data through random intermediate nodes and uses hash key randomization. EALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. It can also provide high destination and route anonymity to protect the network from malicious observers. EALERT is also resilient to intersection attacks and timing attacks.

II. Related Work

The problem included in providing security to the network is well explained in the literature. Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic.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.

ALERT[2] is one of the recent existing routing protocols that can provode all the three types of anonymities together. It 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 because of its non fixed routing paths for source-destination pair.

But the main disadvantages behind this protocol are;
1. ALERT provides all the three types of anonymities,so there could be large end to end delay in transmitting data.
2. It does not satisfy the network constraints in larger network with more number of mobile nodes.
3. Even if the protocol is able to hide the node identities from the malicious attackers it has no methods to detect and identify those malicious nodes.
4. ALERT is implemented under the assumption that the participating nodes are having relatively low velocity, But it never takes into account the high velocity movement of the nodes. In summary,it cannot protect the network from active and stronger attackers.
5. Throughput is the average number of packets successfully delivered per unit time. Usually, it is observed in ALERT that as the packet size and time interval increases, throughput decreases.

Anonymous Location Aided Routing in Suspicious MANETs(ALARM) 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[3]**.**ALARM uses node's current locations to securely disseminate and construct topology snapshots and forward data.With the aid of advanced cryptographic techniques (e.g., group signatures).In this technique, the mobile node presents its secondary identity which helps the node to become untraceable by all the other nodes. In ALARM protocol, certain packets are exchanged for mutual authentication and messages are digitally signed. The digital signature approach leads to message integrity and confidentiality. It uses node's current location value from Location Announcement Message (LAM) to construct a secure MANET map. Location information has become progressively more available through small and cheap GPS receivers. This technique utilizes proactive mode of location based routing. ALARM provides both security and privacy features, including node authentication, data integrity, anonymity, and non-traceability

(tracking-resistance). It also offers protection against passive and active insider and outsider attacks. It also offers resistance to certain insider attacks. ALARM has the following goals:
1. Privacy: There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations cannot be linked.
2. Performance: Security and privacy goals must be achieved without compromising the performance.
3. Security: The network must be resistant to passive and active attacks occurring from both outsider and insider malicious nodes.

But the main disadvantage behind this protocol is that it cannot provide location anonymity of source and destination. Thus a malicious attacker may be easily able to eavesdrop the data.

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks[4] can be deployed in hostile environments. It address two closely related problems: For route anonymity, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for location privacy, ANODR ensures that adversaries cannot discover the real identities of local transmitter.

The anonymous route discovery process establishes an on-demand route between a source and its destination. Each hop en route is associated with a random route pseudonym. Since data forwarding in the network is based on route pseudonyms with negligible overhead, local senders and receivers need not reveal their identities in wireless transmission.As a result, in each locality eavesdroppers or any bystander other than the forwarding node can only detect the transmission of wireless packets stamped with random route pseudonyms. It is hard for them to trace how many nodes in the locality, who is the transmitter or receiver, where a packet flow comes from and where it goes to (i.e., what are the previous hops and the next hops en route), let alone the source sender and the destination receiver of the flow.It presents an untraceable and intrusion tolerant routing protocol for mobile ad hoc networks.The disadvantage of this protocol includes its poor performance in high mobility scenarios.

An ad hoc on-demand position-based private routing algorithm, called A02P[5], is proposed for communication anonymity. Only the position of the destination is exposed in the network for route discovery. To discover routes with the limited routing information, a receiver contention scheme is designed for determining the next hop. Pseudo identifiers are used for data packet delivery after a route is established. Real identities (IDS) for the source nodes, the destination nodes, and the forwarding nodes in the end-to-end connections are kept private. Anonymity for a destination relies on the difficulty of matching a geographic position to a real node ID. This can be enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary. To further improve destination privacy, A02P is proposed. In this protocol, the position of a reference point, instead of the position of the destination, is used for route discovery.Analytical models are developed for evaluating the delay in route discovery and the probability of route discovery failure. A simulator based on NS-2[7] is developed for evaluating network throughput. Analysis and simulation results show that, while A02P preserves communication privacy in ad hoc networks, its routing performance is comparable with other position-based routing algorithms.

