ISSN(Online):2320-9801
ISSN(Print): 2320- 9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 5, May 2014

Anonymous Secure Routing Scheme in Mobile Adhoc Networks

K. Keerthi
Assistant Professor, Asan Memorial College of Engineering and Technology, Chengalpattu, India.

ABSTRACT— Anonymous routing protocols are used by the existing Mobile Ad Hoc Networks (MANETs) to hide node identities and/or routes from outside observers. 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 offer high anonymity protection at a low cost, an Anonymous Location-based Efficient Routing protocol (ALERT) is proposed. ALERT dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver. Thus, ALERT offers anonymity protection to sources, destinations, and routes.

INDEX TERMS—Mobile ad hoc networks, anonymity, routing protocol, geographical routing

I. INTRODUCTION

The fast development of Mobile Ad-Hoc Networks have led to various wireless applications. MANETs are self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. They can be used in that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. Nodes in MANETs are vulnerable to malicious entities. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage.

1.2 Objective

Customization is necessary in any system that delivers matching content to subscribers in their desired format so we propose a content-based publish/subscribe (pub/sub) framework that delivers matching content to subscribers in their desired format. It enables the system to accommodate richer content formats including multimedia publications, also specifying their profile which includes the information about their receiving context. Content conversion is achieved through a set of content adaption operators (image transponder, document translator, etc.).

II. ALERT: AN ANONYMOUS LOCATION-BASED EFFICIENT ROUTING PROTOCOL

2.1 Networks and Attack Models and Assumptions

ALERT can be applied to different network models with various node movement patterns such as random way point model [17] and group mobility model [18]. 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.

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. 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, e.g., with denial-of-service (DoS) attacks, which may cut the routing in existing anonymous geographic routing methods.

2. Incapabilities. 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 bru-tally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

2.2 Dynamic Pseudonym and Location Service

In one interaction of node communication, a source node S sends a request to a destination node D and the destination responds with data. A transmission session is the time period that S and D interact with each other continuously until they stop. In ALERT, each node uses a dynamic pseudonym as its node identifier rather than using its real MAC address, which can be used to trace nodes' existence in the network. To avoid pseudonym collision, we use a collision-resistant hash function, such as SHA-1 [19], to hash a node's MAC address and current time stamp. To prevent an attacker from re computing the pseudonym, the time stamp should be precise enough (e.g., nanoseconds). Considering the network delay, the attacker needs to compute, e.g., 10^5, times for one packet per node.

When a node A wants to know the location and public key of another node B, it will sign the request containing B's identity using its own identity. Then, the location server of A will return an encrypted position of B and its public key, which can be decrypted by A using the pre distributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server.

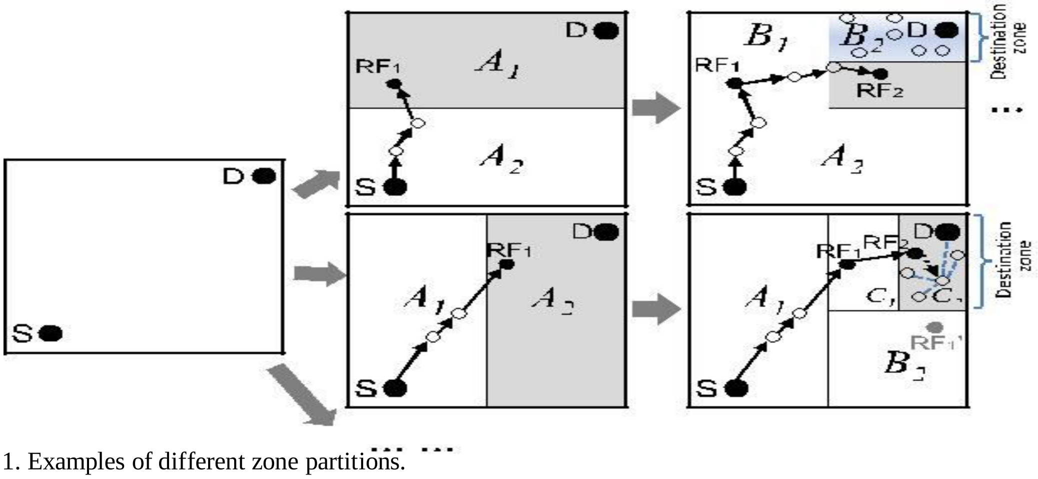

Fig. 1. Examples of different zone partitions.

