Efficient Routing Mechanism for Location Anonymity in MANETs

Padmini. V. K[1],Shamanth.V[2],Jimooth[3],Dhanush. D[4]
[1]Student, Dept. of CSE,APSCE,padminiroysom@gmail.com
[2]Student,Dept. of CSE,APSCE,shamnth23@gmail.com
[3]Student,Dept. of CSE,APSCE, jimooth@yahoo.in
[4]Student,Dept. of CSE,APSCEdhanushdkrishna@gmail.com
Bangalore, India

Prof. C. P. SAMEERANA
HOD, Dept. Of CSE
APSCE
Bangalore, India
hodcse.apsce@gmail.com

***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, we propose an Efficient Routing Mechanism For Location Anonymity in MANETs(ERMFLAIM). ERMFLAIM dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, ERMFLAIM offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively counter intersection and timing attacks.**

Keywords*— Mobile ad hoc networks, anonymity, routing protocol)

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) can be used in a wide number of wireless applications areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Anonymous routing protocols 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 where location devices may be equipped.

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [1] [2] [3] and redundant traffic [4] [5] [6]. 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, Anonymous Location-Aided Routing in Suspicious MANETS (ALARM) cannot protect the location anonymity of source and destination, Secure Dynamic Distributed Routing Algorithm for Ad Hoc Wireless Networks(SDDR) cannot provide route anonymity, Zone-based Anonymous Positioning routing(ZAP) only focuses on destination anonymity and An Anonymous Location-Based Efficient Routing Protocol in MANETs(ALERT) [7] provides anonymity but inefficient routing algorithm is used.

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. 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.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Efficient Routing Mechanism For Location Anonymity in

MANETs (ERMFLAIM). ERMFLAIM dynamically partitions a net-work field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. Specifically, in each routing step, a data sender or forwarder partitions the network field in order to separate itself and the destination into two zones. It then randomly chooses a node in the other zone as the next relay node and uses the AODV algorithm to send the data to the relay node. In addition, ERMFLAIM has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ERMFLAIM is also resilient to intersection attacks and timing attacks.

In summary :

1. *Anonymous routing.*
2. *Low cost.*
3. *Resilience to intersection attacks and timing attacks.*

The remainder of this paper is organized as follows : In Section II, we describe related anonymous routing approaches in MANETs. In Section III, we present the design of the ERMFLAIM routing protocol. Section IV discusses the anonymity performance of ERMFLAIM and its strategies to deal with certain attacks. The conclusion and future work are given in Section V.

II. 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 and proactive routing methods. Since topology routing does not need the node location information, location anonymity protection is not necessary. 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 and redundant traffic routing.

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 , ANODR[8] and Discount-ANODR topological routing[9]. Aad 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 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.

Hop-by-hop authentication is used to prevent adversaries from participating in the routing to ensure route

Category			Name	Identity anonymity	Location anonymity	Route anonymity
Reactive	Hop-by-hop encryption	Topology	ANODR	source, destination	n/a	yes
			Discount-ANODR	source, destination	n/a	yes
		Geographic	Zhou *et al.*	source, destination	source, destination	no
			AO2P	source, destination	source, destination	no
	Redundant traffic	Topology	Aad	destination	n/a	yes
		Geographic	ZAP	destination	destination	no
Proactive	Redundant traffic	Topology	ALARM	source, destination	source	no

Fig. 1. Summary of existing anonymous routing protocols.

anonymity . The works in are based on geographic routing. In GSPR [3], nodes encrypt their location updates and send location updates to the location server. However, GSPR does not provide route anonymity because packets always follow the shortest paths using geographic routing, and the route can be detected by adversaries in a long communication session. Since AO2P does not provide anonymity protection to destinations, the authors further improve it by avoiding the use of destination in deciding the classification of nodes. The improved AO2P selects a position on the line connecting the source and destination that is further to the source node than the destination and replaces the real destination with this position for distance calculation. However, all of these hop-by-hop encryption methods generate high cost due to the use of hop-by-hop public-key cryptography or complex symmetric key cryptography.

Redundant traffic-based routing uses redundant traffic, such as multicast, local broadcasting, and flooding, to obscure potential attackers. Multicast is used in the Aad topological routing algorithm to construct a multicast tree or forest to hide the destination node.ZAP uses a destination zone, and locally broadcasts to a destination zone in order to reach the destination without leaking the destination identity or position. A disadvantage of redundant traffic-based methods is the very high overhead incurred by the redundant operations or packets, leading to high cost. ALARM uses proactive routing, where each node broadcasts its location information to its authenticated neighbors so that each node can build a map for later anonymous route discovery.

