Survey on Efficient and Secure Anonymous Communication in Manets

Roshin Pushpan
MES College of Engineering
Kuttippuram, India

Neena Susan Alex
MES College of Engineering
Kuttippuram, India

Abstract: Mobile ad-hoc networks require anonymous communications in order to thwart new wireless passive attacks; and to protect new assets of information such as nodes locations, motion patterns, network topology and traffic patterns in addition to conventional identity and message privacy. The transmitted routing messages and cached active routing entries leave plenty of opportunities for eavesdroppers. Anonymity and location privacy guarantees for the deployed ad hoc networks are critical in military and real time communication systems, otherwise the entire mission may be compromised. This poses challenging constraints on MANET routing and data forwarding. To address the new challenges, several anonymous routing schemes have been proposed recently.

Keywords: Mobile ad-hoc networks, Anonymity, Routing protocol, Geographic routing, Military communication Network Security.

1. INTRODUCTION

High Security and privacy in ad-hoc networks has been a major issue, while it comes in the field of defense and other such sensitive communications. Most of the communication system provides security in routing and data content. But a secure anonymous communication is not possible just by securing the routing map or data contents. Anonymous communications should focus on anonymity in identity, location and route of the participating nodes. The paper performs an extensive literature survey of various existing anonymous protocols in Manets

Anonymous communication between the Manet nodes are challenging as the nodes are free to move anywhere. No centralized node is there to monitor or to control the other nodes. Here the chance of attack from foreign/malicious nodes is high. Anonymous communication guarantees that no malicious nodes should identify (1) from where the communication starts (2) where it terminates (3) path of communication. Since mobile ad-hoc networks change their topology frequently and without prior notice, routing is a challenging task. Two approaches are used: Topology based and Position based routing. Topology based routing protocols use the information about the links that exist in the network to perform packet forwarding, while in Position based routing algorithms eliminate some of the limitations of topology based approach by using information about the physical position of the participating nodes. This approach doesn't require the establishment or maintenance of routes and nodes have neither to store routing tables nor to transmit messages to keep routing tables up-to-date.

2. LITERATURE SURVEY

Researchers are always being conducted to improve the security and efficiency of the anonymous routing algorithms. Focussing on the basic conditions for the anonymity, an extensive literature survey was made to analyse whether they are providing the anonymity in-

communication. Some of the innovative approaches to anonymity are described.

2.1 ANODR (Anonymous On demand Routing)

ANODR, one of the first anonymous routing schemes for mobile ad-hoc networks [1]. ANODR is a unicast anonymous MANET routing protocol. ANODR is identity i.e. it does not use the nodes' identities but it exploits a route pseudonymity approach to address the route untraceability problem. It uses a trapdoor boomerang onion encryption while forwarding route requests.

2.2 ASR (Anonymous Secure Routing)

The functionality of the ASR[2] protocol proposed by Zhu et al is essentially the same as that of ANODR. ASR makes no use of onion encryption as in ANODR that are built up as the Route request progresses through the network, but instead relies on state information that is kept at the forwarding nodes.

2.3 AO2P(Ad-hoc On demand position based routing protocol)

A02P [10] works in the network with relatively high node densities, where the positions of destinations are the only position information disclosed in the network for routing. In A02P, route is discovered by delivering a routing request message from the source to the position of the destination. However it does not rely on the local position information exchange. In A02P, once a previous hop sends out a routing request, its neighboring nodes who receive the request will contend to access the channel to be the next hop. In the receiver contention mechanism, receiving nodes are divided into different classes according to how close they can bring the routing request towards the destination. A receiver geographically closer to the destination is assigned to a class with a higher priority, and it generally can win the contention. This results in the routes with a lower number of hops. Fewer forwarders are needed and, hence, the ad hoc channel is shared by fewer nodes. In a network with a fixed data rate, these routes generally have a better routing performance. Once a route is built, pseudo IDS and temporary MAC addresses are used for the nodes in the routes, such as sources, destinations, and intermediate forwarders. Since the node identities are not disclosed, communication anonymity can be achieved. For a destination whose position is revealed, its privacy is preserved by hiding the match between a position and its ID through the secure position management scheme. Eavesdroppers or attackers only know that a node at a certain position will receive data, but they do not know which node it is.

