International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Secured Routing Using ALERT in MANETs

Aniket K. Khasnikar[1], Smita Kapse[2]

[1]P.G. Student, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, India

[2]Assistant Professor, Department of Computer Technology, Yeshwantrao Chavan College of Engineering, Nagpur, India

Abstract: ***The routing protocol depends on either hop-by-hop routing table which generates high cost and also unable to provide full anonymity protection to data sources, destinations and routes. So as to provide high anonymity protection at low cost in MANETs (Mobile Ad-hoc Networks), ALERT (Anonymous Location-Based Efficient Routing Protocol) routing protocol can be used. In the ALERT protocol, it partitions the network into zones which randomly chooses nodes as intermediate relay nodes. It also hides the data receiver or initiator between many receivers to strengthen source and destination anonymity protection. Thus it provides Anonymity Protection to sources, destinations and routes. ALERT also achieves comparable routing efficiency to base-line GPSR (Greedy Perimeter Stateless Routing) algorithm.***

Keyword: Anonymity Protection, GPSR Algorithm, Relay nodes, ALERT, MANETs

1. Introduction

Anonymous routing protocols are crucial 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 and destinations, as well as route anonymity. For route anonymity, either end route or out of the route, cannot trace a packet flow back to its source or destination, and no node has information about the real identities and locations of intermediate nodes route. Also, in order to dissociate the relationship between source and destination, it is important to form an anonymous path between the two endpoints and ensure that nodes en route do not know where the endpoints are. Existing anonymity routing protocols can be mainly classified into two categories: hop-by-hop encryption and redundant traffic. Most of the current approaches are limited by focusing on enforcing anonymity at a heavy cost to precious resources because public-key-based encryption and high traffic generate significantly high cost. In addition, many approaches cannot provide all of the aforementioned anonymity protections [1][3][4][2].

In order to provide high anonymity protection for sources, destination, and route with low cost, so Anonymous Location-based and Efficient Routing protocol (ALERT) is proposed. ALERT dynamically partitions a network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non-traceable anonymous route.[8][9]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.

2. Alert: An Anonymous Location-Based Efficient Routing Protocol

A. Dynamic Pseudonym and Location Service

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 the nodes which are existence in the network. To avoid pseudonym collision, we can use collision resistant hash function, such as SHA-1, to hash a node's MAC address and current time stamp. The time stamp should be precise enough to prevent it from recomputing the pseudonym from the attacker. A node's pseudonym will expires after a specific time period in order to prevent adversaries from associating the pseudonyms with nodes. If pseudonyms are changed too frequently, the routing may get disturbed and if pseudonyms are changed too infrequently, the adversaries may associate pseudonyms with nodes across pseudonym changes. Therefore, the frequently change in pseudonym should be appropriately determined. Also each node is associated with location server. 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 [7][6]. Then, the location server of A will return an encrypted position of Band its public key, which can be decrypted by A using the predistributed shared key between A and its location server. When node A moves, it will also periodically update its position to its location server.

B. Routing Algorithm: ALERT

Generally the entire network area is rectangle in which nodes are randomly arranged. The information of the upper-left and bottom-right boundary of the network area is configured into each node when it joins the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT. In ALERT routing protocol, we uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each step as an intermediate relay node, thus dynamically generating an unpredictable routing path for a message. We first horizontally partition the given area into two zones. Then vertically partitions the zone in which the destination node is present. After that, we again horizontally partition zone into two zones. Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and verticalmanner. Such partition process is known as hierarchical zone partition.

C. Source Anonymity

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

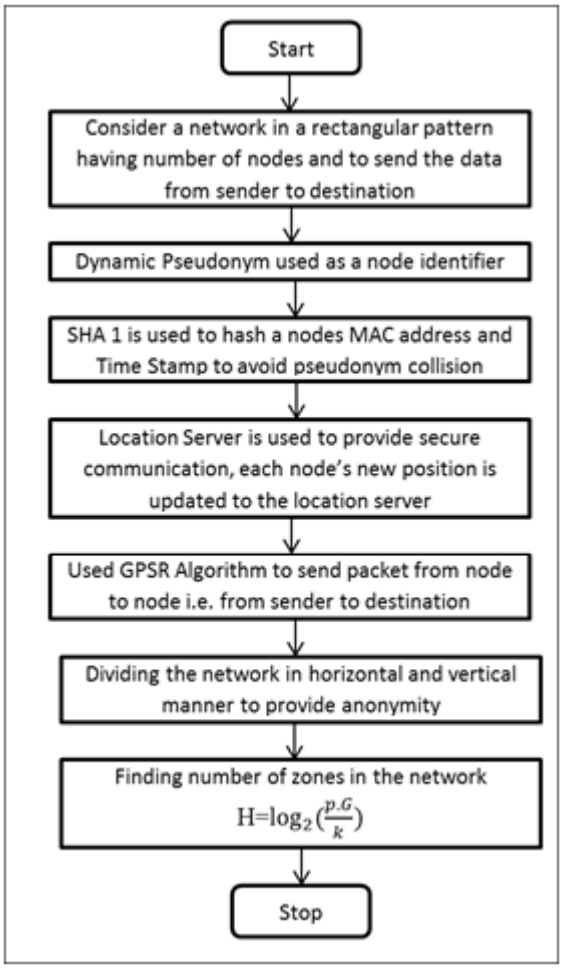

Figure 1: Flowchart of ALERT

3. GPSR Algorithm

The algorithm consists of two methods for forwarding packets, greedy forwarding, which is used wherever possible, and perimeter forwarding, which is used in the regions where greedy forwarding cannot be used.

