International Journal of Recent Development in Engineering and Technology

Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)

International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Anonymity Defender for Preserving Secrecy of Source and Destination in Wireless Networks

Ms. Jane Shifa. I., (M.E), Mrs. F. Sangeetha M.Tech., (Ph.D)

PG Scholar, Dept. of CSE, St. Joseph's College of Engineering, Chennai, India.

Associate Professor, Dept. of CSE, St. Joseph's College of Engineering, Chennai, India.

i.janeshifa@gmail.com

fsangeetha@gmail.com

Abstract— **A wireless ad hoc network is a decentralized type of wireless network. It does not rely on a pre existing infrastructure. Each node partakes in routing by forwarding data for other nodes, so the decision of which nodes forward data is made dynamically on the basis of network connectivity. Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes equipped with both a wireless transmitter and a receiver that communicate with each other via bidirectional wireless links either directly or indirectly. However, this communication is limited to the range of transmitters. This means that two nodes cannot communicate with each other when the distance between the two nodes is beyond the communication range of their own. It is competent of forming a self-configuring and self-maintaining network without the help of a centralized infrastructure, which is frequently infeasible in vital mission applications like military conflict or emergency revitalization. Existing anonymous routing protocols that rely on either hop-by-hop encryption or redundant traffic either generate high cost or cannot provide full anonymity protection to information sources, destinations, and routes. To present high anonymity defense at a low cost, we propose Enhanced Adaptive Acknowledgement with ECC Signatures specially designed for MANETs. In this paper, we adopt a digital signature scheme during the packet transmission process. As in all acknowledgment-based IDSs, it is crucial to guarantee the integrity and legitimacy of all response packets. The projected approach examines the capability of the digital signature with enhancement using public key encryption.**

Keywords—network partitioning, public key encryption, destination zone, random forwarding, anonymity defender.

I. INTRODUCTION

Network establishment

A wireless network is created. Multiple new nodes are added within the network. Each new node added to the network is denoted by a node identifier using dynamic pseudonyms rather than using its real MAC address. Therefore, a node cannot be identified or tracked using its MAC address. A node's pseudonym expires after a specific time period so that the pseudonym cannot be pre-computed.

Network partitioning

For simplicity of design, we presume that the entire network area is generally a rectangle in which nodes are randomly distributed. 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 trace the positions of nodes in the entire area for zone partitions in Anonymity Defender. This features a dynamic and unpredictable routing path, which comprises of a number of dynamically determined intermediary relay nodes. 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 repeatedly splits the smallest zone in an alternating horizontal and vertical approach. We term this partition method hierarchical zone partition. This system 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.

We describe 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. Specifically, in the anonymity defender routing, each data source or forwarder executes the hierarchical zone partition. It initially verifies whether itself and destination are in the similar zone. If so, it splits the zone alternatively in the horizontal and vertical directions. The node repeats this procedure until itself and Z_D are not in the same zone. It then arbitrarily chooses a spot 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 labeled as a random forwarder (RF). Fig 1 illustrates an example where node N3 is the closest to TD, so it is selected as a RF . ALARM[1] aims at achieving k-anonymity [14] for destination node D, where k is a predefined integer. As a result, in the last step, the data are broadcasted to k nodes in Z_D , providing k-anonymity to the destination.

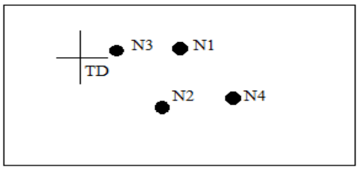

Fig.1. Selecting an RF according to a given TD.

II. RELATED WORK

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the present approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic cause significantly high cost. In addition, many approaches cannot provide all of the abovementioned anonymity protections. For example, ALARM [1] cannot protect the location anonymity of source and destination, SDDR [3] cannot provide route anonymity, and ZAP [2] only focuses on destination anonymity.