2.4 SDAR (Secure Distributed Anonymous Routing)

In contrast to the previously presented protocols, Boukerche et al proposed SDAR[3] which doesn't use temporary or continuously changing identities. Instead SDAR uses a single fixed identity for every node. Every intermediate node inserts its identity as the source address of every message it broadcast. It requires every forwarding node to perform a public key decryption, a public key encryption and a signature generation for every Route request message. It forwards protocol does not require the source node to gather and store information about the network topology.

2.5 ALARM (Anonymous Location Aided Routing)

ALARM [6] 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).Although it doesn't provide full security on the location anonymity of source and destination.

2.6 ALERT(Anonymous Location Based Efficient Routing)

Anonymous Location based efficient Routing Protocol in MANETs-ALERT [7] proposed by Haiying Shen and Lianyu Zhao dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a nontraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. ALERT offers anonymity protection to sources, destinations, and routes. 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[5]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. A notify and go mechanism is incorporated in order to have the source anonymity

3. PERFORMANCE ANALYSIS

A detailed analysis of the techniques seen in section II are done and based on it we have some results which can be used to determine which protocol is better suite for different Manet communication environment.

Computation costs of various existing protocols are found out. Computation costs determine the complexity of encryption/decryption computations by the nodes in each protocol. ANODR, ASR, SDAR and ALARM are analyzed for their computation cost. Results are summarized in the table 1 below.

Table 1:Computation cost of various anonymous routing protocols

Methods	Source	Destination	Intermediate
ANODR	KG+1PK(1PK)	1PK	KG+2PK(2PK)
ASR	KG+1PK(1PK)	1PK	KG+2PK(2PK)
SDAR	KG+2PK(2PK)	(L+1)*PK	KG+1PK(1PK)
ALARM	KG+2PK(2PK)	2PK	0

Numbers in brackets are computation complexity with pre-computation. L is the hops from the source to destination, KG denotes public key generation, PK denotes public key operations

Performance of some geographic routing protocols like ALERT, AO2P, ALARM are compared with GPSR [5], which is a baseline routing protocol of ALERT. In GPSR a packet is always forwarded to the node nearest to the destination. When such a node doesn't exist, GPSR uses perimeter forwarding to find the hop that is closest to destination. Here we evaluate the routing performance in terms of latency, number of hops/packets and delivery rate.

The tests were carried out on NS-2.33 simulator using standard wireless transmission range of 250 m and UDP/CBR traffic with a packet size of 512 bytes. The test field was set to a 1000 m × 1000 m area with 200 nodes moving at a speed of 2 m/s.

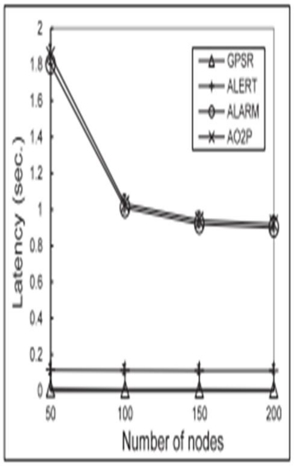

Fig 1(a): Node density

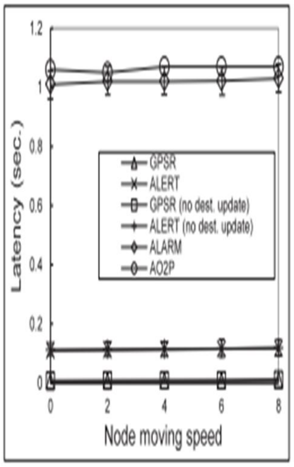

Fig 1(b): Node moving speed

Figure 1(a) shows latency per packet versus total number of nodes. ALERT doesn't take shortest path in routing, while ALARM and AO2P takes shortest path in routing. Latency of ALERT is much lower than ALARM and AO2P. Figure 1(b) shows latency versus node moving speed varies from 2 m/s to 8 m/s. ALERT produce slightly higher latency than GPSR.

