Available online at www.elixirpublishers.com (Elixir International Journal)

Network Engineering

Elixir Network Engg. 83 (2015) 33144-33147

ISSN: 2229-712X

Securing Node Identities and Route Identities using alert in Manets

S.Gowri Shankari and K.Logeswaran

Department of Information Technology, Kongu Engineering College, Perundurai, India.

ARTICLE INFO

Article history:

Received: 11 January 2015;

Received in revised form:

3 June 2015;

Accepted: 13 June 2015;

Keywords

Anonymous routing protocols,
Anonymity protection,
Hierarchical zone partition.

ABSTRACT

MANETs use various anonymous routing protocols for hiding node identities and/or route identities from the outside observers in order to provide anonymity protection. Perhaps, existing anonymous routing protocols generate high cost or cannot offer complete anonymity protection to sources, destination and routes. To suggest high anonymity protection at a low cost, one of the proposed system is ALERT. ALERT energetically partitions the network field into zones and arbitrarily chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. This partition process is called as hierarchical zone partition. In addition ALERT hides the data initiator or receiver among many initiators or receiver to reinforce the source as well as destination anonymity protection. Thus, ALERT offers anonymity protection to sources, destinations, and routes. It also has strategies to effectively encounter the intersection and timing attacks. Experimental results display stability with the theoretical analysis, and show that ALERT achieves better route anonymity protection in a low cost which it is compared with the other anonymous routing protocols.

Introduction

Mobile Ad Hoc Networks (MANETs) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. They may contain one or multiple and different transceivers between nodes. Providing anonymity among the nodes in network is a crucial task.

Anonymous routing protocols are critical in MANETs to give secure communications by hiding node identities and preventing traffic analysis attacks from the outside observers. Anonymity in MANETs includes identity anonymity as well as route anonymity. These are considering as a disadvantages of the MANETs while using existing anonymous routing protocols. Existing anonymous routing protocol are classified into two main categories: hop-by-hop encryption [1], [2], [3], [4], [5] and redundant traffic [6], [7], [8], [9]. Most of the recent approaches are to enforcing the anonymity protection at high cost because public key encryption and high traffic construct significantly high cost. In addition, many approaches cannot provide the complete anonymity protection. For example, Anonymous Location-Aided Routing in Suspicious MANETs (ALARM) [4] cannot able to offer the Location anonymity of source and destination, A Secure Dynamic Distributed topology-based Routing algorithm (SDDR) [10] cannot able to offer route anonymity, and Zone based Anonymous Positioning Routing (ZAP) [11] only concentrate on destination anonymity. Most of the anonymity based routing algorithms [2] are base on the geographic routing protocol for example Greedy Perimeter Stateless Routing (GPSR) that acquisitively forwards a packet to the node which is closest to the destination.

On the other hand, some degree of resource is an intrinsic problem in MAETs, in which each node efforts under an energy control. The current increasing growth of multimedia applications imposes higher requirement of routing effectiveness. However, existing anonymous routing protocols create a drastically high cost, which exacerbates the resource restraint 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 unfortunate delay in military operations.

In order to provide high anonymity protection for sources, destination, and route with low cost, one of the proposed system is an Anonymous Location-based and efficient Routing protocol (ALERT). ALERT energetically partitions a network field into zones and arbitrarily chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. At the time of each partitioning zone, the source can check if the destination node is in the same zone or not. The data is broadcasted to the k nodes in the destination zone for providing k-anonymity to the destination. ALERT has a scheme to conceal the data initiator among a number of initiators to reinforce the anonymity protection of the source. ALERT is also resilient to intersection attacks [12] and timing attacks [12]. In summary, the contribution of this work includes:

1. *Anonymous routing*. ALERT provides route anonymity, node anonymity, and location anonymity.
2. *Low cost*. Rather than relying hop-by-hop encryption and redundant traffic, ALERT mainly uses randomized routing of one message copy to provide anonymity protection.
3. *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 [12]. ALERT can also avoid timing attacks because of its nonfixed routing paths for a source destination pair.