Many anonymity routing algorithms are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) [4]) 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. The all-to-all broadcast operation is so expensive in MANETs that the area is relatively unexplored. The way in which unreliable transmissions and mobility interact with the delivery of broadcasts over time make it intractable to find a benchmark or bound on performance. The effect of all-to-all broadcasting on energy efficiency in a MANET is studied in [5]. However, that study assumes that all nodes are directly connected. To our knowledge, the more complicated problem of all-to-all broad- casting in MANETs larger than a single node's transmission range requires further study. One application of all-to-all broadcasting is sharing location information. Many routing protocols proposed for MANETs benefit from having accurate, up-to-date information about the locations of other nodes in the network. The Location Aided Routing (LAR) unicast protocol [6], for example, uses location information to reduce the overhead of finding routes. Other protocols, such as the Depth First Search (DFS) protocol [7], use location information to determine routes directly. [8] and [9] provide surveys of MANET routing protocols that use location information.

The legend traversal problem in a MANET is similar to both the Traveling Sales- man Problem (TSP) and the Minimum Spanning Tree (MST) problem [10]. While there are several known algorithms to solve the TSP and MST problems, they work only for static networks. Also, in general they rely on global knowledge to solve the problem, while the legend is limited to its own local knowledge. Thus new methods are needed to solve the legend traversal problem in a MANET. The algorithm in [11] takes a different approach to the TSP. Its ant colony system uses ant-like agents to find a distributed solution to the TSP. However, they also use global knowledge to solve the problem. The GPSAL algorithm proposed in uses ant-like agents that resemble a legend in some ways. However, these agents are unicast from one node to another, instead of traversing the entire network like a legend. Ant-like agents augment a unicast routing protocol in [13] to form an Ant-AODV hybrid.

In that protocol, multiple ants act independently to collect connectivity information to update AODV routing tables. Conversely, limited resource is an inherent problem in MANETs, in which each node labors under an energy constraint.

MANETs complex routing and stringent channel resource constraints impose strict limits on the system capacity. Further, the recent increasing growth of multimedia applications (e.g., video transmission) imposes higher requirement of routing efficiency. However, existing anonymous routing protocols generate a significantly high cost, which exacerbates the resource constraint problem in MANETs. In a MANET employing a high-cost anonymous routing 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.

III. System Design

This work consists of a number of dynamically determined intermediate relay nodes. It 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.

In a S-D communication, S first embeds a symmetric key K^S , encrypted using D's public key, into a packet. Later, D sends S its requested contents, encrypted with K^S , decrypted by its own public key. Therefore, the packets communicated between S and D can be efficiently and securely protected using K^S . All the nodes from the source zone sent out the packets at the same time. Therefore, the source will be hidden among the nodes. A dynamic routing path is generated and the source node forwards the packet encrypted using the next forwarding nodes' public key. Only that RF can decrypt it with its corresponding private key.

This procedure continues for all the intermediate relay nodes and finally the packet is forwarded to the destination, which the destination will decrypt using its private key. Anonymity defender offers identity and location anonymity of the source and destination, as well as route anonymity.

Unlike geographic routing[11], which always takes the shortest path, Anonymity defender 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. Anonymity defender strengthens the privacy protection for S and D by the unlinkability of the transmission

endpoints and the transmitted data [1]. That is, S and D cannot be associated with the packets in their communication by adversaries. Anonymity defender incorporates the "notify and go" mechanism to prevent an intruder from identifying which node within the source neighbourhood has initiated packets. Anonymity defender also provides k-anonymity to destinations by hiding D among k receivers in ZD. Thus, an eavesdropper can only obtain information on ZD, rather than the destination position, from the packets and nodes en route. The route anonymity due to random relay node selection in anonymity defender prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In anonymity defender, 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 anonymity defender 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 anonymity defender.

