ISSN No. 0976-5697

Volume 5, No. 1, Jan-Feb 2014

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Lowcost and High Anonymity Protection to Manets through Alert

Mr.V. Tamizhazhagan*, Dr. R. Saminathan and Ms. V. Niranchana
Department of Computer Science & Engineering, Annamalai University
Annamalainagar – 608 002, Tamil Nadu, India
tamizh5956@gmail.com, niranchu.bcse06@gmail.com

Abstract: manets feature such as self-organizing and independent infrastructures make them an ideal choice for uses such as communication and information sharing. They use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. On the other hand, limited resource is an inherent problem in manets, in which each node labors under an energy constraint. Manets' complex routing and stringent channel resource constraints impose strict limits on the system capacity. Further, 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 is a battle. To offer high anonymity protection at a low cost, the project proposes 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. Alert hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, offers anonymity protection to sources, destination, and routes. Anonymous routing protocol is crucial in manets to provide secure communication by hiding node identities and preventing traffic analysis attack from outside observers.

Keywords - Mobile Ad Hoc Networks, Anonymity, Routing Protocol, Geographical Routing

I. INTRODUCTION

Anonymous routing protocols[6] are crucial in MANETs to provide secure communications by hiding node identities and preventing 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 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 (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[8] where location devices may be equipped. To provide high anonymity protection (for sources, destination, and route) with low cost, we propose an 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 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[4] 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. We theoretically analyzed ALERT in terms of anonymity and efficiency. We also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocol. ALERT provides route anonymity, identity, and location anonymity of source and destination. **Low cost:** Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection. **Resilience to intersection attacks and timing attacks:** ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue . ALERT can also avoid timing attacks because of its nonfixed routing paths for a source and destination pair. **Extensive simulations:** We conducted comprehensive experiments to evaluate ALERT's performance in comparison with other anonymous protocols. This protocol is implemented over the MANET network and simulated using NS2[13].

II. RELATED WORKS

A. Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology:

The anonymity set is the set of all possible subjects. With respect to acting entities, the anonymity set consists of the subjects who might cause an action. With respect to addresses, the anonymity set[1] consists of the subjects who might be addressed. Therefore, a sender may be anonymous only within a set of potential senders, his/her sender anonymity set, which itself may be a subset of all subjects worldwide who may send messages from time to time. The same is true for the recipient, who may be anonymous within a set of potential recipients, which form his/her recipient anonymity set. Both anonymity sets may be disjoint, be the same, or they may overlap. The anonymity sets may vary over time. A subject is a possibly acting entity such as, e.g., a human being (i.e. a natural person), a legal person, or a computer. (An organization is not acting as a legal person we neither see as a single subject nor as a single entity, but as (possibly structured) sets of subjects or entities. Otherwise, the distinction between "subjects" and "sets of subjects" would completely blur. But we need that distinction e.g. to sensibly define group pseudonyms.) Since sending and receiving of particular messages are special cases of "attributes" of senders and recipients, this is slightly more general than the setting. This generality is very fortunate to stay close to the everyday meaning of "anonymity" which is not only used w.r.t. subjects active in a particular context, e.g. senders and recipients of messages, but to subjects passive in a particular context as well, e.g. subjects the records within a database relate to. "Not identifiable within" means "not uniquely characterized within". Anonymity ensures that a user may use a resource or service without disclosing the user's identity.

The requirements for anonymity provide protection of the user identity [1]. Anonymity is not intended to protect the subject identity. [1] Anonymity requires that other users or subjects are unable to determine the identity of a user bound to a subject or operation." Compared with this explanation, our definition is more general as it is not restricted to identifying users, but any subjects. the "usual suspects" :-) The set of possible subjects depends on the knowledge of the attacker. Thus, anonymity is relative with respect to the attacker. Addressees are subjects being addressed. Since we assume that the attacker does not forget anything he knows, the anonymity set cannot increase w.r.t. a particular action. Especially subjects joining the system in a later stage do not belong to the anonymity set from the point of view of an attacker observing the system in an earlier stage. (Please note that if the attacker cannot decide whether the joining subjects were present earlier, the anonymity set does not increase either: It just stays the same.) Due to linkability, cf. below, the anonymity set normally can only decrease. All other things being equal, anonymity is the stronger, the larger the respective anonymity set is and the more evenly distributed the sending or receiving, respectively, of the subjects within that set from the above discussion follows that anonymity in general as well as the anonymity of each particular subject is a concept which is very much context dependent (on, e.g., subjects population, attributes, time frame, etc). In order to quantify anonymity within concrete situations, one would have to describe the system in sufficient detail which is practically not (always) possible for large open systems (but maybe for some small data bases for instance). Besides the quantity of anonymity provided within a particular setting, there is another aspect of anonymity: its robustness.