III. ERMFLAIM : EFFICIENT ROUTING MECHANISM FOR LOCATION ANONYMITY IN MANETS.

A. *Networks and Attack Models and Assumptions*

Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide untraceability, is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable. A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity.

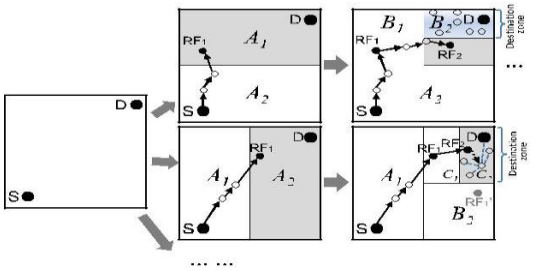


Fig. 2. Examples of different zone partitions.

In this work, the attackers can be battery powered nodes that passively receive network packets and detect activities in their vicinity. They can also be powerful nodes that pretend to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets. The assumptions below apply to both inside and outside attackers.

1. *Capabilities of the Adversary*. By eavesdropping, the adversary nodes can analyze any routing protocol and obtain in-formation about the communication packets in their vicinity and positions of other nodes in the network. They can also monitor data transmission on the fly when a node is communicating with other nodes and record the historical communication of nodes. They can intrude on some specific vulnerable nodes to control their behavior.
2. *Incapabilities of the Adversary*. The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public / private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

B. The ERMFLAIM Routing Algorithm

For ease of illustration, we 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 ERMFLAIM.

ERMFLAIM features a dynamic and unpredictable routing path, which consists of a number of dynamically deter-mined intermediate relay nodes. As shown in the upper part of Fig. 1, given an area, we horizontally partition it into two zones A_1 and A_2. We then vertically partition zone A_1 to B_1 and B_2. After that, we horizontally partition zone B_2 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. ERMFLAIM 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 ERMFLAIM. We 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 ERMFLAIM routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and ZD are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the AODV 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 N3 is the closest to TD, so it is selected as a RF . ERMFLAIM aims at achieving k-anonymity for destination node D, where k is a predefined integer. Thus, in the last step, the data are broadcasted to k nodes in ZD , providing k-anonymity to the destination.

Given an S-D pair, the partition pattern in ERMFLAIM 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 ERMFLAIM. 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 ZD. S then randomly selects the first temporary destination TD_1 in zone A_1 where ZD resides. Then, S relies on AODV 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 A1 into regions B_1 and B_2 so that ZD and itself are separated in two different zones. Then, RF_1 randomly selects the next temporary destination TD_2 and uses AODV to send pkt to TD_2. This process is repeated until a packet receiver finds itself residing in ZD , i.e., a partitioned zone is ZD having k nodes. Then, the node broadcasts the pkt to the k nodes.

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 ZD , 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 B1 into C_1 and C_2 vertically, so that itself and ZD are separated. Note that RF_1 could vertically partition A_2 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, ERMFLAIM sets the partition in the alternative horizontal and vertical manner in order to ensure that a pkt approaches D in each step.

As AODV, 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.

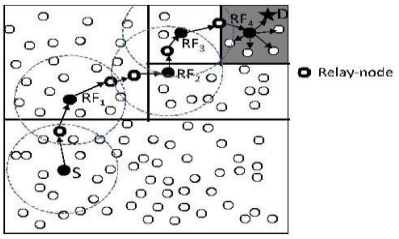


Fig. 3. Routing among zones in ALERT.

C. Anonymity of Source Node

ERMFLAIM contributes to the achievement of anonymity by restricting a node's view only to its neighbors and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source or a forwarding node. To strengthen the anonymity protection of the source nodes, we further propose a lightweight mechanism called "notify and go." Its basic idea is to let a number of nodes send out packets at the same time as S in order to hide the source packet among many other packets.

"Notify and go" has two phases: "notify" and "go." In the first "notify" phase, S piggybacks its data transmission notification with periodical update packets to notify its neighbors that it will send out a packet. The packet includes two random back-off time periods, t and t0. In the "go" phase, S and its neighbors wait for a certain period of randomly chosen time *2t ; tt0* before sending out messages. S's neighbors generate only several bytes of random data just in order to cover the traffic of the source. t should be a small value that does not affect the transmission latency. A long t0 may lead to a long transmission delay while a short t0 may result in interference due to many packets being sent out simultaneously. Thus, t0 should be long enough to minimize interference and balance out the delay between S and S's farthest neighbor in order to prevent any intruder from discriminating S. This camouflage augments the privacy protection for S by -anonymity where is the number of its neighbors. Therefore, it is difficult for an attacker to analyze traffic to discover S even if it receives the first notification.

