Ensuring Anonymity in MANET using Alert Protocol

M. Meenakshi[1] P. Srinivasa Ragavan[2]
[1]Master of Engineering [2]Assistant professor
[1, 2]CSE Department
[1, 2] P. S. R. Engineering College, Sivakasi, India.

Abstract---Mobile Ad Hoc Networks (MANET) has been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, the routing attacks getting more attention because it's changing the whole topology it and it causes more damages to MANET. The existing algorithm not provides the anonymity protection and finding the malicious node with degree of evidence from the expert knowledge and detects the important factors for each node. In proposed method the ALERT protocol is developed for overcome the existing problem. ALERT protocol is mainly providing a high anonymity protection with low cost. Using proposed protocol the network fields are dynamically partitions into zones and zones are randomly chosen from the nodes as intermediate relay nodes, which form a non-traceable by anonymous route. Particularly in every routing step, a data sender or forwarder division the network field in order to disconnected itself and the destination into two zones. In the last step, the data are broadcast to k nodes in the destination zone providing k-anonymity to the destination. ALERT is also flexible to timing attacks and intersection attacks. In addition, the experiments demonstrate the effectiveness of proposed approach with the consideration of several performances metric.

Keywords: Anonymous, GPSR, ALERT Protocol, MANET.

I. INTRODUCTION

A natural evolutionary step is to adopt such location-based operation to MANETS. This results in terms of location-based MANETS. In such a MANET, devices rely on location information in their operation. The main distinguishing feature of the envisaged location-based MANET environment is the communication paradigm, based not on permanent or semi-permanent identities, addresses or pseudonyms, but on instantaneous node location. In other words, a node (A) decides to communicate to another node (B), depending on exactly where (B) is located at present. If node location information is sufficiently granular, a physical MANET map can be constructed and node locations—instead of persistent node identities—can be used in place of network addresses. In some applications, such as military, law enforcement and search-and-rescue, node identities are not nearly as useful as node locations. Such critical settings have certain characteristics in common.

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 enroute 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 enroute.

In order to provide high anonymity protection (for sources, destination, and route) with low cost, we propose an Anonymous Location-based and Efficient Routing proTocol (ALERT). ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a 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 GPSR algorithm to send the data to the relay node. In the last step, the data is broadcasted to k nodes in the destination zone, providing k-anonymity to the destination. In addition, ALERT has a strategy to hide the data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT is also resilient to intersection attacks and timing attacks. We theoretically analyzed ALERT in terms of anonymity and efficiency. We also conducted experiments to evaluate the performance of ALERT in comparison with other anonymity and geographic routing protocols. In summary, the contribution of this work includes:

A. Anonymous routing. ALERT provides route anonymity, identity, and location anonymity of source and destination.

B. Low cost. Rather than relying on hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.

C. Resilience to intersection attacks and timing attacks. ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. ALERT can also avoid timing attacks because of its non-fixed routing paths for a source destination pair.

D. Extensive simulations. We conducted comprehensive experiments to evaluate ALERT's performance in comparison with other anonymous protocols.

II. ANONYMOUS ROUTING PROTOCOLS

This will 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.

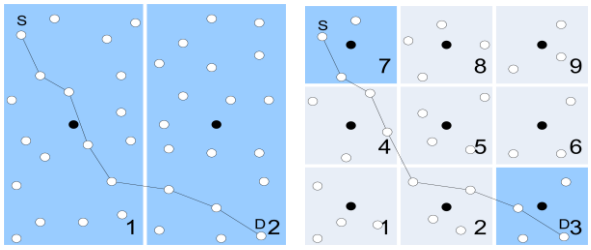

Fig. 1: By traffic analysis such as timing analysis and payload matching, colluded attackers (represented by black nodes) can divide the network space into smaller cells and shrink the anonymity set into a specific cell.

A. Anonymous Location-based and Efficient Routing proTocol (ALERT)

ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a 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. 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 A1 and A2. We then vertically partition zone A1 to B1 and B2. After that, we horizontally partition zone B2 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.

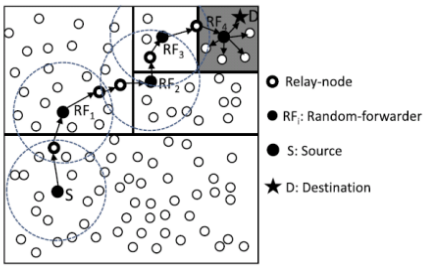

Fig. 2: Routing among zones in ALERT.