Robustness of anonymity characterizes how stable the quantity of anonymity is against changes in the particular setting, e.g. a stronger attacker or different probability distributions[1]. We might use quality of anonymity as a term comprising both quantity and robustness of anonymity. To keep this text as simple as possible, we will mainly discuss the quantity of anonymity in the sequel, using the wording "strength of anonymity".

B. Mix Zones: User Privacy in Location-aware Services:

The model assumes the existence of a trusted middleware system, positioned between the underlying location system(s) and untrusted third-party applications. Applications register interest in a geographic space with the middleware; we refer to this space as an application zone.

Example spaces include hospital grounds, university buildings or a super-market complex. Users register interest in a particular set of location-aware applications and the middleware limits the location information received by applications to location sightings of registered users located inside the application zone. Each user has one or more unregistered geographical regions [12]where no application can trace user movements; we call such areas mix zones, because once a user enters such a zone, user identity is mixed with all other users in the mix zone[2], as will become clearer shortly. A boundary line is defined as the border between a mix zone and an application zone. Applications do not receive a traceable user identity associated with a location sighting, but instead receive a pseudonym. The pseudonym[1] allows communication between user and application; such communication must pass through a trusted intermediary to pre- vent trivial linking of a pseudonym with an underlying user identity.

The pseudonym of any given user changes whenever the user enters a mix zone. The aim of the mix zone model[2] is to prevent tracking of long-term user movements, but still permit the operation of many short-term location-aware applications. We have shown in our previous paper how some more obvious pseudonymity[1] mechanisms can be trivially defeated, allowing identication of the user behind each pseudonym. Since third-party applications are untrusted they may collude, therefore all third-party application providers are treated as one combined global hostile observer. How well can this attacker correlate movements of users into the mix zone with movements into a subsequent application zone? In other words, can the attacker link together user pseudonyms, and therefore track long-term user movements? Consider an example scenario. An attacker may be able to use historical data from nearby application zones or analytical methods to infer likely user movement across the mix zone. User exit boundary line and time is often strongly correlated to user entry boundary line and time. For example, two users walking down a corridor in opposite directions are much more likely to continue in the same direction than turn around and retrace their steps.

The middleware can use historical data from inside the mix zone to provide a (probably far superior) model of user movement; movement patterns are not time- invariant, but are likely to be self-similar over short time spans, after twenty-four hours and after seven days. A movement matrix is generated to record the frequency of ingress and egress points for different time periods across the mix zone[2] at different times in the day or week. Such a movement matrix provides an upper bound on the accuracy of the model the attacker can generate. A location system scenario (e.g. E911-enabled cellular phones in an urban setting) can therefore be examined using the mix zone model[2] the model takes into ac- count the geometry of the zones, the temporal and spatial resolution of the sightings, and the statistical behavior of the user population to provide a quantitative assessment of how well a hostile observer is able to deanonymize individual users. When designing a system this analysis can be run iteratively, changing the layout of the zones or the resolution of the sightings until the desired level of anonymity[1] is achieved.

C. ALARM: Anonymous Location-Aided Routing in Suspicious MANETs:

This technique[3] requires an off-line group manager (GM) that initializes the underlying group signature scheme and enrolls all legitimate MANET nodes as group members. (This is done well before MANET deployment.) In case of a dispute, the GM is responsible for opening the contested group signature and determining the signer. Depending on the specific group signature scheme, the GM may also have to handle future joins for new members as well as revocation of existing members. However, we claim that in most envisaged MANET[10] scenarios, membership is likely to be fixed, i.e., all joins can be done in bulk, a priority. Also, revocation might not be feasible since it would require propagating in real-time updated revocation information to all legitimate MANET nodes.

