International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5 Issue: Special 4, pp: 790-991 20 May 2016

Anonymous Private Routing and Secure Transmission Protocol in Ad Hoc Networks (APRSTPN)

DeepaV H (1CD14SCS07)
4rdSemM.Tech, CSE,
CiTech, Bangalore.

Dr. K Sathyanarayanareddy
Professor& HOD, Dept. of ISE,
CiTech, Bangalore.

Mr. Manjunatha P B
Asst. Prof., Dept. of CSE,
CiTech, Bangalore.

***Abstract*—There are large numbers of papers on routing in Mobile Ad Hoc Networks (MANETs) that use anonymous routing protocols which hide node identities and/or routes from outside observers in order to provide anonymity protection. However, the present anonymous routing protocols either have hop-by-hop encryption or redundant traffic either generates high cost or cannot provide full anonymity protection to source nodes, destination nodes, and routes. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications. To provide high anonymity protection with low cost, we proposeAnonymous Private Routing and Secure Transmission Protocol in Ad Hoc Networks (APRSTPN). APRSTPN dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediary relay nodes, forming a nontraceable anonymous route. It also hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, APRSTPN offers anonymity protection to sources, destinations, and routes. It also avoids the dead-end problem using geographic routing without compromising anonymity protection. APRSTPNachieves better route anonymity protection and lower cost compared to other anonymous routing protocols.**

***Index Terms*—**Anonymous routing protocol, mobile ad hoc networks, APRSTPN, anonymity, hierarchical zone partitioning, geographical routing, distributed location service.

I. INTRODUCTION

RAPID development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as education, emergency services, entertainment and military. MANETs have a self-organizing and independent infrastructure, making them an ideal choice for uses such as communication and information sharing. Because of the decentralization and openness features of MANETs, it is not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are prone to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Though anonymity may not be required in civil-oriented applications, it is crucial in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted data packets, track our soldiers (i.e., nodes), attack the sender nodes, and block the data transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage.

Anonymous routing protocols are very crucial in MANETs to give secure communications by hiding node identities and preventing traffic analysis attacks from observers outside the network. Anonymity in MANETs includes identity and location anonymity of data sources (i.e., senders) and destinations (i.e., recipients), as well as route anonymity. 'Location and identity anonymity of source nodes and destination nodes' means it is hard if possible for other nodes to obtain the real identities and exact locations of sources and destinations. For route anonymity, attackers, either en route or out of the route, cannot trace the flow of packet back to its source or to the destination, and none of the nodes have information about the true identities and locations of intermediary nodes en route. In order to dissociate the link between source and destination (i.e., relationship unobservability [1]), it is important to form an anonymous path between the two end-points and make sure that nodes en route do not know about where the endpoints are, mainly in MANETs, where location devices can be equipped.

Existing anonymous routing protocols in MANETs are mainly classified into two categories: hop-by-hop encryption [2], [3], [4], and redundant traffic [5]. Many of the present approaches are limited to focus on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate consequentially high cost. In addition, most of the approaches cannot provide all of the aforementioned anonymity protections. For example, ALARM [4] cannot protect the location anonymity of source and destination, SDDR [6] cannot provide route anonymity. Many anonymity routing algorithms [3], [4], [5] are based on the geographic routing protocol (e.g., Greedy Perimeter Stateless Routing (GPSR) [7]) that greedily forwards a packet to the

node closest to the destination. Nevertheless, 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, APRSTPN dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediary relay nodes that form a nontraceable anonymous route. Specifically, in each routing stage, a data forwarder partitions the field of network in order to separate itself and the destination into two zones. It then randomly selects a node in the other zone as the very next relay node and uses the GPSR [7] algorithm to send the data to the relay node. In the last stage, the sent data is communicated to k nodes in the destination zone, giving k-anonymity to the destination. In addition, APRSTPN has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. APRSTPN is also resilient to intersection attacks and timing attacks. In summary, the contribution of this work includes:

1. Anonymous routing. APRSTPN provides anonymous route, identity, and location anonymity of source nodes and destination nodes.
2. Low cost. Than relying on hop-by-hop encryption and redundant traffic, APRSTPN mainly uses randomized routing of one message copy to provide anonymity protection.
3. Resilience to intersection and timing attacks. APRSTPN has a strategy to effectively counter intersection attacks, which proves to be a tough open issue. APRSTPN can also avoid timing attacks because of its non-fixed routing paths for a source-destination pair.