Mobile Ad-Hoc Networks 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. 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, on demand location-based anonymous MANET routing protocol (PRISM)[6] achieves privacy and security against both outsider and insider adversaries. The PRISM protocol which supports anonymous reactive routing in suspicious location based MANETs. PRISM relies on group signatures to authenticate nodes, ensure integrity of routing messages while preventing node tracking. PRISM works with any group signature scheme and any location-based forwarding mechanism. PRISM reveals less of the topology and is therefore extra privacy-friendly. This provides privacy against insider and outsider adversaries. Source authenticates the destination and destination authenticates source node. It imports one time secrete key for authentication and encryption. Packets are transmitted based on location forwarding mechanism,but it cannot provide any route anonymity that may allow the malicious attackers to track the route.

Greedy Perimeter Stateless Routing(GPSR)[8] is a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet forwarding decisions. GPSR makes greedy forwarding decisions using only information about a router's immediate neighbors in the network topology. When a packet reaches a region where greedy forwarding is impossible, the algorithm recovers by routing around the perimeter of the region. By keeping state only about the local topology, GPSR scales better in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations increases. Under mobility's frequent topology changes, GPSR can use local topology information to find correct new routes quickly.

The Zone Routing Protocol (ZRP)[9] combines the advantages of the proactive and reactive approaches by maintaining an up-to-date topological map of a zone centered on each node,thus using hybrid approach for routing. Within the zone, routes are immediately available. For destinations outside the zone, ZRP employs a route discovery procedure, which can benefit from the local routing information of the zones.it aims to address excess bandwidth and long route request delay of proactive and reactive routing protocols.But ZAP focuses only on destination anonymity and so the degree of protection is low.

III. System Methodology

The limited resource is an inherent problem in MANETs, in which each node labours under an energy constraint. MANETs' complex routing and stringent channel resource constraints impose strict limits on the system capacity[10].The recent increasing growth of multimedia applications (e.g.,video transmission) imposes higher requirement of routing efficiency. However, 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 and thus a reliable anonymity needs to be established.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Enhanced Anonymous Location-based and Efficient Routing Protocol (EALERT). EALERT 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 [8] 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, EALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. EALERT is also resilient to intersection attacks and timing attacks.

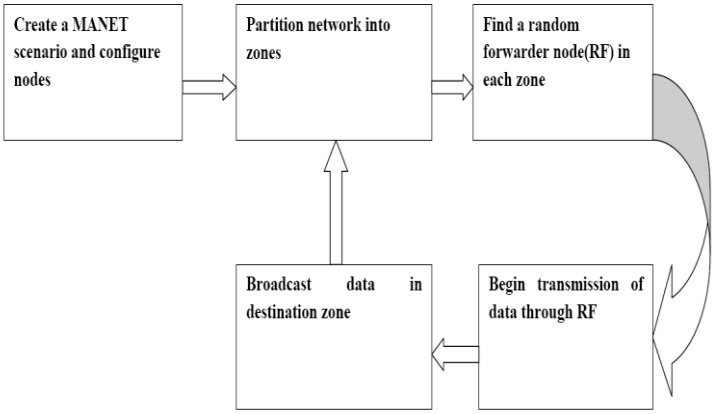

Fig 3.1 EALERT-Block diagram

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.So 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. The main problem while implementing ALERT[2] was that the energy of the source nodes seems to degrade after a certain time, thus the communication may become dead. This is due to the continuous functioning of the source node assigned to it. In EALERT,partial function can be handed over to Random Forwarders (RF),thus persisting the communication for long period of time.