2.3 The ALERT 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 ALERT.

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. 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. 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. 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 ALERT routing, each data source or forwarder executes the hierarchical zone partition. It first checks whether itself and destination are in the same zone. If so, it divides the zone alternatively in the horizontal and vertical directions. The node repeats this process until itself and Z_D are not in the same zone.

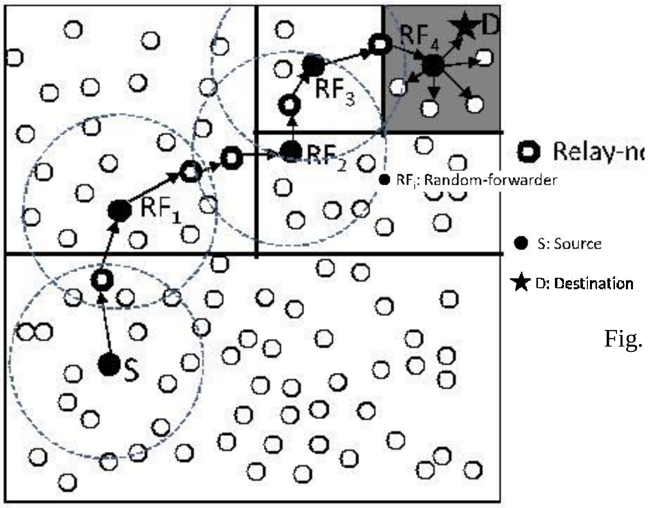

Fig. 2. Routing among zones in ALERT.

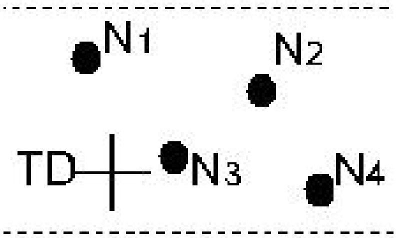

Fig. 3. Choosing a RF according to a given TD

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 [25] 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.

2.4 The Destination Zone Position

The reason we use Z_D rather than D is to avoid exposure of D. Zone position refers to the upper left and bottom-right coordinates of a zone. One problem is how to find the position of Z_D, which is needed by each packet forwarder to check whether it is separated from the destination after a partition and whether it resides in Z_D. Let H denote the total number of partitions in order to produce Z_D. Using the number of nodes in Z_D (i.e., k), and node density _, H is calculated by

$$H ¼ \log_2 \overline{{}_{-\,-}}^{\,G} ; \overline{k}$$

where G is the size of the entire network area. Using the calculated H, the size G, the positions ð0; 0Þ and ðx_G; y_GÞ of the entire network area, and the position of D, the source S can calculate the zone position of Z_D.

III. ANONYMITY PROTECTION AND STRATEGIES AGAINST ATTACKS

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

3.1 Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing [29], [3], [4], [10], [11], which always takes the shortest path, ALERT makes the route between a S-D pair difficult to discover by randomly and dynamically selecting the relay nodes. The resultant different routes for transmissions between a given S-D pair make it difficult for an intruder to observe a statistical pattern of transmission. This is because the RF set changes due to the random selection of RFs during the transmission of each packet. Even if an adversary detects all the nodes along a route once, this detection does not help it in finding the routes for subsequent transmissions between the same S-D pair.

3.2 Resilience to Timing Attacks

In timing attacks [16], through packet departure and arrival times, an intruder can identify the packets transmitted between S and D, from which it can finally detect S and D. For example, two nodes A and B communicate with each other at an interval of 5 seconds. After a long observation time, the intruder finds that A's packet sending time and B's packet receiving time have a fixed five second difference such as (19:00:55, 19:01:00) and (20:01:33, 20:01:38). Then, the intruder would suspect that A and B are communicating with each other.