II. RELATED WORK

A. *ALERT: An Anonymous Location-Based Efficient Routing Protocol*

Alert can be applied to different network models with various node movement patterns such as random way point model and group mobility model. Considering a MANET being deployed in a large field where geographic routing is used for node communication to reduce the latency of communication. The location of a sender who sent the message may be revealed by merely exposing the direction of transmission. Therefore, an anonymous transmission protocol that can provide intractability is needed to strictly ensure the anonymity of the sender when the sender communicates with another side of the field. Moreover, a malicious attacker observing may try to block the data packets by compromising number of nodes, intercepting the packets on number of nodes, or even tracing back to the sender by detecting the direction of data transmission. Hence, the route must also be undetectable. A malicious attacker observing may also try to detect destination nodes by analysing the traffic by launching an intersection attack. Hence, the destination node too needs the protection of anonymity. Here, the attackers may be battery powered nodes that passively receive network packets and detect activities in their region. They may also be powerful nodes that presume to be legitimate nodes and inject packets to the network according to the analytical results from their eavesdropped packets.

B. *ALARM: Anonymous Location-Aided Routing in Suspicious MANETs*

In most of the traditional mobile network scenarios, nodes establish communication based on persistent public identities. However, in few hostile and suspicious MANET settings, node identities should not be exposed and node movements should be untraceable. Instead, the nodes need to communicate based on their current locations. In this paper, they address some interesting issues that are arising in such MANETs by designing an anonymous routing framework (ALARM). It uses the nodes' current locations to construct a secure MANET map. Based on the current map constructed, each node decides which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve authentication of the node, integrity of data, untraceability (tracking-resistance) and anonymity. It also offers a resistance to certain insider attacks.

C. *AO2P: Ad Hoc On-Demand Position Based Private Routing Protocol*

Privacy is needed in ad hoc networks. Ad hoc on-demand position-based private routing algorithm, called A02P, proposed for anonymity in communication. Just the position of the destination node is exposed in the network for the discovery of route. To discover the routes with the fewer amounts of routing information, a receiver contention scheme is designed for determining the next hop. Pseudo identifiers are made used for data packet delivery after a route is been established. Real identities (IDS) for the sources, the destinations, and the forwarding nodes in the end-to-end connections are kept private. Destination anonymity relies on the difficulty of matching a geographic position to a true node ID. This is enforced by the use of secure position service systems. Node mobility enhances destination anonymity by making the match of a node ID with a position momentary. To improve destination privacy, R-A02P is proposed. Here in this protocol, the position of a reference point, rather than that of the position of the destination, is used for route discovery. Analytical models are developed for evaluating the delay in

route discovery and the probability of route discovery failure. Analysis and simulation results show that, while A02P preserves communication privacy in ad hoc networks.

III. MODELS AND ASSUMPTIONS

A. *Zone Partitioning*

This model uses hierarchical zone partitioning to partition the network field and nodes communicate between the zones.

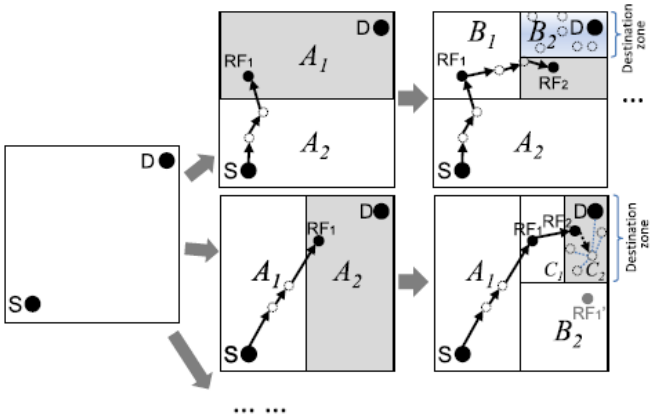

Fig. 1. Examples of different zone partitions

B. *Encryption and Random Forwarder Selection*

Uses symmetric key encryption and randomly chooses a node in next zone to transmit the data.

C. *Relay Node Selection*

Relay node is chosen in same zone to transmit the data to the random forwarder in the next zone.

D. *Decryption and Verification*

The destination node receives the data and can further be verified.

IV. OUR PROPOSED PROTOCOL SPECIFICATIONS

A. *Dynamic Pseudonym and Location Service*

InAPRSTPN, each node uses a dynamic pseudonym as its node identifier rather than using its original MAC address, which is used to trace nodes' existence in the network. To avoid the pseudonym collision, we need a collision resistant hash function, viz, SHA-1, to hash the node's MAC address and current time stamp. For preventing an attacker from recomputing the pseudonym, the time stamp should be small enough (e.g., nanoseconds). There can be number of nodes for an attacker to listen, so the computing overhead cannot be acceptable, and the success rate is also low. To further make it more complicated for an attacker to compute the timestamp; we increase the computation complexity using randomization for the time stamps. A node's pseudonym expires after a specified period of time in order to prevent adversaries from pseudonyms being associated with nodes. Every node with a periodic time piggybacks its updated position and pseudonym to "hello" messages, and keeps sending messages to its neighbors. And, each node maintains a routing table that keeps its neighbors' pseudonyms with their locations.