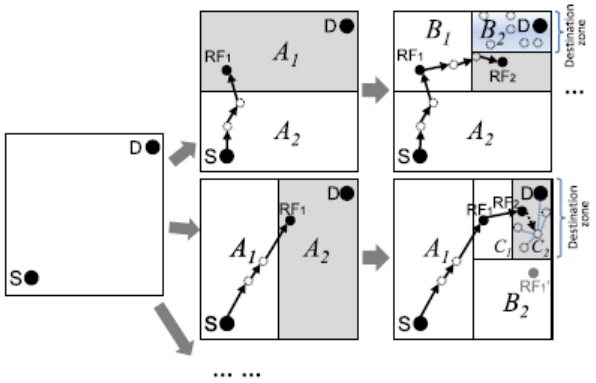

Fig 3.2 Example of zone partition

EALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically determined intermediate relay nodes. As shown in the upper part of Fig 3.2, 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. EALERT 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. A packet in EALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. 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, EALERT sets the partition in the alternative horizontal and vertical manner in order to ensure that a packet approaches D in each step.

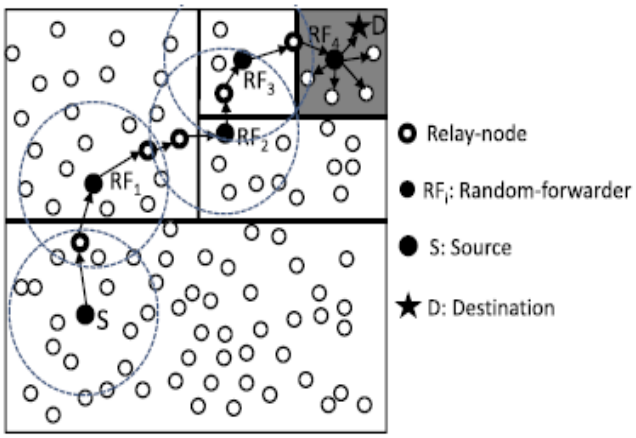

Fig 3.3 Routing among zones in EALERT

Fig 3.3 shows an example of routing in EALERT. 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 3.3 is the destination zone. Specifically, in the EALERT 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.Then it chooses a Random Forwarder node (RF),possessing the highest energy among all the nodes present in each zone.Using the GPSR algorithm,each RF calculates the shortest path of data transmission with all other nodes in each zone.Thus the data will be transmitted between various RFs,relay nodes and finally to destination D.The main difference of EALERT in contrast to other existing routing protocols is that the nodes are considered to be in motion.Therefore,periodic updation of routing table is required.

In contrast to ALERT[2] where the source node performs all the functions including shortest path calculation,selection of data routing,source anonymity etc,and also malicious nodes will be easily able to detect the source and destination nodes due to their stationary nature, EALERT assigns the responsibility partially to the RF present in each zone.It has the function to select the routing paths,thus saves the energy of the source node.

In order to hide the packet content from adversaries,EALERT employs hash key randomization method in which the hash key is known only to source and destination, that enhances protection. Hash functions are functions that compress an input of arbitrary length to a result with a fixed length output called a hash value. If hash functions satisfy additional requirements, they are a very powerful tool in the design of techniques to protect the authenticity of information.Thus they provide confidentiality, source and destination authentication and data authentication.A cryptographic hash function H is a hash function with security properties;

1. H should accept a block of data of any size as input.
2. H should produce a fixed-length output no matter what the length of the input data is.
3. H should accept an input of any length, and outputs a random string of fixed length.
4. Given a message M, it is easy to compute its corresponding code h, this makes hardware and software implementations cheap and practical.
5. H should behave like random function while being deterministic and efficiently reproducible.

In EALERT,only the source and destination node shares the secret key and all other nodes are unaware of the key being shared between the terminal nodes.The communication is established in such a way that source will send the data randomly in block format along with the hash key specified for each data.Dummy data block will also be sent to confuse the hacker.Even if the attacker is able to track the data in extreme cases,it is of no use, since they are unaware of the key for decrypting the data.Finally the destination node rearranges the data block and decrypts the data. Usually the nodes being deployed in the field will be with different speed and energy,but the hacker may introduce certain malicious nodes with same energy and speed as that of the original,so that they may eavesdrop the data being passed.Thus a clone may be detected in the scenario,not necessary. In such cases,the algorithm tries to remove both the similar nodes to improve the degree of security.