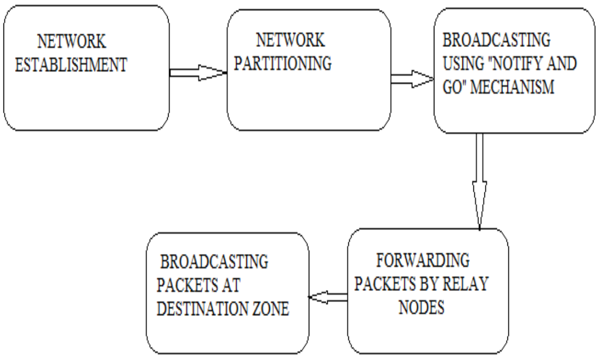
NETWORK ESTABLISHMENT
NETWORK PARTITIONING
BROADCASTING USING "NOTIFY AND GO" MECHANISM
FORWARDING PACKETS BY RELAY NODES
BROADCASTING PACKETS AT DESTINATION ZONE

Fig.2. Overall System Architecture

A. 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 ρ', H is calculated by

$$H= \log((\rho.G)/k),$$

where G is the size of the entire network area. Using the calculated H, the size G, the positions (0,0) and (x_G, y_G) of the entire network area, and the position of D, the source S can calculate the zone position of Z_D. Assume anonymity defender partitions zone vertically first. After the first vertical partition, the positions of the two generated zones are

(0,0), (0.5 x_G, y_G) and (0.5 x_G, 0),(x_G, y_G).

S then finds the zone where Z_D is located and divides that zone horizontally. This recursive process continues until H partitions are completed.

The final generated zone is the desired destination zone, and its position can be retrieved accordingly. Therefore, the size of the destination zone is $G/2^H$. For example, for a network with size G = 8 and position represented by (0,0) and (4, 2), if H = 3 and the destination position is (0:5, 0:8), the resulting destination zone's position is (0, 0) and (1, 1) with size of 8/ 2^3=1.

B. Source Anonymity

Anonymity defender contributes to the accomplishment 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 t_0 . In the "go" phase, S and its neighbors wait for a certain period of randomly chosen time €[t,t+t0] 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 t_0 may lead to a long transmission delay while a short t_0 may result in interference due to many packets being sent out simultaneously. Thus, t_0 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 n-anonymity where n 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.

Anonymity defender 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 = 0. After S decides the next TD, it forwards the packet to the next relay node, which is its neighbor based on GPSR. To prevent the covering packets from being differentiated from the ones sent by S, S encrypts the TTL field using K^{RN} 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.

C. Litheness 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.

Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks. In anonymity defender, the "notify and go" mechanism and the broad- casting in Z_D both put the interaction between S-D into two sets of nodes to obfuscate intruders. More importantly, the routing path between a given S-D and the communication delay (i.e., time stamp) change constantly, which again keeps an intruder from identifying the S and D.

D. Approach to defy 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 anonymity defender 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 communicating, 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.

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 [2] 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 occasion- ally fail to observe D's reception of packets. Since packets are delivered to Z_D always 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. It 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 pkt_1 and pkt_2 are mixed, an attacker observes that D is not in the recipient set of pkt_1 though D receives pkt_1 in the delivery time of pkt_2 . Therefore, the attacker would think that D is not the recipient of every packet in Z_D in the transmission session, thus blocking the intersection attack. Because the attacker may grab and analyze packets on air, the last forwarding node alters a number of bits in each packet to prevent the attacker from identifying identical packets in one broadcasting. This function is provided by the field (Bitmap) K_{pub} in each packet. The Bitmap records the altered bits and is encrypted using the destination's public key K_{pub} for recovering the original data. Since destination is not always within the recipient set, and the packet forwarded to a destination is different from the original packet, the attacker cannot identify the destination from its observation history by calculating the intersection set of nodes. This incurs two extra costs. One is the one- hop broadcasting of the recipients in the destination zone. The other is the encryption cost of changed bits.The percentage of nodes in Z_D that can receive the packet (i.e., coverage percent) is,

