International Conference on Innovative Trends in Electronics Communication and Applications 2015 [ICIECA 2015]

ISBN	978-81-929742-6-2		VOL	01
Website	icieca.in		eMail	icieca@asdf.res.in
Received	02 - April - 2015		Accepted	15 - November - 2015
Article ID	ICIECA021		eAID	ICIECA.2015.021

Location Based Routing Protocol in Manet Using Alert

R Gayathri[1]

[1]Assistant Professor, Department of Computer Science and Engineering,
Aalim Muhammed Salegh College of Engineering, Chennai, Tamilnadu, India

Abstract: *Mobile Ad Hoc Networks (MANETs) 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. I propose an Anonymous Location-based Efficient Routing proTocol (ALERT). For anonymity ALERT hides mainly source and destination identity using pseudonym which changes frequently. And ALERT also hide route between source and destination. With this ALERT also having stratergy against intersection attacks. I show that ALERT achieves better route anonymity protection and lower cost compared to other anonymous routing protocols. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol.*

Keywords*:* Mobile ad hoc netwI.

INTRODUCTION

Now a day's using mobile Ad-hoc Network, numerous wireless applications can be developed and these are used in much number of areas like mainly in military, education, commerce, entertainment.

MANET- MANET's basic features are self-organizing and independent infrastructure. All the nodes in the network are mobile and use wireless communications to communicate with other nodes. But as perspective of security of MANET, these networks get easily broken their security. Mainly data get lost or stolen by tampering and analyzing data and traffic analysis eavesdropping method or attacking routing protocol. For this security issue one solution is to use anonymous routing in the network that cannot be identified by any other nodes or attacker or observer. Although this anonymous routing is not required in general application .but it is very essentiial in Military, Banking like application, where security of communication is main purpose.

Anonymous routing provides secure communication between two nodes by hiding nodes original identity and prevents these nodes from traffic analysis attacks of adversaries.

In this paper the main task of anonymous routing is to hide identity and location of data sources (i.e sender, receipent) and route.so attacker cannot easily identify identity and location in network of nodes.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [9], [12], [2], [6], [1] and redundant traffic [11], [7], [4],[10], [14], [13], [3]. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM [6] cannot protect the location anonymity of source and destination, SDDR [16] cannot provide route anonymity, and ZAP [3] only focuses on destination anonymity. Many anonymity routing algorithms [3], [2], [3], [6], [1], [14], [10] are based on the geographic routing protocol (e.g.,

Cite this article as: R Gayathri. "Location Based Routing Protocol in Manet Using Alert". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 143-152. Print.

Greedy Perimeter Stateless Routing (GPSR) [17]) that greedily forwards a packet to the node closest to the destination. However, the protocol's strict relay node selection makes it easy to reveal the source and destination and to analyze traffic.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, I 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 [17] 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 [19] and timing attacks [19]. I theoretically analyzed ALERT in terms of anonymity and efficiency. I also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols.

Motivation and Contribution

The motivation of this paper is to ALERT can be used in different network models with node movement patterns. Such as random way point model and group mobility model. Generally ALERT provides unpredictable and dynamic routing path, which having no. of dynamically selected intermediate nodes.

1. First ALERT partitions given network area into two zones as horizontally (or vertically).

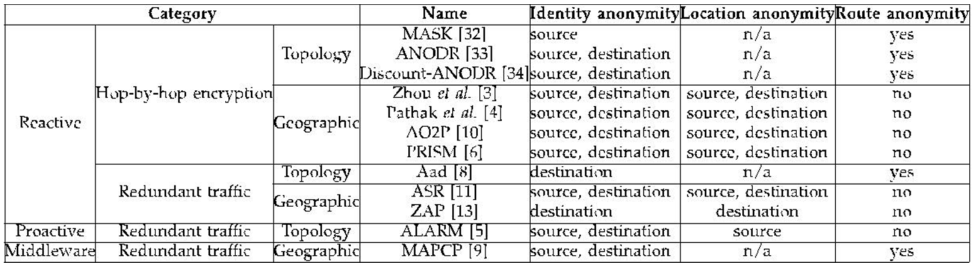
2. Then again split every partition into two zones as vertically (or horizontally). This process called as hierarchical zone partition.