3.1. Routing Algorithm

The routing algorithm of EALERT can be summarized as follows;

1. Deploy the nodes.
2. Make movement to all nodes.
3. Find neighbor node distances using GPSR algorithm and update zone regularly.
4. Calculate the initial energy of all nodes.
5. Choose intermediate nodes.
6. Assign the RF node with maximum energy in each zone.
7. Apply the node transition probability protocol to RF node.
8. Check clone detection in each zone.
9. If no clone is detected,use reverse hashing key randomization(with hash key).
10. Re-route all routing paths with dynamic interval.

3.2. Anonymity Protection And Strategies Against Attacks

EALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing] which always takes the shortest path, EALERT 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. EALERT 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. EALERT incorporates the notify and go mechanism to prevent an intruder from identifying which node within the source neighborhood has initiated packets.

EALERT 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 EALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route. In EALERT, 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 EALERT 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. In contrast, these attacks are easy to perform in geographic routing, since the route between a given S-D pair is unlikely to change for different packet transmissions, and thus, the number of involved nodes is much smaller than in EALERT.

In timing attacks[1], through packet departure and arrival times, an intruder 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 long 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 [2]. In EALERT, the notify and go mechanism and the broadcasting in ZD both put the interaction between S-D into two sets of nodes to obfuscate intruders. More importantly, 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.

In an intersection attack[10], an attacker with information about active users at a given time can determine the sources and destinations that communicate with each other through repeated observations. Intersection attacks are a well known problem and have not been well resolved. Though EALERT 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.

Fig.a in fig 3.4 is the status of a ZD after a packet is broadcasted to the zone. The arrows show the moving directions of nodes. We can see that nodes a, b, c, d, and D are in ZD. Fig.b is the subsequent status of the zone the next time a packet is transmitted between the same S-D pair. This time, nodes d, e, f, g, and D are in ZD. Since the intersection of the in-zone nodes in both figures includes d and D, D could be identified by the attacker. Therefore, the longer an attacker watches the process, the easier it is to identify the destination node.

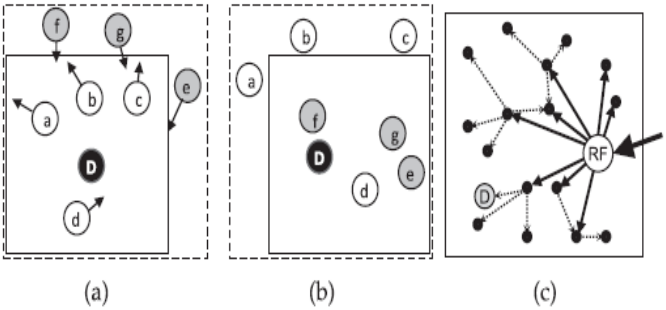

Fig 3.4 Intersection attack and solution

The attacker can be puzzled and lose the cumulated observation by making it occasionally fail to observe D's reception of packets. Since packets are delivered to ZD constantly in long-duration sessions rather than using direct local broadcasting in the zone, the last RF multicasts packet pkt1 to a partial set of nodes, say m nodes out of the total k nodes in the zone. The m nodes hold the packets until the arrival of the next packet pkt2. Upon the arrival of the next packet, the m nodes conduct one-hop broadcasting to enable other nodes in the zone to also receive the packet in order to hide D. Fig.c shows the two-step process with the first step in solid arrows and the second step in dashed arrows. We can see that the first step reaches a number of nodes in the destination zone, but the destination is reached in the second step. Because the deliveries of pkt1 and pkt2 are mixed, an attacker observes that D is not in the recipient set of pkt1 though D receives pkt1 in the delivery time of pkt2. Therefore, the attacker would think that D is not the recipient of every packet in ZD in the transmission session, thus foiling the intersection attack.

IV. Results And Discussions

Our experiments verify that the proposed protocol can, indeed, successfully cope with a high number of adversaries, while operating in an adversarial environment. The simulation is done by using network simulator (NS-2) software[7], with different number of mobile nodes ranging from 0-150.The simulation time is 30 seconds, and the simulated mobility network area is 600m × 400m square. To represent ad hoc network we deploy 150 mobile nodes.One chosen as the source(node 0) and one as destination(node 149).