D. On Delivery Guarantees of Face and Combined Greedy-Face Routing in Ad Hoc and Sensor NetworksK

A simplified variant of the GFG protocol strictly employs the left hand traversal rule (the same definition is possible for the right hand rule as well). When face exploration encounters the next closer intersection the first edge of the next visited face is determined by simply choosing the edge lying in counterclockwise direction from the intersected edge. Obviously, when strictly applying the left hand rule[5] in this method will visit the same face sequence as GFG, i.e. F1, F2, F1, F3, F4. This is due to the fact, that (in the depicted case) on encountering the next edge crossing with starting at a point p, the next adjacent face which intersects with the open line segment point can always be traversed by using the left hand rule and selecting from the crossing edge the next one in counterclockwise direction[2].

E. A Survey of Mobility Models for Ad Hoc Network Research:

Mobility models[11] that represent multiple MNs whose actions are completely independent of each other. In an ad hoc network[9], however, there are many situations where it is necessary to model the behavior of MNs as they move together. For example, a group of soldiers in a military scenario may be assigned the task of searching a particular plot of land in order to destroy land mines, capture enemy attackers, or simply work together in a cooperative manner to accomplish a common goal. In order to model such situations, a group mobility model[5] is needed to simulate this cooperative characteristic. We present five group mobility models. We note that four of the five group mobility models are closely related. The most general of these four models is the Reference Point Group Mobility (RPGM) model[10].

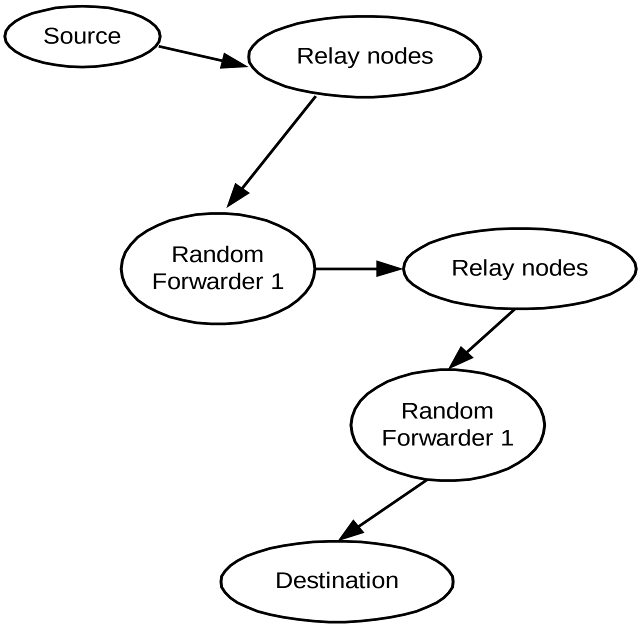


Figure. 1 Routing process in Alert

Fig. 1 Routing process in ALERT represents how the data is transferred from source to destination ,source send the data to the relay nodes and the random location selected in the zone, nearest node to the relay node, then it forwads the message packets to the random forwarder, it sends to the destination .

III. NETWORK MODEL

Network model consider the random way point model and the group mobility model Network are classified into Zone. 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[7] 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.