3. After partitioning ALERT randomly select a node in each zone at each step as an intermediate relay node ,in this way ALERT provide dynamically creating an unpredictable routing path

Related Work

Anonymous routing schemes in MANETs have been studied in recent years. By the different usage of topological information, they can be classified into on-demand or reactive routing methods [7], [15], [8], [11], [12], [2], [14], [10], [3], and proactive routing methods [5]. Also there are anonymous middleware working between network layer and application layer [4]. Since topology routing does not need the node location information, location anonymity protection is not necessary.

TABLE 1: Summary of Existing Anonymous Routing Protocols



Category			Name	Identity anonymity	Location anonymity	Route anonymity
Reactive	Hop-by-hop encryption	Topology	MASK [32]	source	n/a	yes
			ANODR [33]	source, destination	n/a	yes
			Discount-ANODR [34]	source, destination	n/a	yes
		Geographic	Zhou *et al.* [3]	source, destination	source, destination	no
			Pathak *et al.* [4]	source, destination	source, destination	no
			AO2P [10]	source, destination	source, destination	no
			PRISM [6]	source, destination	source, destination	no
	Redundant traffic	Topology	Aad [8]	destination	n/a	yes
		Geographic	ASR [11]	source, destination	source, destination	no
			ZAP [13]	destination	destination	no
Proactive	Redundant traffic	Topology	ALARM [5]	source, destination	source	no
Middleware	Redundant traffic	Geographic	MAPCP [9]	source, destination	n/a	yes

HELPFUL HINTS

Figures and Tables

Table 1 shows the classification of the methods along with their anonymity protection. To clearly show the featured anonymity protection in different reactive routing methods, the table provides a finer classification of different anonymity methods, including hop-by-hop encryption [7], [15], [8], [11], [12], [11], [14], [10] ,and redundant traffic routing [7], [14], [3].

In hop-by-hop encryption routing, a packet is encrypted in the transmission of two nodes en route, preventing adversaries from tampering or analyzing the packet contents to interrupt the communication or identify of the two communicating nodes. Hop-by-hop encryption routing can be further divided into onion routing and hop-by-hop authentication. In onion routing, packets are encrypted in the source node and decrypted layer by layer (i.e., hop by hop) along the routing path. It is used in Aad [7], ANODR [15] and Discount-ANODR [8] topological routing. Aad [7] combines onion routing, multicast, and uses packet coding policies to constantly change the packets in order to reinforce both destination and route anonymity. The onion used in ANODR [15] is called trapdoor boomerang onion (TBO), which uses a trapdoor function instead of public key-based encryption. ANODR needs onion construction in both route discovery and return routing, generating high cost. To deal with this problem, the authors further proposed Discount-ANODR that constructs onions only on the return routes

ALARM [6] uses proactive routing, where each node broadcasts its location information to its authenticated neighbours 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. Different from all other studied methods. MAPCP [4] is a middleware between network and application layers, in which every hop in the routing path executes probabilistic broadcasting that chooses a number of its neighbours with a certain probability to forward messages.

Mix zones [13] and GLS [20] are zone-based location services. Mix zones are an anonymous location service that unveils the positions of mobile users in a long time period in order to prevent users' movement from being tracked. Each location aware application that can monitor nodes' locations on top of Mix zones is only allowed to monitor the nodes that are registered to it. Therefore, by letting each node associate with some zones but stay unregistered, these users' location changes are untraceable in unregistered zones. Although GLS also uses hierarchical zone partition-ing, its use is for location service while in ALERT, its use is for anonymous routing. ALERT is also different from GLS in the zone division scheme. A zone in ALERT is always divided into two smaller rectangles, while GLS divides the entire square area into four sub squares and then recursively divides these into smaller squares. The zone division in ALERT occurs when selecting a next forwarding node, so the zones are formed dynamically as a message is being forwarded. In contrast, the zone division and hierarchies in GLS are configured in advance and the location servers are selected based on the different hierarchies

Organization

The rest of this paper is organized as follows. I introduce the preliminary work in Section II. I give the formal model of ALERT in Section III. An efficient ALERT scheme is proposed in Section IV. I analyse the proposed scheme in Section V. Finally, the conclusions are given in Section VI.

PRELIMINARIES

For ease of illustration, I assume the entire network area is generally 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.

ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically deter-mined intermediate relay nodes.