ERMFLAIM utilizes a TTL field in each packet to prevent the packets issued in the first phase from being forwarded in order to reduce excessive traffic. Only the packets of S are assigned a valid TTL, while the covering packets only have a TTL. After S decides the next TD, it forwards the packet to the next relay node, which is its neighbor based on AODV. To prevent the covering packets from being differentiated from the ones sent by S, S encrypts the TTL field using obtained from the periodical "hello" packets between neighbors. Every node that receives a packet but cannot find a valid TTL will try to decrypt the TTL using its own private key. Therefore, only NRN will be able to success-fully decrypt it, while other nodes will drop such a packet.

D. The Dead End Problem.

Dead end is one common problem in the geographic routing in which each node is aware of the positions of its neighbors in order to forward a packet to the neighbor nearest to the destination. A dead end occurs when a packet is forwarded to a node whose neighbors are all further away from the destination than itself and then the packet is routed between neighbors iteratively.

ERMFLAIM can incorporate existing solutions, such as face routing, to avoid the dead-end problem without

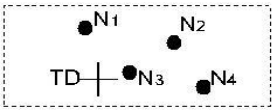


Fig 4.Choosing RF according to a given TD.

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

IV. ANONYMITY PROTECTION AND STRATEGIES AGAINST ATTACKS

A. Anonymity Protection

ERMFLAIM offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing , which always takes the shortest path, ERMFLAIM 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. ERMFLAIM 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.

ERMFLAIM incorporates the "notify and go" mechanism to prevent an intruder from identifying which node within the source neighborhood has initiated packets. Thus, an eaves-dropper can only obtain information on Z_D , rather than the destination position, from the packets and nodes en route.

The route anonymity due to random relay node selection in ERMFLAIM prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ERMFLAIM, 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 ERMFLAIM 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 ERMFLAIM.

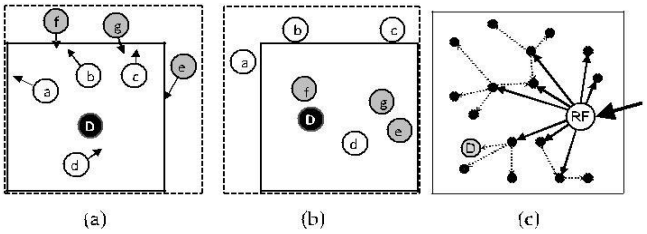


Fig. 5. Intersection attack and solution.

B. Timing Attacks

In timing attacks , 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. Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In ERMFLAIM, the notify and go mechanism 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.

C. Counter Intersection Attacks

In an intersection attack, 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 ERMFLAIM 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 Z_D 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. 5a is the status of a Z_D 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 Z_D . Fig. 5b 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 Z_D . 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.

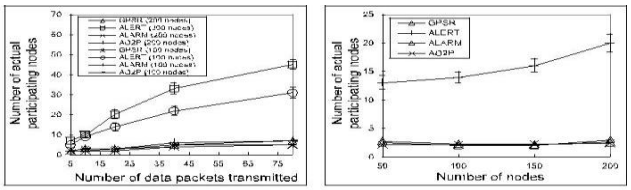
To counter the intersection attack, ZAP dynamically enlarges the range of anonymous zones to broadcast the messages or minimizes communication session time. However, the former strategy increases the communication overhead, while the latter may not be suitable for long-duration communication. Instead of adopting such a mitigating mechanism, we propose another strategy to resolve this problem. Note that 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 Z_D constantly in long-duration sessions rather than using direct local broadcasting in the zone, the last RF multicasts packet pkt_1 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 pkt_2. 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. 5c 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 Z_D in the transmission session, thus foiling the intersection attack.

V. PERFORMANCE EVALUATION

In this section, we provide an experimental evaluation of the ERMFLAIM protocol, which exhibit consistency with our analytical results. Both prove the superior performance of ERMFLAIM in providing anonymity with low cost. Recall that anonymous routing protocols can be classified into hop-by-hop encryption and redundant traffic. We compare ERMFLAIM with two recently proposed anonymous geographic routing protocols, AO2P [29] and ALARM [13], which are based on hop-by-hop encryption and redundant traffic, respectively. All of the protocols are geographic routing, so we also compare ERMFLAIM with the baseline routing protocol GPSR [1] in the experiments. 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 with its key, which is verified by the next hop en route. This 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. 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 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 a long path length with a higher routing cost than GPSR.

We use the following metrics:
(1) The number of actual participating nodes.
(2) The number of random-forwarders.
(3) The number of remanent nodes in a destination zone.
(4) The number of hops per packet.
(5) Latency per packet.



(a) Different number of packets transmitted. (b) Different network size.

Fig. 6. The number of actual participating nodes.