The important results that are generated through extensive simulations can be shown in the succeeding graphs that show the enhanced performance of EALERT compared with other protocols. The factors which evaluates the effectiveness of anonymity protection and efficiency are;

1. Latency per packet
2. Energy remaining
3. Average key generating time
4. Network life time
5. Source anonymity
6. Destination anonymity

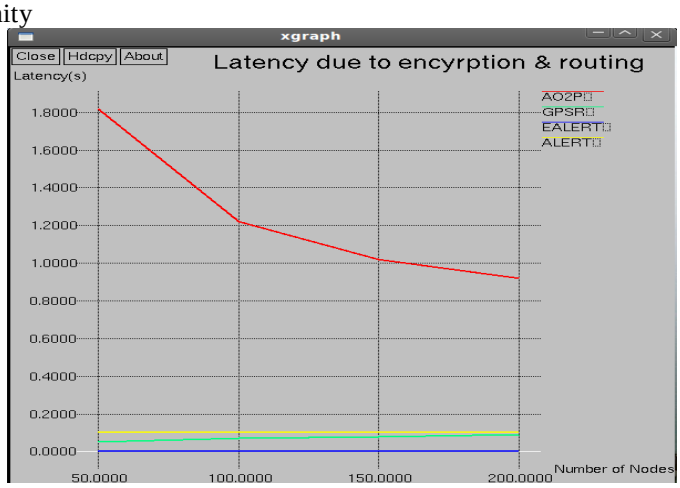

Fig 4.1 Latency caused by encryption and routing

The graph represents the latency per packet versus the total number of nodes ie,node density.As depicted in the graph,the latency of EALERT is much lower than ALARM[3],AO2P[4] and ALERT[2].This is caused due to the time cost of encryption,since it uses the hash key randomization method of cryptography.It needs to encrypt the packets once,while AO2P needs to encrypt in each hop in routing and ALARM needs to periodically authenticate its neighbours.

Fig 4.2 shows the superior performance of EALERT as compared to ALERT.As the transmission range increases the energy of the source node also reduces,but much more in case of ALERT,since the source node is assigned with all the responsibilities of routing.While in case of EALERT,partial function is carried out by RFs.