A. Greedy Forwarding

If a node knows its radio neighbors' positions, the locally optimal choice of next hop is the neighbor geographically closest to the packet's destination. Forwarding in this regime follows successively closer geographic hops, until the destination is reached.

B. The RightHand Rule: Perimeters

This rule states that when arriving at node one nodefrom another node, the next edge traversed is the next one sequentially counterclockwise about first nodefrom edge (one node ;another node). It is known that the right-hand rule traverses the interior of a closed polygonal region (a face) in clockwise edge order.

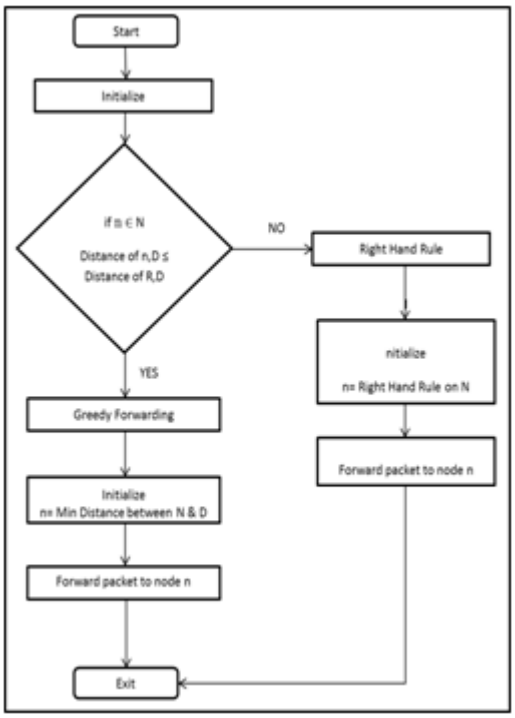

Figure 2: Flowchart of GPSR Algorithm

In the above flowchart, R is the node receiving packet, p is a packet, D destination, N is a set of one-hop neighbor of R, n is a node of set N.

4. Anonymity Protection And Strategies Against Attacks

a) Anonymity Protection

ALERT offers identity and location anonymity of the source and destination, as well as route anonymity. Unlike geographic routing 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 [5][8]. This is because the RF set changes due to the random selection of RFs during the transmission of each packet.

b)Resilience to Timing Attacks

In timing attacks, by using packet departure and arrival times, an intruder can identify the packets transmitted between Sender and Destination, from which it can finally detect Sender and Destination. Avoiding the exhibition of interaction between communication nodes is a way to counter timing attacks [10]. In ALERT, the notify and go mechanism and the broadcasting in Zone Destinationare put in the interaction between Sender Destination into two sets of nodes to intruders.

c) 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 [9]. Intersection attacks are a well-known problem and have not been well resolved.

5. Conclusion

In previous anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, generate high cost. 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 route. ALERT also 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. It can also achieve comparable routing efficiency to the base-line using GPSR algorithm.

References

[1] HaiyingShen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs", IEEE Transaction on Mobile Computing, 2013.
[2] K.E. Defrawy and G. Tsudik, "ALARM: Anonymous Location- Aided Routing in Suspicious MANETs", IEEE International Conference on Network Protocols (ICNP), 2007.
[3] Sk. Md. M. Rahman, M. Mambo, A. Inomata, and E. Okamoto, "An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks", International *Symposium* Applications on Internet (SAINT), 2006.
[4] Z. Zhi and Y.K. Choong, "Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy", 3rd International Workshop on Mobile Distributed Computing (ICDCSW), 2005.
[5] X. Hong, M. Gerla, G. Pei, and C.C. Chiang, "A Group Mobility Model for Ad Hoc Wireless Networks," 2nd ACM International Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
[6] M.F. Mokbel, C.-Y. Chow, and W.G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy", Thirty Second International Conference on Very Large Databases (VLDB), 2006.
[7] X. Wu, "DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles", International Conference on Wireless Communication and Mobile Computing, 2006.
[8] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks", IEEE 29th Annual International Conference on Local Computer Networks (LCN), 2004.
[9] X. Wu, J. Liu, X. Hong, and E. Bertino, "Anonymous Geo- Forwarding in MANETs through Location Cloaking," IEEE Transaction on Parallel and Distributed Systems, 2008.
[10] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems", International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), 2001.