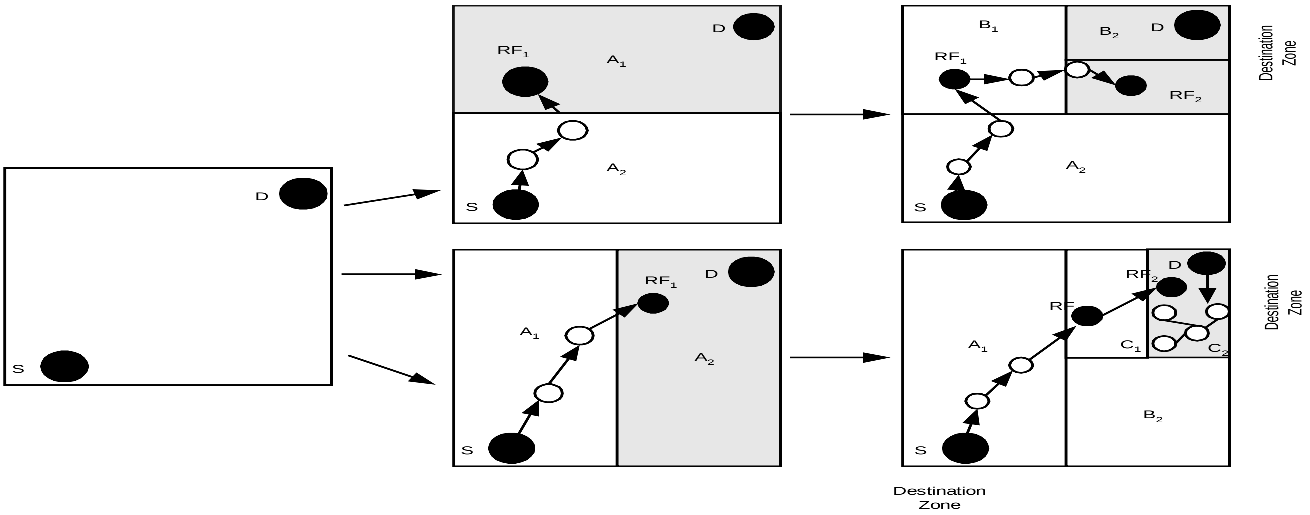


Figure. 2 Hierarchical Zone Partition and Routing Process in ALERT

A. *Architecture:*

The network field is dynamically partitions a into a zones and randomly chooses nodes in zones as intermediate relay nodes[Fig. 2], which form a non traceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to k -nodes in the destination zone, providing k-anonymity to the destination.

IV. ZONE PARTITION

In ALERT the communication range is partitioned into the Zones. If the source and destination are not present in the same zone, during the Zone partition the condition to be considered is, the forwarder and the destination not present in the same zone. Till this condition satisfied it will be portioned into horizontal and vertical zones. In this, Random forwarder is selected randomly in the zone. RF is selected in the following way. First the randomly the location is selected from the particular Zone. The node nearest to the location is selected as the Random Forwarders.

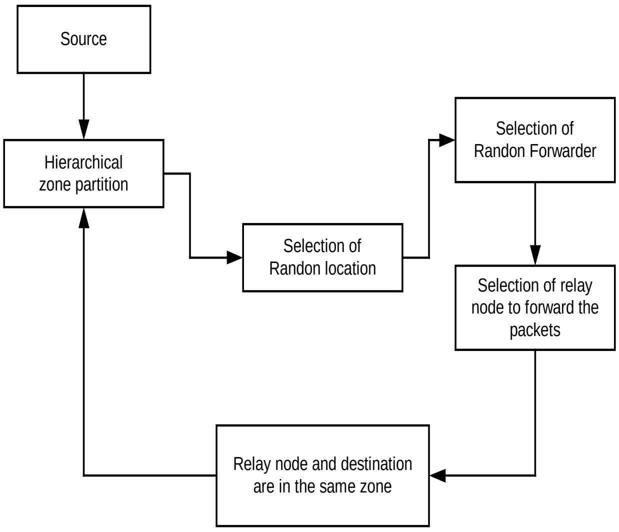

Source
Hierarchical zone partition
Selection of Randon location
Selection of Randon Forwarder
Selection of relay node to forward the packets
Relay node and destination are in the same zone

Figure. 3 Zone Partition in Alert

Fig.3.Zone partition in ALERT represents how the data is transferred from source to destination ,source send the data to the relay nodes and the random location selected in the zone, nearest node to the random location then it forwads the message packets to the random forwarder, it sends to the destination .