We assume that the public key and location of the destination of a data transmission can easily be known by other nodes, but its true identity requires protection. We utilize a secure location service to give the information of each node's location and public key. This kind of a location service enables a source node, which is aware of the destination identity, to securely obtain the location and public key of the destination. The public key can be used to enable two nodes to securely establish a symmetric key K_s for secure communication. Specifically, trusted normal nodes or dedicated service provider nodes are used to provide location service. Each node has a location server. The existence of each location servers are opposed by the ad hoc property of MANETs, and it is not needed to use location servers for MANET without security consideration. Anyways, anonymous communication requires third party servers to reliably collect and transmit confidential information.

A. *The APRSTPN Routing Algorithm*

For ease of illustration, we assume the entire network area is generally a rectangle in which nodes are randomly scattered. The information of the network area is configured into bottom-right node and upper left node boundary that joins in the system. This information helps a node to locate the positions of other nodes in the entire network area for zone partitions in ALERT.

APRSTPN features a dynamic and unpredictable routing path, consisting of a number of dynamically chosen intermediary relay nodes. As depicted in the upper part of Fig. 1, given a network area, we horizontally and vertically partition it into two zones A_1 and A_2 and further A_1 to B_1 and B_2 respectively. Then, we horizontally partition the zone B_2 into further two zones. Such consecutive zone partitioning splits the smallest size zone in an alternating horizontal and vertical manner. This partitioning process is called hierarchical zone partitioning. APRSTPN 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 APRSTPN. We call the zone having k nodes where D resides as the destination zone, denoted by Z_D. k controls the degree of anonymity protection of the destination node. The darkened zone in Fig. 2 is the destination zone. Specifically, in the APRSTPN routing, each data forwarder runs the hierarchical zone partitioning by first checking whether the data forwarder and destination node are in the same zone. If yes, it further divides the zone alternatively in horizontal and vertical directions. The nodes repeat this process unless the data forwarder and Z_D are not in one zone. Then by randomly choosing a position in an other zone called temporary destination (TD), and uses the GPSR routing algorithm to send the data to the node that is nearest to TD. TD is called as the random forwarder (RF). Fig. 3 shows an example where node N_3 is the nearer to TD, hence it is selected as a Random forwarder RF. APRSTPN aims at achieving k-anonymity [9] for the node D (i.e., destination node), and k is a predefined integer. In the final step, the data is broadcasted to all the k nodes in Z_D, thereby providing k-anonymity to the destination zone.

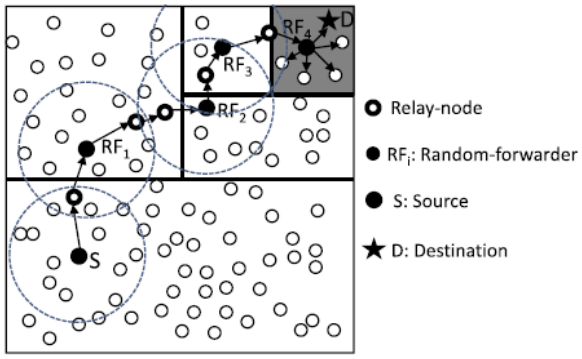

Fig.2. Routing among zones.

Given a Source-Destination pair, the partition pattern in APRSTPN varies depending on the randomly selected TDs and the order of division of network area horizontally and vertically, thereby giving a better anonymity protection. Fig. 1 presents two possible routing paths for a packet pkt sent by sender S to the destination D in APRSTPN. Other possible paths being, in the upper routing data flow, data source S horizontally divides the area first into two equal-size zones, A_1 and A_2, in a way to separate S and Z_D. Then S randomly chooses the first temporary destination TD_1 in the partitioned zone A_1 where Z_D is present. Further, S relies on GPSR to forward the pkt to TD_1. The pkt is sent by several relay nodes until it reaches a node that further cannot find a neighbor nearer to TD_1. This node is chosen to be the first random-forwarder RF_1. Upon RF_1 receiving the pkt, it vertically partitions the region A_1 into two regions B_1 and B_2 such that Z_D and it are separated into two different zones. Then, this process is being repeated until a packet receiver finds itself in Z_D, (i.e., a partitioned zone is Z_D having k nodes). After that, the node broadcasts the pkt to all the k nodes in that zone.The lower part of Fig. 1 shows another routing path based on a different partition pattern.