Tele:
E-mail addresses: gowrishankari92@gmail.com

4. *Extensive simulations*. Comprehensive experiments were conducted to evaluate ALERT's performance in comparison with other anonymous protocols.

Related Work:

Anonymous routing schemes in MANETs have been deliberate in recent years. Also there are nameless middleware working between network layer and application layer [8].The two main categories of existing anonymous routing protocols are hop-by-hop encryption [1], [2], [3], [4], [5] and redundant traffic [6], [7], [8], [9].In hop-by-hop encryption routing, a packet is encrypted in the transmission of the two nodes, preventing adversaries from tampering or analyzing the packet contents to interrupt the statement.

In the AO2P [9] geographic routing algorithm, pseudonym identity is used as node identifier instead of using nodes real identity. It also chooses a neighbor which can reduce the supreme distance from the destination. Since AO2P does not provide destination anonymity protection. ASR [13] conducts authentication between the source and destination before the data transmission. The source and the forwarder insert their public keys to the messages and broadcast the message locally. The destination also responds to the source in the same way.

In each step, the response is encrypted by using the previous node's public key so that only the previous forwarder can decrypt the message and further forward it. still, such public key distribution makes it possible for attackers to trace source/destination. SEAD [14] uses low-cost one-way hash functions instead of symmetric key cryptographic operations. However, all of these hop-by-hop encryption methods create high cost due to the use of complex symmetric key cryptography.

Redundant traffic-based routing uses redundant traffic, such as multicast, local broadcasting, and flooding, to ambiguous potential attackers. ASR [13] shuffles packets to prevent traffic analysis in addition to the hop-by-hop authentication as mentioned above. ZAP [11] uses a destination zone, and broadcasts to a destination zone locally in order to reach the destination without leaking the destination identity. A main disadvantage of redundant traffic-based methods is the high overhead incurred by the redundant operations leading to high cost. Some methods like ZAP only perform local broadcast in a destination zone, these methods cannot offer source or routing anonymity.

ALARM [4] uses proactive routing; it uses nodes current locations to construct a secure MANET map. Each node broadcasts its location information to its authenticated neighbors so that each node can build a map for the future anonymous route discovery. However, this map leaks destination node location and compromises the route anonymity. Mix zones [15] and GLS [16] are zone-based location services. Mix zones is an anonymous location based service that shows the positions of mobile users in a long time period in order to prevent the users' movement. It can only monitor the registered nodes location. Although GLS also uses hierarchical zone partitioning for location service while in ALERT, it is used for anonymous routing. ALERT is quite different from GLS in the zone division scheme. A zone in ALERT is always split into two smaller rectangles, while GLS divides the entire square area into four sub squares and then recursively divides these into smaller squares. In ALERT, if the source and destination node is in the same zone means it splits the required zone into two. Likewise it consecutively splits the zones.

Routing Algorithm-ALERT:

ALERT features an energetic and random routing path, which consists of a number of dynamically determined intermediate relay nodes, as shown in the Figure 1. In a given area, first horizontally partition it into two zones A1 and A2. Then, vertically partition zone A1 to B1 and B2. After that, horizontally partition zone B2 into two zones.

Such zone partitioning consecutively splits the smallest zone in an alternating horizontal and vertical manner. So this partition process is called as hierarchical zone partition. ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone in each steps as an intermediate relay node, thus dynamically generating an unpredictable routing path for a message.

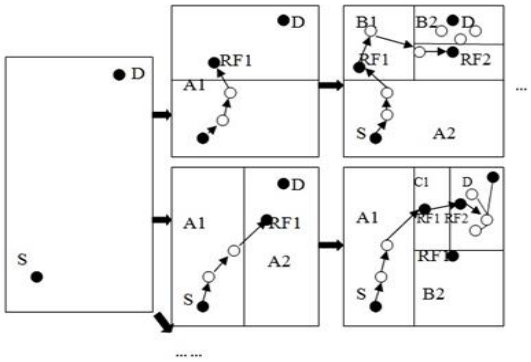

Figure 1. Examples of different zone partitions

Figure 2 shows an example of routing in ALERT. 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 Figure 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.