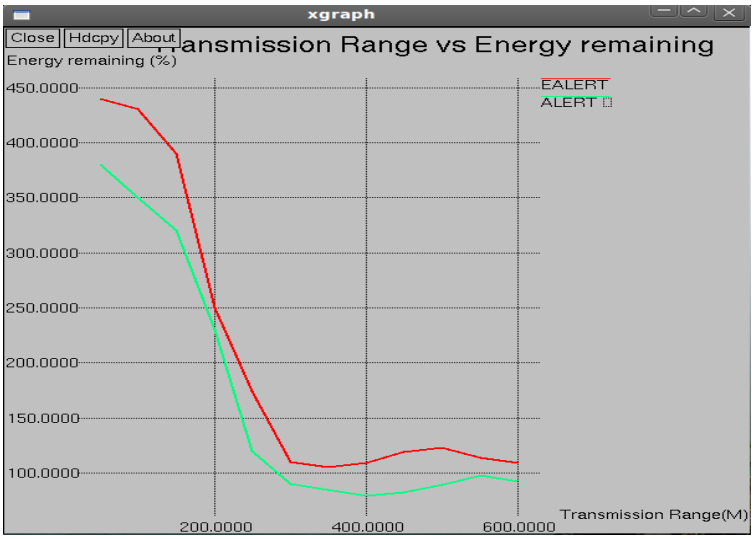

Fig 4.2 Transmission range vs energy remaining

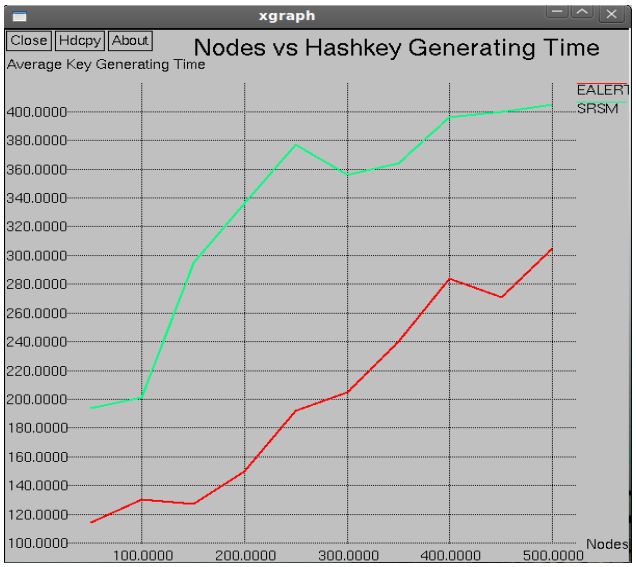

Fig 4.3 Nodes vs hash key generating time

As shown in thr graph 4.3,as number of nodes in MANETs increases the time needed to generate the hash function also increases since all the nodes participating needs hash function for ensuring protection.Here EALERT is compared with SRSM protocol since ALERT doesn't employ hash keys.The graph shows the superior performance of EALERT.

Source anonymity is much better employed in EALERT as can be seen from the graph 4.4,since the energy of the source can be saved for long period of time due to the involvement of RFs.Thus for more data duration,source anonymity can be continued with less degree of degradation.

The network life time is one important parameter while dealing with the perfimance evaluation.More the life time of a network more is its reliability.The network life time of EALERT is more as compared to ALERT [2] as shown in the graph 4.5,since the degradation of source node energy is less.

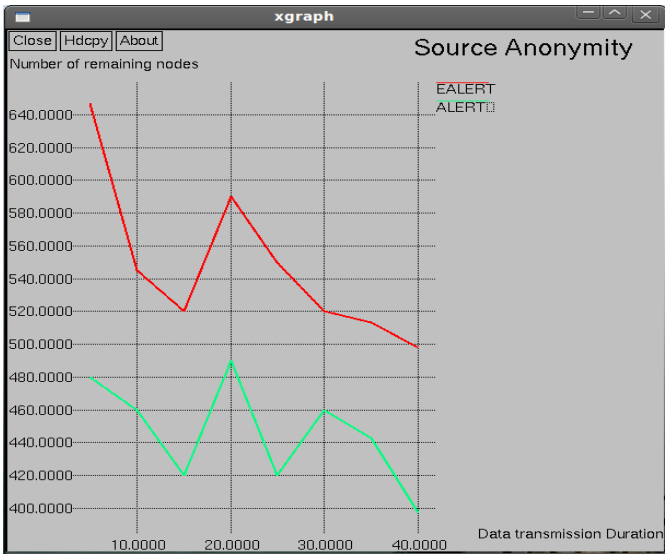

Fig 4.4 Source anonymity

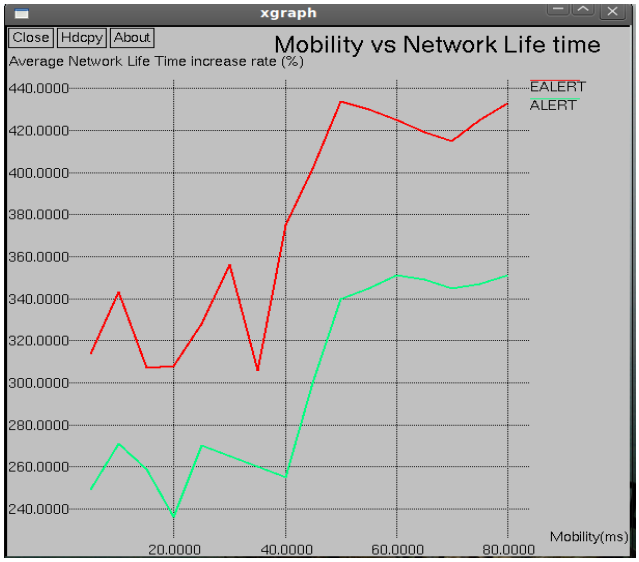

Fig 4.5 Mobility vs network life time

From the graph 4.6,it can be observed that higher node mobility leads to less remaining nodes(ie.destination anonymity) and hence negatively impacts the anonymity protection of the destination.This means that EALERT is more suitable in low mobility environments to protect destinations from destination attack.