A. *The number of actual participating nodes*

Figure 3(a) demonstrates the cumulated actual participating nodes in ERMFLAIM, GPSR, ALARM and AO2P, with 100 and 200 nodes moving at a speed of 2m/s. Since ALARM, GPSR and AO2P have a similar routing scheme, and thus have similar number of actual participating nodes, we use GPSR to also represent ALARM and AO2P in discussing the performance difference between them and ERMFLAIM. We see that ERMFLAIM generates many more actual participating nodes since it produces many different routes between each S-D pair. The figure shows that he number of actual participating nodes up to 30 in the 100 nodes case and is up to 45 in the 200 nodes case. In ERMFLAIM, more nodes in the network produce more actual participating nodes because each routing involves different random forwarders, which is a key property of ERMFLAIM to provide routing anonymity. On the contrary, GPSR only has a slight increase in the number of participating nodes because it always takes the shortest path based on greedy routing. Figure 3(b) shows the number of actual participating nodes after the transmission of 20 packets versus the number of nodes in the network. We see that the number of actual participating nodes in GPSR is steady with a marginal increase. This is because the increased node density provides shorter routes. We can also see that ERMFLAIM generates dramatically more participating nodes anonymity property of ERMFLAIM. On the contrary, the shortest routing paths in ALARM, AO2P and GPSR follow the same greedy routing principle, which are easy to identify by adversaries through traffic analysis. Especially, when there are only few nodes that communicate in the network, the route between two nodes could become very clear.

B. *Destination anonymity protection*

Figure 5 depicts the number of remanent nodes with 5 partitions and a 2m/s node moving speed when the node density equals 100, 150, and 200. The figure shows that the number of remanent nodes increases as node density grows while it decreases as time goes on. This is because a higher node density leads to more nodes in the destination zone and a greater chance that more nodes remain in the destination zone after a certain time. Also, because of node mobility, the number of nodes that have moved out of the destination zone increases as time passes.

C. *Routing performance*

In this experiment, we evaluated the routing performance of ERMFLAIM compared with GPSR, AO2P, and ALARM in terms of latency, number of hops per packet,

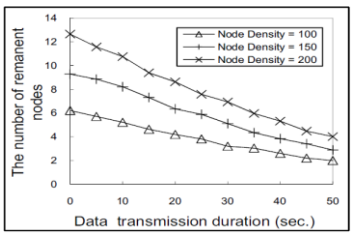


Fig. 7. Destination anonymity.

and delivery rate. For GPSR, if a destination node has moved away from its original position without a location update, the forwarding nodes will continue to forward the packet to other nodes until the routing path length reaches a predefined TTL. In a transmission session, if the position of a packets destination is changed but is not updated in the location service, the packet may not successfully reach the destination.

VI. CONCLUSION

Previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ERMFLAIM 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. ERMFLAIM 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. In addition, ERMFLAIM has an efficient solution to counter intersection attacks. ERMFLAIM’s ability to fight against timing attacks is also analyzed. It can also achieve comparable routing efficiency to the base-line AODV algorithm.

REFERENCES

[1] M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An anonymous on-demand position-based routing in mobile ad hoc networks," in Applications and the Internet, 2006. SAINT 2006. International Symposium on, Jan 2006, pp. 7 pp.–306.

[2] Z. Zhi and Y. Choong, "Anonymizing geographic ad hoc routing for preserving location privacy," in Distributed Computing Systems Workshops, 2005. 25th IEEE International Conference on, June 2005, pp. 646–651.

[3] K. El Defrawy and G. Tsudik, "ALARM: Anonymous location-aided routing in suspicious manets," in Network Protocols, 2007. ICNP 2007. IEEE International Conference on, Oct 2007, pp. 304–313.

[4] I. Aad, C. Castelluccia, and J.-P. Hubaux, "Packet coding for strong anonymity in ad hoc networks," in Securecomm and Workshops, 2006,Aug 2006, pp. 1–10.

[5] X. Wu and B. Bhargava, "AO2P: ad hoc on-demand position-based private routing protocol," Mobile Computing, IEEE Transactions on, vol. 4, no. 4, pp. 335–348, July 2005.

[6] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous geo-forwarding in manets through location cloaking," Parallel and Distributed Systems, IEEE Transactions on, vol. 19, no. 10, pp. 1297–1309, Oct 2008.

[7] H. Shen and L. Zhao, "ALERT: An anonymous location-based efficient routing protocol in manets," Mobile Computing, IEEE Transactions on, vol. 12, no. 6, pp. 1079–1093, June 2013.

[8] J. Kong and X. Hong, "ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks," in Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing, ser. MobiHoc '03. New York, NY, USA: ACM, 2003, pp. 291–302.

[9] L. Yang, M. Jakobsson, and S. Wetzel, "Discount anonymous on demand routing for mobile ad hoc networks," in Securecomm and Workshops, 2006, Aug 2006, pp. 1–10.