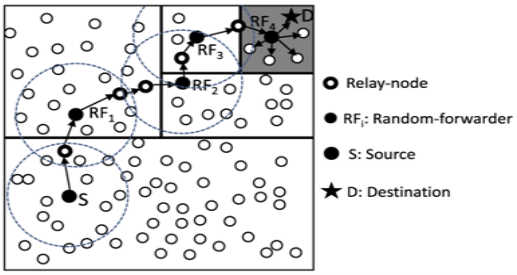

Figure 2. Routing among zones inn ALERT

The node repeats this process until and Z_D are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and send the data to the node which is closest to TD. This node is defined as a random forwarder (RF). ALERT aims at achieving *k*-anonymity 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.

Position of the Destination Zone

The reason for using 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), node density ρ, and size of the entire network area G, H is calculated by

$$H=\log_2(\rho.G/k) \quad (3.1)$$

The position of D and the source S can calculate the zone position of ZD. Assume ALERT partitions zone vertically first. S then finds the zone where ZD is located and divides that zone horizontally. This recursive process continues until H partitions are completed.

Source anonymity

ALERT contributes to the achievement of anonymity by restricting a node's view only to the neighbors and constructing the same initial and forwarded messages. This makes it difficult for an intruder to tell if a node is a source node or a forwarding node. To toughen the anonymity protection of the source nodes, trivial mechanism called "notify and go" is used. It has two phases: "notify" and "go". The basic idea is to send out the packets among the number of nodes the same time S for hiding the source packet among many other packets.

In the first "notify" phase, source S piggybacks its data transmission announcement with periodical update packets to notify its neighbors that it will send out packet. The packet includes two random back-off time periods, t and t_0. In the second "go" phase, S and its neighbors wait for a certain period of arbitrarily chosen time € [t, t+t_0] before sending out messages. ALERT utilizes a TTL field in each packet to prevent the packet issued in the first phase from being forwarded in order to reduce extreme traffic.

To prevent the wrapper packets from being differentiated from the ones sent by S, S encrypts the TTL field using k_{pub}^{RN} obtained from the review "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. As a result, only NRN will be able to successfully decrypt it, while other nodes drop such a packet.

Route anonymity

ALERT can provide the route anonymity in MANETs. It uses the AODV routing protocol for selecting the route from source to destination. It uses a threshold value for selecting the nearest neighbor node. The source node can select the neighbor node which contains the less than or equal to threshold value. Thus it creates an anonymous path between the source and destination.

Node anonymity

In one interaction of node communication , a source node S send 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.

Parameter setup

Table 1. Simulation Properties

Routing Protocols	ALERT-AODV, ALERT-DSR
Simulation Time	50sec
Packet Size	512 Bytes
Propagation Model	TwoRayGround Model
Traffic Type	CBR
Antenna Type	Omni Directional
Node Deployment	Random

Result Analysis

Nodes Vs Throughput

Throughput is referred as the number of successfully received packets in a unit time and it is represented in kbps. In ALERT-AODV, throughput is increased by 66.5%, when it is compared with ALERT-DSR as shown in Figure 3

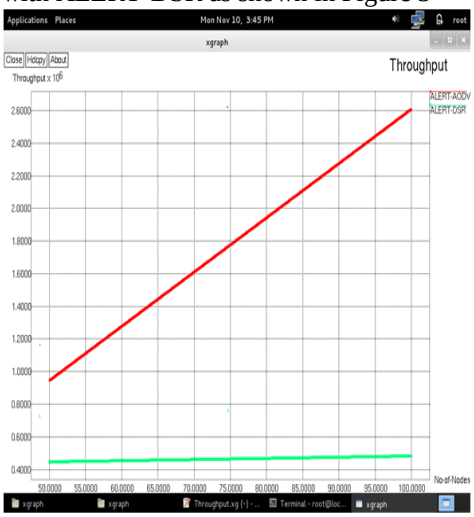

Figure 3. Nodes Vs Throughput

Nodes Vs Latency

Latency refers to the average time elapsed after a packet is send and before it is received. From the Figure 4, when ALERT-AODV is compared with ALERT-DSR, latency is decreased by 42% in ALERT-AODV.