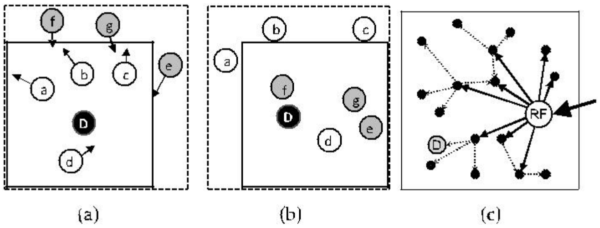

Fig. 5. Intersection attack and solution.

3.3 Strategy to 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 [16]. Though ALERT offers k-anonymity to D, an intersection attacker can still identify D from repeated observations of node movement and communication if D always stays in 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.

IV. THEORETICAL ANALYSIS

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

In our analysis scenario, we 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 1;000 m _ 1;000 m and the number of nodes equals 200. We set H ¼ 5 to ensure that a reasonable number of nodes are in a destination zone.

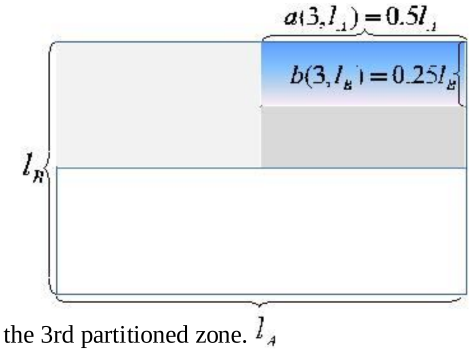

Fig. 6. The side lengths of the 3rd partitioned zone.

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

^{1}A

$_2$bh=2

að h; l_AÞ ¼ c ; ð1Þ

l_B

$_2$dh=2

bð h; l_BÞ ¼ e : ð2Þ

The side lengths of the destination zone after H partitions are aðH; l_AÞ and bðH; l_BÞ. Fig. 6 shows an example of three partitions of the entire network area. The side lengths of the final zone after the three partitions are

l_A

að3; l_AÞ ¼ $_2$b3=2c¼ 0:5l_A ð3Þ

and

l_B

bð3; l_BÞ ¼ $_2$d3=2e¼ 0:25l_B: ð4Þ

V. PERFORMANCE EVALUATION

In this section, we provide experimental evaluation of the ALERT protocol, which exhibit consistency with our 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. We compare ALERT with two recently proposed anonymous geographic routing protocols: AO2P [10] and ALARM [5], 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 [30] 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 30 s 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.

VI. CONCLUSION AND FUTURE WORK

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. 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. In addition, ALERT has an efficient solution to counter intersection attacks. ALERT's ability to fight against timing attacks is also analyzed. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. 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 comprehen-sive theoretical and simulation results.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Man-agement a Consolidated Proposal for Terminology, Version 0.31," technical report, 2005.

[2] Sk.Md.M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks," Proc. Int'l Symp. Applications on Internet (SAINT), 2006.

[3] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc [28] K.C. Lee, J. Haerri, L. Uichin, and M. Gerla, "Enhanced Perimeter Routing for Preserving Location Privacy," Proc. Third Int'l Work-shop Mobile Distributed Computing (ICDCSW), 2005. Routing for Geographic Forwarding Protocols in Urban Vehicular Scenarios," Proc. IEEE GlobeCom Workshops, 2007.

[4] V. Pathak, D. Yao, and L. Iftode, "Securing Location Aware [29] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Services over VANET Using Geographical Secure Path Routing," Ad Hoc Networks: Research Articles," Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.

[5] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- [30] "Ke Liu's NS2 Code," http://www.cs.binghamton.edu/~kliu/ Aided Routing in Suspicious MANETs," Proc. IEEE Int'l Conf. Network Protocols (ICNP), 2007.

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