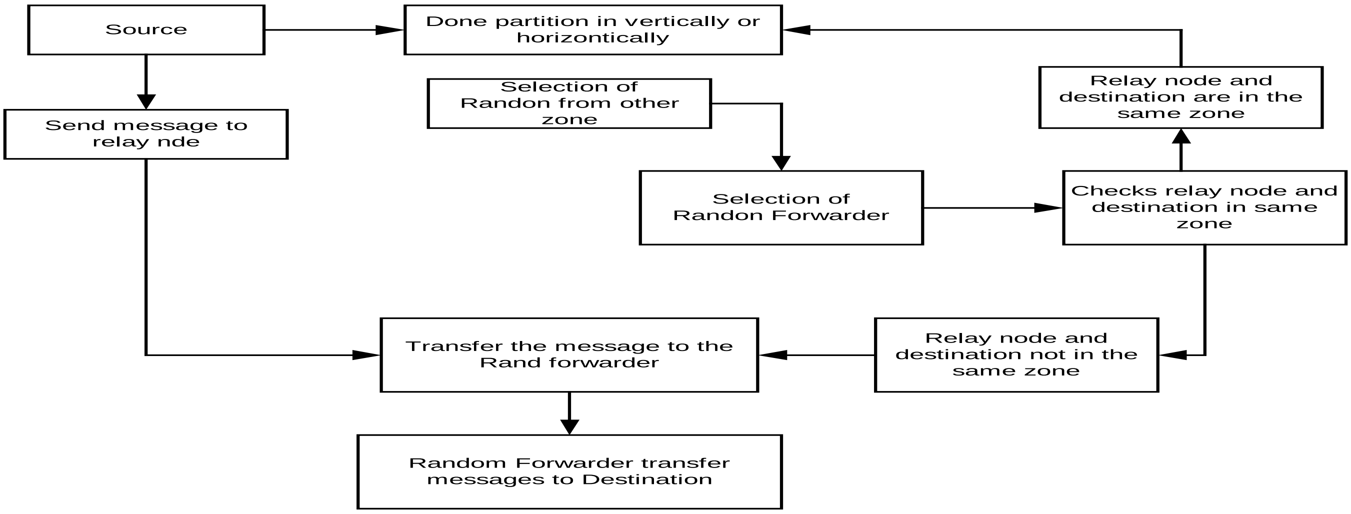

Source
Done partition in vertically or horizontically
Send message to relay nde
Selection of Randon from other zone
Relay node and destination are in the same zone
Selection of Randon Forwarder
Checks relay node and destination in same zone
Transfer the message to the Rand forwarder
Relay node and destination not in the same zone
Random Forwarder transfer messages to Destination

Figure. 4 Alert Process

Fig.4 explains how the zone partitions take place in ALERT. Consider the Source and the destination is in the same zone and the packet transfer taken place in the following ways. First the zone is divided into horizontal or vertical zone. And the random location selected in the zone, nearest node to the random location considered as the Random Forwarder .When the zone partition taken place one condition to be checked whether the forwarder and Zone destination are not in the same zone. Hierarchical partition takes place till the above condition satisfied. And then routing process takes place in ALERT.

V. ALERT ROUTING

ALERT 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.5 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.