B. The Destination Zone Position

The reason we use Z_D rather than D is to avoid D from being exposed. How do we find the position of Z_D that is needed by every packet forwarder to check if it is separated from the destination after a horizontal/vertical partition and if it is residing in Z_D. Here, let H represent 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

$$H = \log_2(\rho.G/k)$$

Where G is the size of the entire network area. Using the computed H, the size G, the positions (0, 0) and (x_G, y_G) of the complete network area, and D's position, with these the source S can compute the zone position of Z_D.

C. Source Anonymity

APRSTPN contributes to the achievement of anonymity by restricting a node's view only to its neighbors and also by constructing the same initial and forwarded messages thereby making it difficult for an intruder/attacker to guess if a node is a source node or a forwarding node. To increase the anonymity protection of the source nodes, we introduce a lightweight mechanism called "notify and go." Its main idea is to let many nodes send packets at the same time as S to hide the source packet among the many other packets. This mechanism has two phases: The first "notify" phase, here S piggybacks its data transmission notification with timely update packets to notify its neighboring nodes that it will send a packet out. That packet consists of 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 $\in [t, t+t_0]$ before sending out messages.

D. Anonymity might compromise due to dead end

Dead end is one of the most common problems in the geographic routing where each node knows about the positions of its neighboring nodes in order to forward a packet to the neighbour closest to the destination. A dead end usually occurs when a packet is sent to a node which has all the neighbors further away from the destination than itself and then the packet is iteratively routed between neighbors. In ALERT, the transmission of every packet is on the basis of a series of RFs which decide about the region a packet should be forwarded to. Among any of the two RFs, the relay nodes perform the GPSR routing. Each relay node has no information about the S or D except the information on

destination zone. Its routing action is based on the coordinate of the next TD. Therefore, to avoid the dead-end problem without exposing any direct information about the S or D, and without compromising anonymity protection.We use Grid Location Service (GLS) [8] in APRSTPN. GLS is a new distributed location service that helps to track mobile node locations. GLS when combined with geographic forwarding allows the construction of ad hoc mobile networks that scale to a larger number of nodes than possible. GLS is decentralized and runs on the mobile nodes themselves which require no fixed infrastructure. Every mobile node regularly updates a small set of other nodes (its location servers) with its current location. A node forwards its position updates to its location servers without even knowing their actual identities, associated by a predefined ordering of node identifiers and a predefined geographic hierarchy. GLS is a location service that is built upon a number of location servers distributed throughout the network. There are three main activities in GLS: location server selection, location query request, and location server update.GLS is based on the idea that a node maintains its current location in a number of location serversdistributed throughout the network. These location servers are not specially designated; each node acts as a location server on behalf of some other nodes. The location servers for a node are relatively dense near the node but sparse farther from node; this ensures that anyone near a destination can use a closeby location server to find out the destination, also while limiting the number of location servers for every node.

IV. CONCLUSION

Already existing anonymous routing protocols, either relay on hop-by-hop encryption or redundant traffic, thus generating high cost. Also, some of the protocols are not able to provide complete anonymity protection to the source node, destination node, and to the route. Anonymous Private Routing and Secure Transmission Protocol in Ad-hoc Networks (APRSTPN) is distinguished by its low cost and anonymity protection for sources, destinations, and routes. It mainly uses dynamic hierarchical zone partitioning and random relay node selections to make it complicated for an intruder to detect the two end-points and nodes en route. A packet in APRSTPN includes the source and destination zones instead of their positions to provide anonymity protection to the source node and the destination node. APRSTPN further increases 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 that provides anonymity to the source, and uses broadcasting for destination anonymity. In addition, APRSTPN has an efficient solution to avoid the dead-end problem without compromising anonymity protection. APRSTPN ability to fight against timing attacks is also analyzed. It can achieve comparatively better routing efficiency to the base-line algorithm GPSR. Similar to that of other anonymity routing algorithms, APRSTPN is also not completely bulletproof to all attacks. Future work lies in reinforcing APRSTPN in an attempt to restrain stronger, active attackers.

REFERENCES

[1] A. Pfitzmann, M. Hansen, T. Dresden, and U. Kiel, "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management 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 Routing for Preserving Location Privacy," Proc. Third Int'l Workshop Mobile Distributed Computing (ICDCSW), 2005.

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

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

[11] A. Perrig, R. Canetti, D. Song, and J.D. Tygar, "Efficient and Secure Source Authentication for Multicast," Proc. Network and Distributed System Security Symp. (NDSS), 2001.