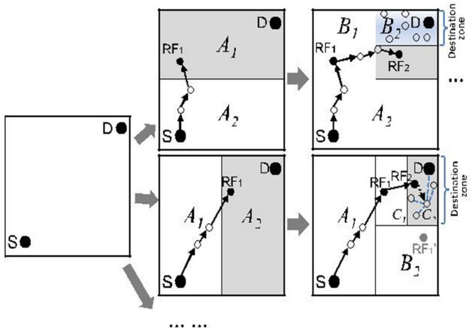


Fig. 1. Examples of different zone partitions.

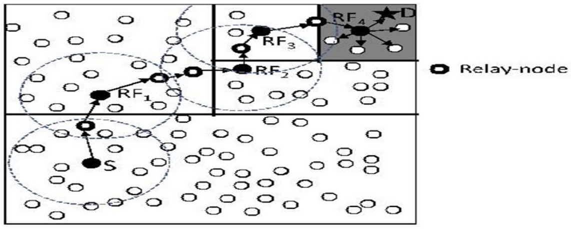
As shown in the upper part of Fig. 1, given an area, I horizontally partition it into two zones A_1 and A_2. I then vertically partition zone A_1 to B_1 and B_2. After that, I horizontally partition zone B_2 into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. I 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.

Fig. 2 shows an example of routing in ALERT. I call the zone having k nodes where D resides the destination zone, denoted as Z_D. k is used to control the degree of anonymity protection for the destination. The shaded zone in Fig. 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 it until it and Z_D are not in the same zone

Cite this article as: R Gayathri. "Location Based Routing Protocol in Manet Using Alert". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 143-152. Print.

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. This node is defined as a random forwarder (RF). Fig. 3 shows an example where node N_3 is the closest to TD, so it is selected as a RF. ALERT aims at achieving k-anonymity [18] for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in Z_D, providing k-anonymity to the destination.

Fig. 2. Routing among zones in ALERT



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. Fig. 1 shows two possible routing paths for a packet pkt issued by sender S targeting destination D in ALERT. There are also many other possible paths. In the upper routing flow, data source S first horizontally divides the area into two equal-size zones, A_1 and A_2, in order to separate S and Z_D. S then randomly selects the first temporary destination TD_1 in zone A_1 where Z_D resides. Then, S relies on GPSR to send pkt to TD_1. The pkt is forwarded by several relays until reaching a node that cannot find a neighbor closer to TD_1. This node is considered to be the first random-forwarder RF $_1$. After RF $_1$ receives pkt, it vertically divides the region A_1 into regions B_1 and B_2 so that Z_D and it are separated in two different zones. Then, RF $_1$ randomly selects the next temporary destination TD_2 and uses GPSR to send pkt to TD_2. This process is repeated until a packet receiver finds itself residing in Z_D, i.e., a partitioned zone is Z_D having k nodes. Then, the node broadcasts the pkt to the k nodes.

The lower part of Fig. 1 shows another routing path based on a different partition pattern. After S vertically partitions the whole area to separate itself from Z_D, it randomly chooses TD_1 and sends pkt to RF $_1$. RF $_1$ partitions zone A_2 into B_1 and B_2 horizontally and then partitions B_1 into C_1 and C_2 vertically, so that itself and Z_D are separated. Note that RF $_1$ could vertically partition A_2 to separate itself from Z_D 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.

FORMAL MODEL OF ALERT

In this section, I give the formal Algorithm and Routing method of ALERT.

Pseudonym and Location of Node: Dynamic pseudonym is another name or identity given to node. In ALERT pseudonym used as node identifier with replacement of its real MAC address. Nodes MAC addresses can be used to trace nodes existence in the network. Therefore replacing MAC address with pseudonym is the main advantage of ALERT protocol. This pseudonym is the combination of MAC address and Current time stamp. But if this information is known by attacker then it is easily find out the node. Therefore, to prevent this time stamp can be randomly selected. This pseudonym is not permanent; it expires after a specific time period so that attacker cannot associate the pseudonym with nodes. With this pseudonym there is one problem is changing pseudonym frequently create routing uneasy. Therefore these pseudonym changes frequently should be appropriately determined.

The ALERT Routing: Generally ALERT provides unpredictable and dynamic routing path,which having no.of dynamically selected intermediate nodes.