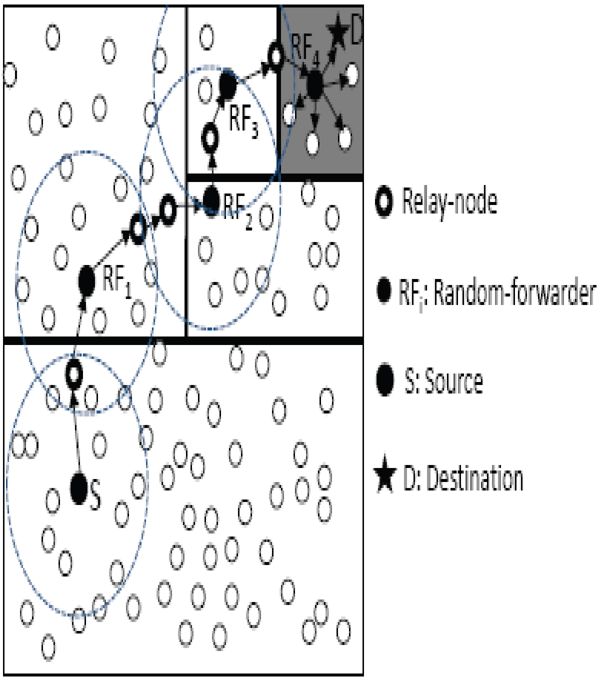
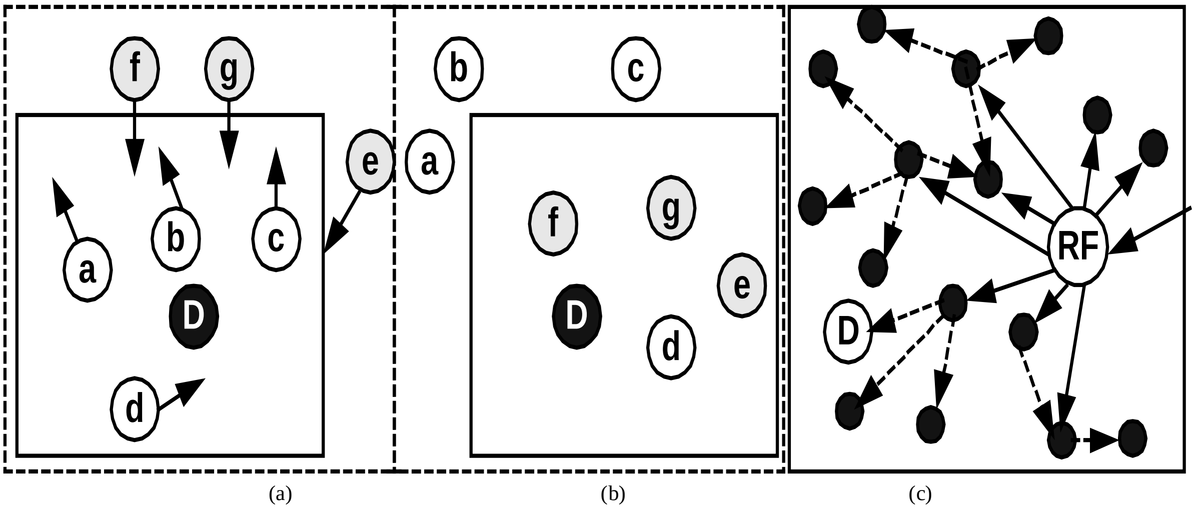


Figure.5 Alert Routing Process

VI. RESILIENCE TO INTERSECTION ATTACK:



(a) (b) (c)

Figure. 6 Intersection Attack

Fig. 6(a) 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. 6(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. It uses the one –hop broadcasting technique to avoid this.

Fig. 6(c) shows the two-step process with the first step in solid arrows and the second step in dashed arrows. It can be 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 *pkt*1 and *pkt*2 are mixed, an attacker observes that *D* is not in the recipient set of *pkt*1 though *D* receives *pkt*1 in the delivery time of *pkt*2. 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.

VII. PERFORMANCE EVALUATION

a. The number of actual participating nodes. These nodes include RFs and relay nodes that actually participate in routing. This metric demonstrates the ability of ALERT's randomized routing to avoid routing pattern detection.

b. The number of random-forwarders. This is the number of actual RFs in a S-D routing path. It shows routing anonymity and efficiency.

c. The number of remaining nodes in a destination zone. This is the number of original nodes remaining in a destination zone after a time period. A larger number provides higher anonymity protection to a destination and to counter the intersection attack. We measure this metric over time to show effectiveness on the destination anonymity protection.

d. The number of hops per packet. This is measured as the accumulated routing hop counts divided by the number of packets sent, which shows the efficiency of routing algorithms.

e. Latency per packet is the average time elapsed after a packet is sent and before it is received. It includes the time cost for routing and cryptography. This metric reflects the latency and efficiency of routing algorithms.

f. Delivery rate 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.