$$P_c + m*(P_c)/k,$$

where p_C denotes the percentage of the k m nodes that receive the packet from the m nodes in the second step. To ensure that D receives the packet, p_C should equal 1. $p_C = 1$ can be achieved by a moderate value of m considering node transmission range. A lower transmission range leads to a higher value of m and vice versa. The anonymity and routing efficiency properties of anonymity defender is theoretically analyzed. We examine the number of nodes that can participate in routing that function as camouflages for routing nodes. The number of RFs in a routing path, which shows the route anonymity degree and routing efficiency of anonymity defender. We calculate the anonymity protection degree of a destination zone as time passes to show anonymity defender'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 this analysis scenario, it is assumed 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 x 1,000 m and the number of nodes equals 200. We set H = 5 to ensure that a reasonable number of nodes in the destination.

IV. Conclusion And Future Scope

Anonymity Defender is an efficient, low cost and anonymity protection for sources, destinations, and routes based System. 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 anonymity defender includes the source and destination zones rather than their positions to provide anonymity protection to the source and the destination. Anonymity defender 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, anonymity defender has an efficient solution to counter intersection attacks. Anonymity defender's ability to fight against timing attacks is also analyzed.

Anonymity defender System uses location based information for route discovery and maintains anonymity in location based information. Conversely such system at times are complex and cannot be adoptable for all kind of the user. Thus to increase the performance and to avoid the dependences of the system , ID based Anonymous status is maintained using the Elliptic Curve Cryptographical approach.ECC based mechanism are PKI model and used to enhance the security of the system . Packet encryption is introduced to increase again the status of the system.

V. References

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

[2] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo-Forwarding in MANETs through Location Cloaking," IEEE Trans. Parallel and Distributed Systems, vol. 19, no. 10, pp. 1297-1309, Oct.2008.

[3] 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.

[4] 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.

[5] Stefano Basagni, Irnrich Chlamtac, Barry A. Woodward, "A Distance Routing Effect Algorithm for Mobility (DREAM)" (Oct. 1998), *Proc. MobiCom*, Dallas, TX, pp. 76–84.

[6] Qing Song and Xiaofan Wang, "Efficient Routing on Large Road Networks Using Hierarchical Communities" (Mar. 2011),*IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 1, pp. 132–140.

[7] Reza Shokri, Nasser Yazdani, Ahmad Khonsari, "Chain-based Anonymous Routing for Wireless Ad Hoc Networks" (Jun. 2011),*IEEE Trans.* pp. 297 – 302.

[8] Puttini,R.;Percher,J,;Me,L;de Sousa,R.,Computers and Communications, 2004. Proceedings. ISCC 2004. Ninth International Symposium on (Volume:1) pp. 331 – 338.

[9] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. IEEE 28th Int'l Conf. Distributed Computing Systems (ICDCS '08), pp. 411-420, 2008.

[10] 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.

[11] Ke Liu, Nael Abu-Ghazaleh,Kyoung-Don Kang, "Location verification and trust management for resilient geographic routing", Journal of Parallel and Distributed Computing, volume 67 Issue 2, February 2007, pp. 215-228.

[12] T. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '06), pp. 12-12, 2006.

[13] J. Hendricks, G. Ganger, and M. Reiter, "Verifying Distributed Erasure-Coded Data," Proc. 26th ACM Symp. Principles of Distributed Computing, pp. 139-146, 2007.

[14]Q. Wang, K. Ren, W. Lou, and Y. Zhang, "Dependable and Secure Sensor Data Storage with Dynamic Integrity Assurance," Proc. IEEE INFOCOM, Apr. 2009.

[15] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no. 1, pp. 69-73, 2012.

[16]M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions,"http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof mass email deletions, Dec. 2006.

[17]J.Kincaid, "MediaMax/TheLinkup Closes Its Doors," http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits-doors, July 2008.