1. First ALERT partitions given network area into two zones as horizontally (or vertically).
2. Then again split every partition into two zones as vertically (or horizontally). This process called as hierarchical zone partition.
3. After partitioning ALERT randomly select a node in each zone at each step as an intermediate relay node ,in this way ALERT provide dynamically creating an unpredictable routing path.

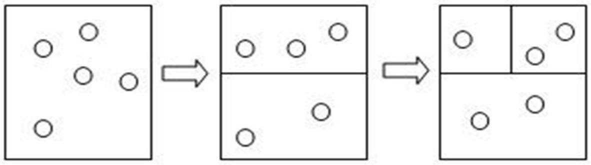


Fig. 1 Horizontal Partitioning

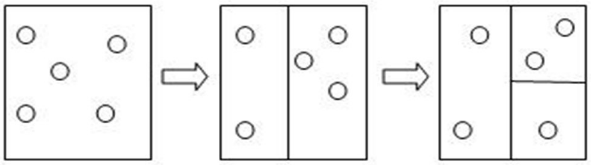
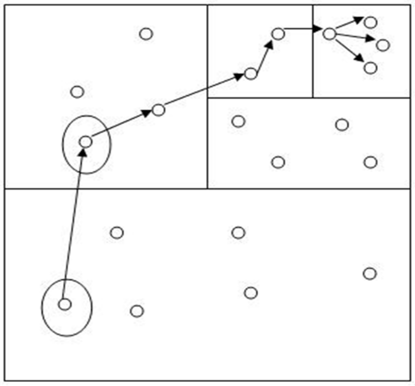


Fig. 2 Vertical Partitioning

Above fig. shows both partitioning, here we generally network considered in rectangle form. In this rectangle circle consider as nodes. Consider one example of routing in ALERT .Following fig shows this

Fig 3. Zonal Routing of Nodes



In this example I first horizontally partition network then vertically and so on. While this partitioning each data source of forwarder node checks whether itself and destination nodes are not in same zone. If it is not then partitioning continues. In above fig where the destination node locates that zone is called as destination zone denoted as ZD and that zone having k nodes, which is used to control the degree of anonymity.

While in routing first source node randomly chooses a node in other zone known as temporary destination (TD) and then uses GPSR routing algorithm to send the data to node close to TD. This process continues to reach data to destination node. A node closer to TD known as Random Forwarder (RF) .But in destination zone data is broadcasted in ZD to k nodes which provides k anonymity i.e attacker or observer does not known at destination node.

Here one assumption is taken that destination node with not leave the destination zone during the data transmission to it. So it can successfully receive the full data without any loss. For successful completion of data transmission destination node send a confirmation to source node. If source node not receives to confirm during predefined time period, it will resend packets. As a large no. of hierarchies generated they create more routing hops which increases anonymity degree but also increase the delay.

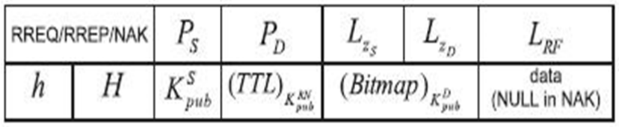
Location of Destination Zone: Zone position is made from the upper left and bottom right coordinates of a zone. It is used by each packet forwarder to check whether it is separated from destination zone or not, To calculate zone position we have H denotes total no. of partitions in order to produce ZD and no .of nodes i.e k and node density ρ ,

$H = \log2(\rho.G/k)$ eq(1)

Cite this article as: R Gayathri. “Location Based Routing Protocol in Manet Using Alert”. *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 143-152. Print.

Where as G=size of entire network area Using H and G the position (0,0) & (Xg , Yg) of entire network area and position of destination node d the source can calculate the zone position of ZD.

Packet Format: For successful routing between source and destination some information is needed, which is embeds in the packet by source and each packet forwarder node. For ALERT following packet format is use.



RREQ/RREP/NAK		P_S	P_D	L_{z_S}	L_{z_D}	L_{RF}
h	H	K^S_{pub}	$(TTL)_{K^{KN}_{pub}}$	$(Bitmap)_{K^D_{pub}}$		data (NULL in NAK)

Fig.4 ALERT Packet Format

RREQ/RREP/NAK- use to acknowledge the loss of packet.