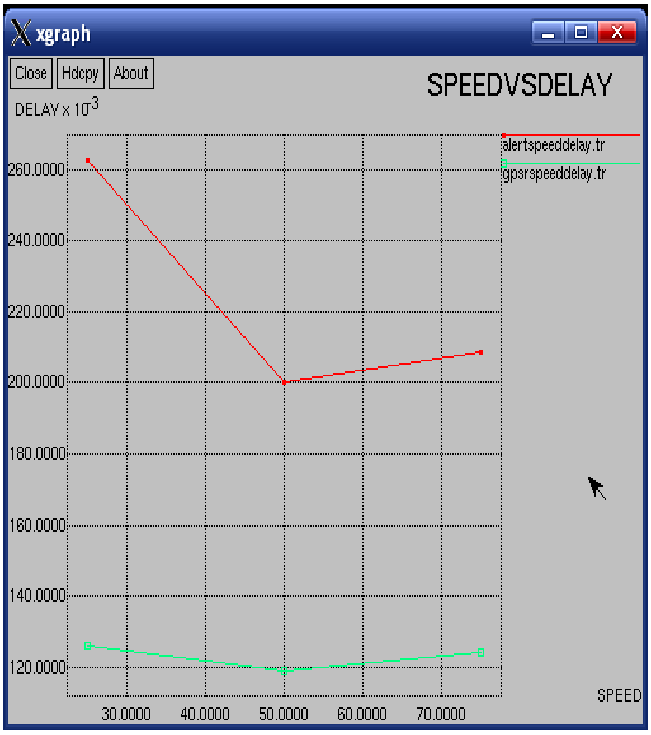


Figure.7 Speed versus Delay

In Fig.7 This graph shown comparison between the Speed and delay in the network with the GPSR and ALERT .While the Mobility Speed of the nodes increases in the network the routing process taken place in the network. The speed of the communicating nodes increase in the network the delay to reach the destination increases in the network. If the packet reaches the destination greater than particular time specified as threshold time that is considered as the delay. Due to the Mobility speed of the communicating node increases the location is changed accordingly so the delay increased in the network.

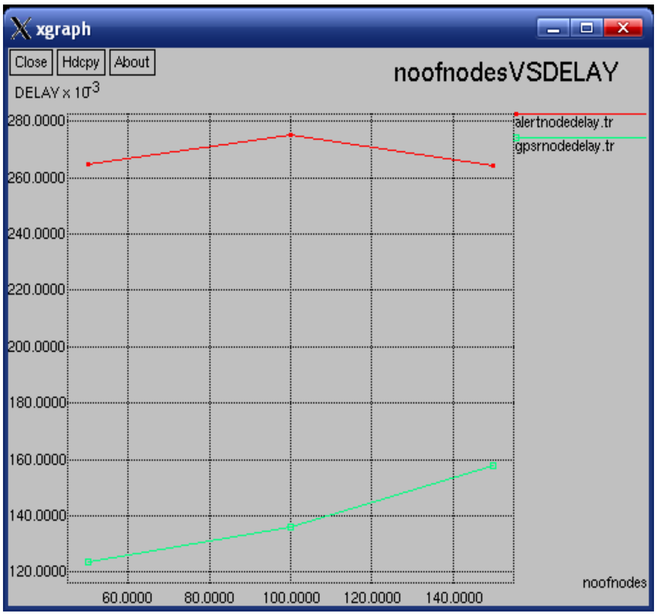


Figure. 8 Number of Nodes versus Delay

In Fig.8 This graph shown comparison between the Number of Nodes and delay in the network with the GPSR and ALERT. while the number of nodes increases in the network the routing process taken place in the network. The communicating nodes increase in the network the delay to reach the destination increases in the network. If the packet reaches the destination greater than particular time specified as threshold time that is considered as the delay. Due to the support features of selecting the Random forwarder and the anonymity property it will increase the delay.

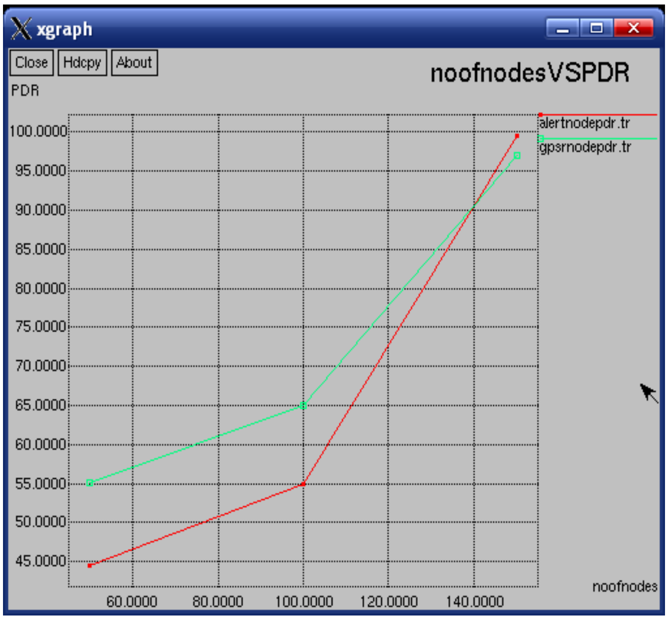


Figure. 9 Number of Nodes versus PDR

Fig. 9 This graph shown comparison between the Number of Nodes and PDR in the network with the GPSR and ALERT. while the number of nodes increases in the network the routing process taken place in the network. The communicating nodes increase in the network the packet delivery ratio of the destination increased in the network. The packets need to travel the more routing node and then it needs to reach the destination So the Packet delivery ratio in destination also increased.