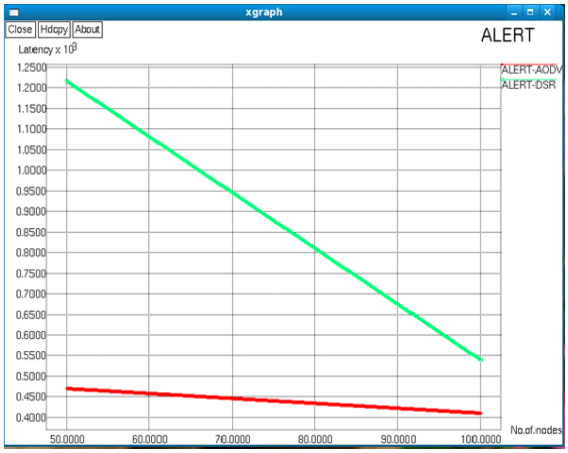

Figure 4. Nodes Vs Latency

Nodes Vs Packet Delivery Ratio

Packet Delivery Ratio is referred as the fraction of packets that are successfully delivered to a destination node. Packet Delivery Ratio in ALERT-AODV is increased by 56%, when it is compared with ALERT-DSR. It is shown in the Figure 5.

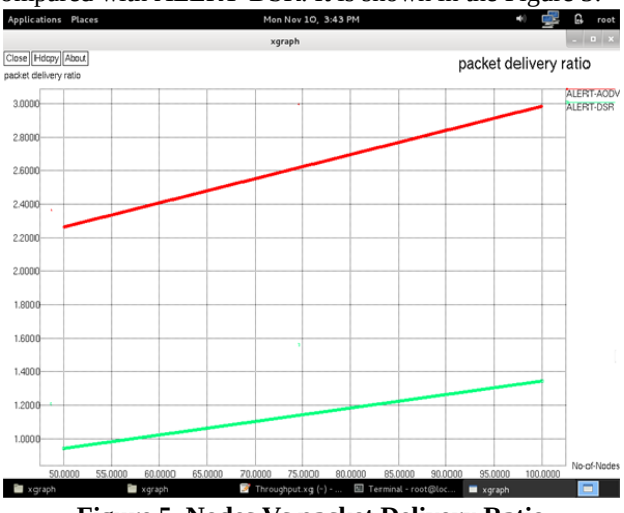

Figure 5. Nodes Vs packet Delivery Ratio

Conclusion and Future Work

Existing anonymous routing protocols, relying on either hop-by-hop encryption or redundant traffic, create high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. ALERT is familiar 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 tricky 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 communications for destination anonymity. In addition, ALERT has an efficient solution to counter intersection attacks as well as timing attacks. Experiment results show that ALERT can offer high anonymity protection at a low cost when compared to other anonymity algorithms. Future work lies in reinforcing ALERT in an attempt to prevent stronger and active attackers.

Acknowledgment

First of all I would like to extend my sincere gratitude to my supervisor Mr.K.Logeswaran for providing me the opportunities of taking the part in Master of Information Technology Program and his ideas and suggestions, which have been very helpful in the project. I am so deeply grateful for his help professionalism and valuable guidance throughout this project.

References

[1] 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.

[2] 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.

[3] 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.

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

[6] Y.-C. Hu, A. Perrig, and D.B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Wireless Networks, vol. 11, pp. 21-38, 2005.

[7] Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] J. Raymond, "Traffic Analysis: Protocols, Attacks, Design Issues, and Open Problems," Proc. Int'l Workshop Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability (WDIAU), pp. 10-29, 2001.

[13] B. Zhu, Z. Wan, M.S. Kankanhalli, F. Bao, and R.H. Deng, "Anonymous Secure Routing in Mobile Ad-Hoc Networks," Proc. IEEE 29th Ann. Int'l Conf. Local Computer Networks (LCN), 2004.

[14] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[15] A.R. Beresford and F. Stajano, "Mix Zones: User Privacy in Location-Aware Services," Proc. IEEE Second Ann. Conf. Pervasive Computing and Comm.Workshops (PERCOMW), 2004.

[16] 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.