P_s- Pseudonym of a source.

P_d – pseudonym of a destination.

Lzs & Lzd – are the position of Hth partitioned source zone and destination zone.

h- Number of divisions.

H – Maximum number of division allowed.

In this paper, I use two different network models, random way point model [17] and group mobility model [18]. With the random way point model as the default setting, I also compare the performance of ALERT in the group mobility model. In the group mobility model, we set the movement range of each group to 150 m with 10 groups [6] and to 200 m with five groups.

Anonymity Protection: The main goal of ALERT is to provide identity and location anonymity of source and destination in MANET. For this ALERT dynamically and randomly chooses relay node for forming route between source and destination. So due to this intruder cannot observe a stastical pattern of transmission. Anonymous path between source and destination ensures that a node on the path does not know where the endpoints are. Unlinkability is major strength of privacy protection i.e source and destination cannot be associated with the packets in their communication by adversaries.

Strategy against Intersection Attacks: Intersection attack, in which an attacker can determine communicating nodes using observation of routing between them and collecting information about them Active Users To counter intersection attack ALERT proposes a strategy. In this it broadcasted the packets in destination zone ZD. So that attacker confuse who is destination .This broadcasting is done in two steps. In first step packet is broadcasted but not reach to destination node. In second step nodes who receive the packets then forward packets to remaining node who yet not receive in this destination node is present so it receive the packet. In this situation attacker get confused and can't concentrate in their observation

ANALYSIS OF THE SCHEME

In this section, I theoretically analyze the anonymity and routing efficiency properties of ALERT. I analyze the number of nodes that can participate in routing that function as camouflages for routing nodes. I estimate the number of RFs in a routing path, which shows the route anonymity degree and routing efficiency of ALERT. I calculate the anonymity protection degree of a destination zone as time passes to demonstrate ALERT's ability to counter intersection attacks. In this section, I also use figures to show the analytical results to clearly demonstrate the relationship between these factors and the anonymity protection degree

Security

In this analysis scenario, I assume that the entire network area is a rectangle with side lengths l_A and l_B and the entire area is partitioned H times to produce a k-anonymity destination zone. For the parameters of results in the figures, unless otherwise indicated, the size of the entire network zone is 1000 mX1000 m and the number of nodes equals 200. I set H = 5 to ensure that a reasonable number of nodes are in a destination zone.

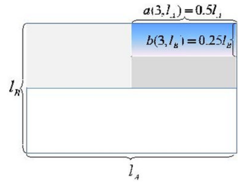


Fig. 5. The side lengths of the 3rd partitioned zone.

I first introduce two functions to calculate the two side lengths of the hth partitioned zone:

$a(h,I_A)=1_A/2^{(h/2)'}$ eq(2)

$b(h,I_B)=I_B/22^{[h/2]}$ eq(3)

The side lengths of the destination zone after H partitions are $a(h,I_A)$and $b(h,I_B)$. Fig. shows an example of three partitions of the entire network area. The side lengths of the final zone after the three partitions are

$a(3,I_A)=1_A/2^{[3/2]'}=0.5I_A$ eq(4)

and

$b(3, I_B)= I_B /2^{[3/2]})'=0.25I_B$ eq(5)

The Number of Possible Participating Nodes: The intention of his analysis is to characterize how many possible nodes are able o participate in one S-D routing. The number of these nodes shows how many nodes can become camouflages in a routing path. These possible participating nodes include RFs and the relay nodes between two RFs using GPSR. The nodes that actually conduct the routing are not easily discovered among the many possible participating nodes, thus making the routing pattern undetectable. Because the positions of both S and D affect the number of possible participating nodes in routing, the positions influence routing anonymity. I first calculate the probability that partitions are needed to separate S and D denoted as $p_s(\sigma)$-1. I use to denote the closeness between S and D. $p_s(\sigma)$ actually is the probability that D is located in a position that can be separated from a given S using σ partitions. I can get

$p_s(\sigma) = 1/2\ \sigma \quad 0< \sigma<=H$ eq(6)

I use $Ne(\sigma)$ to denote the expected number of nodes that possibly take part in routing based on a given closeness

$Ne(\sigma) = a(\sigma,I_A)_{,}b(\sigma,I_B)$ eq(7)

where p denotes the density of nodes. By considering different closeness σ I arrive at the final expected number of possible participating nodes from a S to any D:

$Ne =\Sigma^H{}_{\sigma=1} Ne(\sigma)\ p_s(\sigma)= \Sigma^H{}_{\sigma=1} a(\sigma,I_A)_{,}b(\sigma,I_B)\ p\ \ 1/2^{\sigma}$ eq(8)

I set the total number of nodes in the network to 100, 200, and 400, respectively, and use (5) to calculate the number of possible participating nodes.