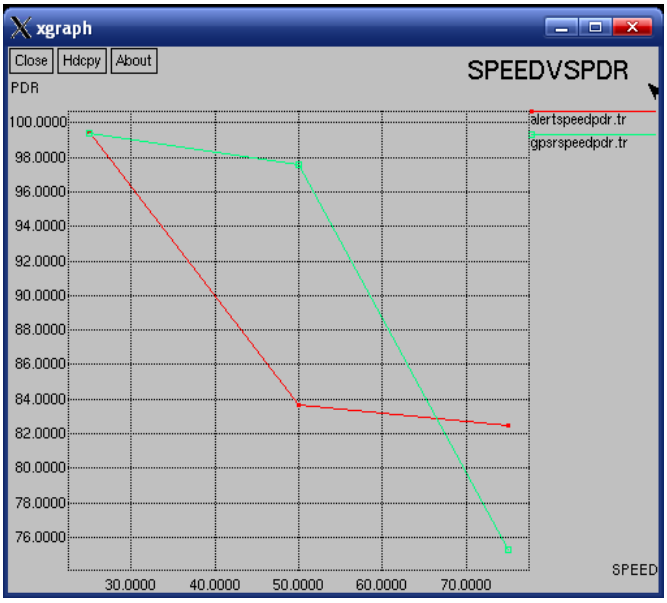


Figure. 10 Speed versus Delay

Fig.10 This graph shown comparison between the Speed and packet delivery ratio in the network with the GPSR and ALERT .While the Mobility Speed of nodes increases in the network the routing process taken place in the network. The speed of the communicating nodes increases in the network the packet delivery ratio reduced in the network Due to the Mobility speed of the communicating node increases the location is changed accordingly so the packet delivery ratio will be decreased.

VIII. CONCLUSION

In this paper, it is shown that ALERT is distinguished by its low cost and anonymity protection for sources, destinations and routes. It uses 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. A packet in ALERT includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/receivers. It has the “notify and go” mechanism for source anonymity, and uses local broadcasting for destination anonymity.

IX. REFERENCES

[1] Pfitzmann, M. Hansen, T. Dresden, and U. Kiel. Anonymity, unlinkability, unobservability, pseudonymity, and identity management consolidated proposal for terminology. Version 0.31. Technical report, 2005.

[2] R. Beresford and F. Stajano. Mix zones: User privacy in location-aware services. In Proc. of PERCOMW, 2004.

[3] K. El Defrawy and G. Tsudik. Alarm: Anonymous location-aided routing in suspicious manets. In Proc. of ICNP, 2007.

[4] H. Frey and I. Stojmenovic. On delivery guarantees of face and combined greedy-face routing in ad hoc and sensor networks. In Proc. of MobiCom, 2006.

[5] X. Hong, M. Gerla, G. Pei, and C.C. Chiang. A group mobility model for ad hoc wireless networks. In Proc. of MSWiM, 1999.

[6] Y.Zhang,W.Luo,” Anonymous communications in MobileAdhoc networks,”proc.IEEE INFOCOM,2007.

[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] L. Yang, M. Jakobsson, and S. Wetzel, “Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.

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

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

[11] Y. Xue, B. Li, and K. Nahrstedt, “A Scalable Location Management Scheme in Mobile Ad-Hoc Networks,” technical report, 2011.

[12] J. Li, J. Jannotti, D.S.J. De, C. David, R. Karger, and R. Morris, “A Scalable Location Service for Geographic Ad Hoc Routing,” Proc.ACM MobiCom, 2008.

[13] Teerawat Issariyakul, Ekram Hossain, “Introduction to Network Simulator NS2”, Springer, 2009.