B. GPSR algorithm:

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 wireless networks comprised of numerous mobile stations, the routing problem of finding paths from a traffic source to a traffic destination through a series of intermediate forwarding nodes is particularly challenging. When nodes move, the topology of the network can change rapidly. Such networks require a responsive routing algorithm that finds valid routes quickly as the topology changes and old routes break. Yet the limited capacity of the network channel demands efficient routing algorithms and protocols that do not drive the network into a congested state as they learn new routes. The tension between these two goals, responsiveness and bandwidth efficiency, is the essence of the mobile routing problem. Greedy Perimeter Stateless Routing, GPSR, is a responsive and efficient routing protocol for mobile, wireless networks. Unlike established routing algorithms before it, which use graph-theoretic notions of shortest paths and transitive reachability to find routes, GPSR exploits the correspondence between geographic position and connectivity in a wireless network, by using the positions of nodes to make packet forwarding decisions. GPSR uses greedy forwarding to forward packets to nodes that are always progressively closer to the destination. In regions of the network where such a greedy path does not exist (*i.e.*, the only path requires that one move temporarily farther away from the destination), GPSR recovers by forwarding in perimeter mode, in which a packet traverses successively closer faces of a planar subgraph of the full radio network connectivity graph, until reaching a node closer to the destination, where greedy forwarding resumes.GPSR will allow the building of networks that cannot scale using prior routing algorithms for wired and wireless networks. Such classes of networks include:

1) *Rooftop networks:*
   Fixed, dense deployment of vast numbers of nodes
2) *Ad-hoc networks:*
   Mobile, varying density, no fixed infrastructure
3) *Sensor networks:*
   Mobile, potentially great density, vast numbers of nodes, impoverished per-node resources
4) Vehicular networks
   Mobile, non-power constrained, widely varying density.

C. Attack Mitigation:

ALERT has a strategy to effectively counter intersection attacks, which have proved to be a tough open issue. ALERT can also avoid timing attacks because of its non-fixed routing paths for a source destination pair. 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 route anonymity due to random relay node selection in ALERT prevents an intruder from intercepting packets or compromising vulnerable nodes en route to issue DoS attacks. In ALERT, 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 ALERT 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 ALERT.

III. Related Works

As reviewed in [2] Karim El Defrawy, Gene Tsudik Proposed a secure link-state based routing protocol

(ALARM). ALARM uses nodes' current locations to securely disseminate and construct topology snapshots and forward data. With the aid of advanced cryptographic techniques (e.g., group signatures), ALARM provides both security and privacy features, including node authentication, data integrity, anonymity, and untraceability (tracking-resistance). It also offers protection against passive and active insider and outsider attacks. To the best of our knowledge, this work represents the first comprehensive study of security, privacy, and performance tradeoffs in the context of link-state MANET routing. Flooding is used to disseminate LAMs; scalability becomes problematic for large MANETS (thousands of nodes). Any node can lie about its location or generate multiple LAMs as part of a Sybil attack.

As reviewed in [3] Xiaoxin Wu, Jun Liu, Xiaoyan Hong, and Elisa Bertino,Traditionally, the anonymity of an entity of interest can be achieved by hiding it among a group of other entities with similar characteristics, i.e., an anonymity set. In mobile ad hoc networks, generating and maintaining an anonymity set for any ad hoc node is challenging because of the node mobility and, consequently, the dynamic network topology. We propose protocols that use the destination position to generate a geographic area called an anonymity zone (AZ). A packet for a destination is delivered to all the nodes in the AZ, which make up the anonymity set. The size of the anonymity set may decrease, because nodes are mobile, yet the corresponding anonymity set management is simple. We design techniques to further improve node anonymity and reduce communication overhead. We use analysis and extensive simulation to study the node anonymity and routing performance and to determine the parameters that most impact the anonymity level that can be achieved by our protocol.

As reviewed in [4] X. Wu, J. Liu, X. Hong, and E. Bertino Anonymous routing schemes in MANETs can be classified into on-demand or reactive routing methods, proactive routing methods and anonymous middleware routing method. A finer classification of reactive routing methods includes hop-by-hop encryption and redundant traffic routing which either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. An Anonymous Location-based Efficient Routing protocol (ALERT) was used to offer high anonymity protection at a low cost. Like other anonymity routing algorithms, ALERT is not completely bulletproof to all attacks. To prevent the occurrence of stronger and active attackers, we propose a Secure Cryptographic Based Mix-Zones Routing Protocol (SCMIX).The idea for mix-zones is to prevent the adversary from accessing the content of messages, including the Node's signatures. All legitimate nodes within the mix-zone obtain a symmetric key and utilize this key to encrypt all their messages while within the zone.