The Number of Random-Forwarders: The number of RFs determines the length of the routing path in ALERT. Therefore, it reflects the energy efficiency and degree of anonymity of ALERT. From the anonymity view, for a network with a fixed number of nodes, more RFs offer higher anonymity but will reduce the number of nodes in the destination zone, and consequently reduce the anonymity protection of destination node. Therefore, the number of RFs should be carefully determined to ensure a sufficient number of nodes located in the destination zone. For a pair of S-D with closeness σ, we define $p_i(\sigma ,i)$ as the probability that an S-D routing path has i RFs. The number of RFs is determined by the zone partition pattern.

Destination Anonymity Protection: Destination anonymity is determined by the number of nodes in the destination zone, which is related to node density and the size of the destination zone. According to the work in [13], the probability that a node with a moving speed *v* remains in the destination zone, which is a circular area with radius r, after time period t, denoted by $p_r(t)$, is exponentially distributed:

Where $p_r(t) = e^{-t/\beta(r)}$ eq(9)

$\beta(r) = \Pi r/2v$ eq(10)

Cite this article as: R Gayathri. "Location Based Routing Protocol in Manet Using Alert". *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 143-152. Print.

In order to apply (9) and (10) to my method, I assume the Hth partitioned destination zone is a square that can be approximated by a circle covering approximately (see fig:6) the same area. This assumption is feasible, which only requires a square for the entire network area (i.e., $l_A = l_B$) and an even number of partitions (i.e., $a(H, l_A)= b(H, l_A)$). I use 2r' to denote the side length of the destination zone. Hence, we can calculate the radius of this approximate circle as below:

$$\Pi r2 = (2r')2 \rightarrow r = 2r' / \sqrt{\Pi} \qquad \text{eq(11)}$$

For ALERT to be usable, I need to ensure that the pseudonym and location exchange cost is low compared with regular communication messages. Let N, N_L, f, F, and T denote the total number of nodes, the number of location servers, the frequency of pseudonym, and location updates and the frequency of regular communication messages, respectively. The number of messages exchanged between location servers within time T is N_L x (N_{L-}1) x f x T, the number of messages for pseudonym updates is N x f x T. The number of communication messages in the network is N x F x T. Therefore, if the location servers incur only a small fraction of messages, we need to make sure that N_L x (N_L-1) x f x T/ N x F x T <<1.Regular communication frequency should be much higher than update exchange messages. thus ,f << F, so that N x f x T./ N x F x T <<1.Therefore

$$\frac{N_L \text{ x } (N_L-1) \text{ x } f \text{ x } T + N \text{ x } F \text{ x } T << 1}{N \text{ x } F \text{ x } T}$$

$$\frac{N_L \text{ x } (N_L-1) \text{ x } f \text{ x } T << 1}{N \text{ x } F \text{ x } T}$$

$$\frac{N_L \text{ x } (N_L-1) \text{ x } f \quad << 1}{N \text{ x } F}$$

which can be satisfied if N_L is comparable to $\sqrt{}$N. This is reasonable when the transmission range of nodes is modest so that only a small number of location servers are needed.