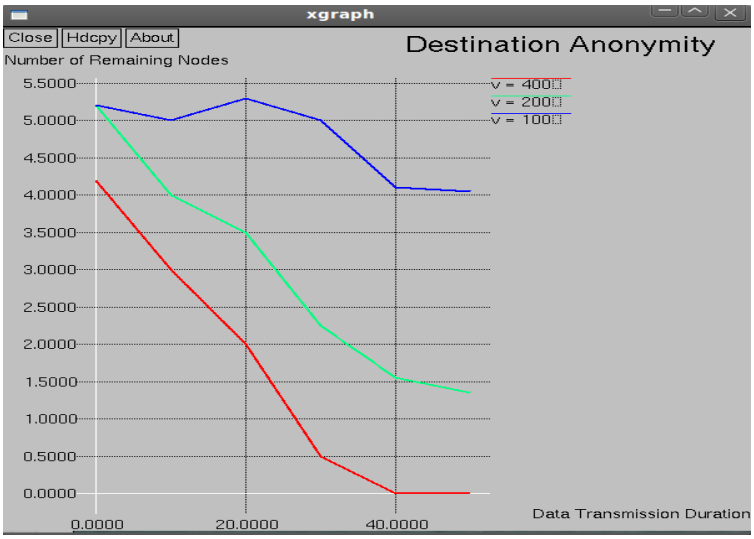

Fig 4.6 Destination anonymity

V. Conclusion

Security in MANET is an essential component for basic network functions like packet forwarding and routing and network management. Previous anonymous routing protocols are unable to provide complete source, destination and route anonymity. In order to provide high anonymity protection with low cost, EALERT can be employed. EALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. It reduces the source node load by assigning the routing responsibility to random forwarder nodes in each zone and each of the nodes uses hash keys to ensure data protection. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/receivers and uses local broadcasting for destination anonymity. In addition, EALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. EALERT is also resilient to intersection attacks and timing attacks. Experimental results demonstrates the superior performance of EALERT as compared to existing routing protocols. Future work relies on choosing a deputy RF node having the second energy value when the RF becomes dead due to the attack from a hacker.

References

[1]. Y. Zhang,W.Liu,andW. Luo, Anonymous Communications in Mobile Ad Hoc Networks, Proc. IEEE INFOCOM, 2005.
[2]. L. Zhao and H. Shen, ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs, Proc. Int'l Conf. Parallel Processing (ICPP), 2011.
[3]. K.E. Defrawy and G. Tsudik, ALARM: Anonymous Location- Aided Routing in Suspicious MANETs, Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.
[4]. 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.
[5]. 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.
[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]. The Network Simulator- ns-2, http://www.isi.edu/nsnam/ns, 2012.
[8]. K.C. Lee, J. Haerri, L. Uichin, and M. Gerla, Enhanced Perimeter Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios, Proc. IEEE GlobeCom Workshops, 2007.
[9]. Nicklas Beijar, Zone Routing Protocol (ZRP), Networking Laboratory, Helsinki University of Technology,2006.
[10]. Elizabeth, Royer, Chai-Keong, Toh: A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, April 1999, IEEE Personal Communications.
[11]. Perkins, C. E., Royer, E. M.: Ad-hoc On-Demand Distance Vector Routing, February 1999, Proc. 2nd IEEE Workshop on Mobile Computer Systems and Applications, pp. 90-100.
[12]. Perkins, C. E., Bhagwat, P.: Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers, October 1994,Computer Communications, pp. 234-244
[13]. G.Nithya,G.Sujatha,Improving The Security in MANETS Using MRF ALERT Protocol, IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014