As reviewed in [5] Chao-Chin Chou, David S. L. Wei, An efficient anonymous communication protocol, called MANET Anonymous Peer-to-peer Communication Protocol (MAPCP), for P2P applications over mobile ad-hoc networks (MANETs) is proposed in this work. MAPCP employs broadcasts with probabilistic-based flooding control to establish multiple anonymous paths between communication peers.It requires no hop-by-hop encryption/decryption along anonymous paths and, hence, demands lower computational complexity and power consumption than those MANET anonymous routing protocols. Since MAPCP builds multiple paths to multiple peers within a single query phase without using an extra route discovery process, it is more efficient in P2P applications. Through analysis and extensive simulations, we demonstrate that MAPCP always maintains a higher degree of anonymity than a MANET anonymous single-path routing protocol in a hostile environment Simulation results also show that MAPCP is resilient to passive attacks.

IV. Simulation Results

ALERT routing is analyzed by the NS2 network simulator. Although NS2 has support for wireless and mobile ad-hoc network simulation, geographic routing is not available in the standard NS2 code. The patch simulates IEEE 802.11 MAC layer with a node range of 500m. It provides support for mobility through the random way point model. In the group mobility model, we set the movement range of each group to 150 m with 10 groups and to 200 m with five groups.

The tests were carried out on NS-2.29 simulator using 802.11 as the MAC protocol with a standard wireless transmission range of 250 m and UDP/CBR traffic with a packet size of 512 bytes. The test field in our experiment was set to a 1,000 m _ 1,000 m area with 200 nodes moving at a speed of 2 m/s, unless otherwise specified. The density was set to 50, 100, 150, and 200 nodes per square meters. The duration of each simulation was set to 100 s unless otherwise indicated.

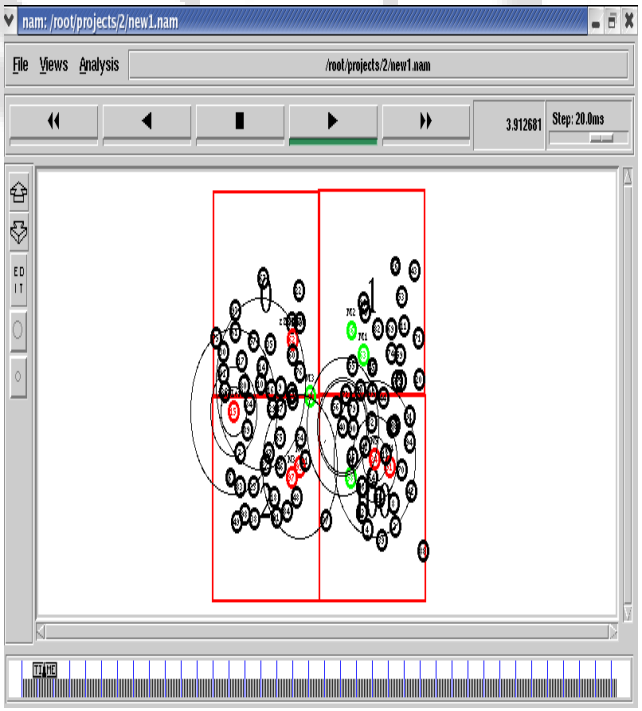

Fig. 3: Routing among Zones

The figure shows the routing among zones using ALERT protocol. It hides the node identity in an anonymous manner. The routing path maintains a minimum distance path by tracking the nearest nodes using GPSR algorithm. The zone leader selects the forwarder node and also forward to the relay nodes in the next zone.

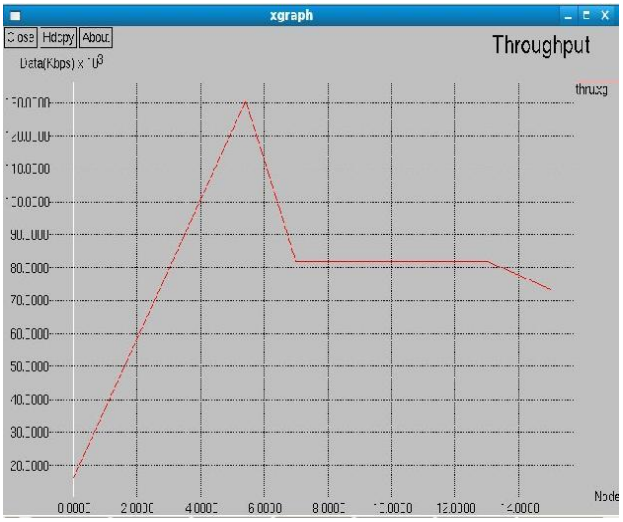

Fig. 4: Data Vs Nodes Throughput

The throughput test was done and analyses were performed on the data sent. The graph above shows results for Data Vs Nodes. The throughput rises at its peak at node 6 and levels off after 6which gradually decreases after 12.