Performance

In this section, I provide experimental evaluation of the ALERT protocol, which exhibit consistency with my analytical results. Both prove the superior performance of ALERT in providing anonymity with low cost of overhead. Recall that anonymous routing protocols can be classified into hop-by-hop encryption and redundant traffic. I compare ALERT with two recently proposed anonymous geographic routing protocols: AO2P [10] and ALARM [6], which are based on hop-by-hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare ALERT with the baseline routing protocol GPSR [1] in the experiments. In GPSR, a packet is always forwarded to the node nearest to the destination. When such a node does not exist, GPSR uses perimeter forwarding to find the hop that is the closest to the destination. In ALARM, each node periodically disseminates its own identity to its authenticated neighbors and continuously collects all other nodes' identities. Thus, nodes can build a secure map of other nodes for geographical routing. In routing, each node encrypts the packet by its key which is verified by the next hop en route. Such dissemination period was set to 30s in this experiment. The routing of AO2P is similar to GPSR except it has a contention phase in which the neighboring nodes of the current packet holder will contend to be the next hop. This contention phase is to classify nodes based on their distance from the destination node, and select a node in the class that is closest to destination. Contention can make the ad hoc channel accessible to a smaller number of nodes in order to decrease the possibility that adversaries participate, but concurrently this leads to an extra delay. Also, AO2P selects a position on the line connecting the source and destination that is further to the source node than the destination to provide destination anonymity, which may lead to long path length with higher routing cost than GPSR

Simulation

In this section I discuss about the simulation of network model.

The tests were carried out on NS-2.29 simulator using 802.11 as the MAC protocol with a standard wireless transmission range of 250 m and UDP/CBR traffic [21] with a packet size of 512 bytes. The test field in our experiment was set to a 1000 m x 1000 m area with 200 nodes moving at a speed of 2 m/s, unless otherwise specified. The density was set to 50, 100, 150, and 200 nodes per square meters. The duration of each simulation was set to 100 s unless otherwise indicated. The number of pairs of S-D communication nodes was set to 10 and S-D pairs are randomly generated. S sends a packet to D at an interval of 2 s. The final results are the average of results of 30 runs. The confidence interval can be thus calculated from different runs and are shown when necessary. The confidence interval information is drawn along with the average point (in a "I" shape) on those figures.

For encryption, the symmetric encryption algorithm is AES and the public key encryption is RSA. Data are generated randomly according to the packet size specified in the paper. Packets are encrypted whenever needed. The encryption algorithm is single threaded, running along with other parts of the experiment on a 1.8 Ghz processor. A typical symmetric encryption costs several milliseconds while a public key encryption operation costs 2-3 hundred milliseconds.

I use the following metrics to evaluate the routing performance in terms of effectiveness on anonymity protection and efficiency:

1. **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.
2. **The number of random forwarders**. This is the number of actual RFs in a S-D routing path. It shows routing anonymity and efficiency.
3. **The number of remaining nodes in a destination Zone***: T*his 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.
4. **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.
5. **Latency per packet**. This 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.
6. **Delivery rate**. This 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.

In this Paper, I conclude that Existing anonymous routing protocols, depend on either hop- by-hop encryption or redundant traffic which generate high cost. And some protocols are not provide complete source, destination, and route anonymity protection. 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. ALERT further strengthens the anonymity protection of source and destination by hiding the data initiator/receiver among a number of data initiators/ receivers. In addition, ALERT has an efficient solution to counter intersection attacks. It can also achieve comparable routing efficiency to the base-line GPSR algorithm. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. Future work lies in reinforcing ALERT in an attempt to thwart stronger, active attackers and demonstrating comprehensive theoretical and simulation results.

References

[1] K.E. Defrawy and G. Tsudik, "PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs)," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2008

[2] 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

[3] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct. 2008.

[4] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applica-tions over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[5] 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

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

[7] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Secure comm and Workshops, 2006

[8] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc

Secure communications and Workshops, 2006

[9] Sk.Md.M.Rahman,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

[10] X. Wu, “AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol,” IEEE Trans. Mobile Computing, vol. 4, no.4, 335-348, July/Aug. 2005.

[11] 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.

[12] Z. Zhi and Y.K. Choong, “Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy,” Proc. Third Int’l Work-shop Mobile Distributed Computing (ICDCSW), 2005.

[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] 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

[15] 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

[16] 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.

[17] 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

[18] L. Sweeney, “k-Anonymity: A Model for Protecting Privacy,” Int’l J. Uncertainity Fuzziness Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002

[19] J. Raymond, “Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems,” Proc. Int’l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobserva-bility (WDIAU), pp. 10-29, 2001

[20] 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, 2000

[21] The Network Simulator - ns-2,” http://www.isi.edu/nsnam/ns

Cite this article as: R Gayathri. “Location Based Routing Protocol in Manet Using Alert”. *International Conference on Innovative Trends in Electronics Communication and Applications (2015)*: 143-152. Print.