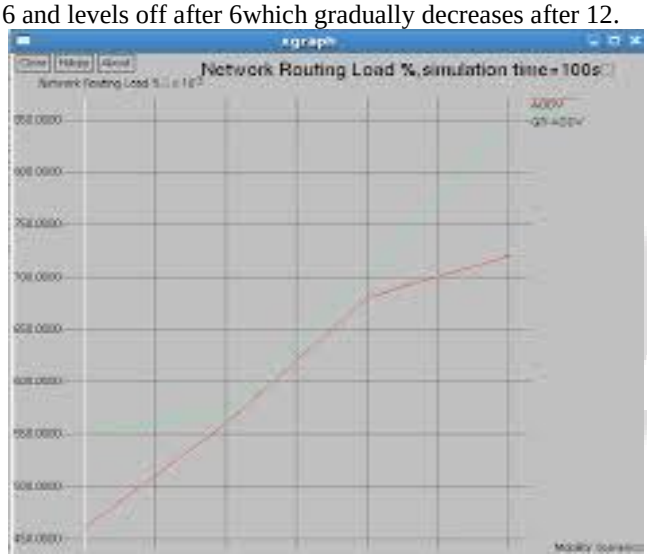

Fig. 5: Routing load Vs Execution time

It shows execution time increases gradually with increase in the routing load. In communications, the lower limit of latency is determined by the medium being used for communications. In reliable two-way communication systems, latency limits the maximum rate that information can be transmitted, as there is often a limit on the amount of information that is "in-flight" at any one moment.

V. Conclusion And Future Work

In this paper we first showed the relevance of using multicast for anonymity in ad hoc networks. Multicast considerably reduces the number of transmissions, with respect to anonymity techniques based on unicast, whenever a given anonymity set is to be reached. To make multicast work with anonymity techniques, such as onion encryption, we devised techniques for packet routing headers and the packet payloads separately. The resulting combination is a constantly changing/unrecognizable packet (header and payload), being routed on a multicast tree to reach a given anonymity set while reducing the transmission costs. Different novel techniques were introduced for different network models: for networks with tamper-resistant devices, the anonymity techniques we introduce alleviate the use of encryption, making it "light"enough without compromising the required level of anonymity. For networks with non-tamper-resistant devices, we introduced new techniques that guarantee anonymity, even when a large number of nodes gets compromised. Though novel, the techniques we present may be combined or adapted to existing security protocols to thwart their corresponding security attacks, without being constrained by our techniques. We evaluate each technique to show its performance costs and benefits.

References

[1] L. Zhao And H. Shen, "Alert: An Anonymous Location-Based Efficient Routing Protocol In Manets," Ieee Transactions On Mobile Computing, Vol. 12, No. 6, June 2013

[2] K.E. Defrawy And G. Tsudik, "Alarm: Anonymous Location-Aided Routing In Suspicious Manets," Ieee Transactions On Mobile Computing, Vol. 10, No. 9, September 2011.

[3] 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.

[4] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, And K. Naik, "An Efficient Anonymous Communication Protocol For Peer-To-Peer Applications Over Mobile Ad-Hoc Networks," Ieee J. Selected Areas In Comm., Vol. 25, No. 1, Pp. 192-203, Jan. 2007.

[5] K.E. Defrawy And G. Tsudik, "Prism: Privacy-Friendly Routingin Suspicious Manets (And Vanets)," Proc. Ieee Int'l Conf.Network Protocols (Icnp), 2009.

[6] V. Pathak, D. Yao, And L. Iftode, "Securing Location Aware Services Over Vanet Using Geographical Secure Path Routing," Proc. Ieee Int'l Conf. Vehicular Electronics And Safety (Icves), 2008.

[7] S. Seys And B. Preneel, "Arm: Anonymous Routing Protocol For Mobile Ad Hoc Networks," Int'l J. Wireless And Mobile Computing, Vol. 3, No. 3, Pp. 145-155, 2009

[8] K.C. Lee, J. Haerri, L. Uichin, And M. Gerla, "Enhanced Perimeter Routing For Geographic Forwarding Protocols In Urban Vehicular Scenarios," Proc. Ieee Globecom Workshops, 2007.

[9] H. Frey And I. Stojmenovic, "On Delivery Guarantees Of Face And Combined Greedy-Face Routing In Ad Hoc And Sensor Networks," Proc. Acm Mobicom, 2006.

[10] Sk. Md. M. Rahman, M. Mambo, A. Inomata, And E. Okamoto, "An Anonymous On-Demand Position-Based Routing In Mobile Ad Hoc Networks", In Proc. Of Saint, 2006.

[11] X. Wu, J. Liu, X. Hong, And E. Bertino, "An Efficient Anonymous Location Service For Geographic Ad Hoc Routing In Manet," International Journal Of Computer Applications Technology And Research Volume 2–Issue 6, 748 - 751, 2013

[12] Priyanka Malgi Dayanand Ambawade "Apsar: Anonymous Position Base Security Aware Routing Protocol For Manets", International Journal Of Computer Applications (0975 – 8887) International Conference On Communication Technology 2013