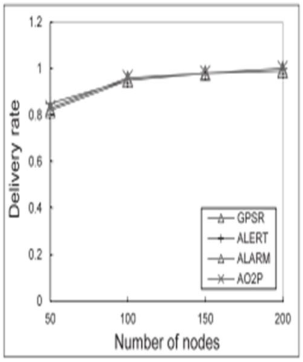

Fig 2(a): Node density

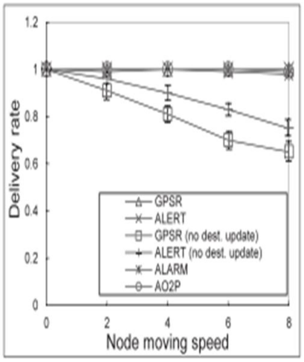

Fig 2(b): Node moving speed

Figure 2(b) presents the delivery rate versus number of nodes with destination update. We see that delivery rate of all techniques that have taken are close to 1. But in figure 2(b), there is a destination update. ALERT produces higher delivery rate than GPSR.

Comparisons are also made with the protocols to check whether they are providing the basic conditions of anonymity in communication. Analysis is summarized as the table below.

Table 2: Summary of existing Anonymous routing protocols

PROTOCOL	IDENTITY	LOCATION	ROUTE
ANODR (TOPOLOGY)	SOURCE DESTINATION	N/A	YES
AO2P (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE DESTINATION	NO
ASR (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE DESTINATION	NO
SDAR (TOPOLOGY)	SOURCE DESTINATION	N/A	YES
ALARM (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE	NO
ALERT (GEOGRAPHIC)	SOURCE DESTINATION	SOURCE DESTINATION	YES

4. CONCLUSION

Anonymous routing protocols, relying on either hop by-hop encryption or redundant traffic, generate high cost. Also, some protocols are unable to provide complete source, destination, and route anonymity protection. Though many researches are going on in this field a widely accepted version of Anonymous routing protocol has yet to come. All the problems have to be solved such that a secure communication with authentic source and destination to be made in MANET environment with security considerations.

5. ACKNOWLEDGEMENTS

We express our sincere gratitude to all who help in the completion of this paper with their valuable suggestions.

6. REFERENCES

[1] X. Hong J. Kong. Anodr: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. In ACM MOBIHOC-03, pages 291-302, 2003.

[2] M. S. Kankanhalli F. Bao B. Zhu, Z. Wan and R. H. Anonymous Secure Routing in Mobile Ad-Hoc Networks. 29th IEEE International Conference on Local Computer Networks (LC04),pages 102-108, 2004.

[3] L. Xu A. Boukerche, K. El-Khatib and L. Korba. Sdar: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. In 29th IEEE International Conference on Local Computer Networks (LC04), pages 618-624, 2004.

[4] G. Yee R. Song, L. Korba. Anondsr: Efficient anonymous dynamic source routing for mobile ad-hoc networks. In ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN), 2005.

[5] H. T. Kung Brad Karp. Gpsr: Greedy perimeter stateless routing for wireless networks. In MobiCom, 2000.

[6] K.E. Defrawy and G. Tsudik. Alarm: Anonymous location- aided routing in suspicious manets. In Proc. IEEE Intl Conf. Network Protocols (ICNP), 2007.

[7] Lianyu Zhao Haiying Shen. Alert: An anonymous location-based efficient routing protocol in manets. In IEEE Transactions on mobile computing, vol 6,no.12, 2013.

[8] Z. Zhi and Y.K. Choong. Anonymizing geographic ad hoc routing for preserving location privacy. In Proc. Third Intl Workshop Mobile Distributed Computing (ICDCSW), 2005.

[9] D.B. Johnson Y.-C. Hu, A. Perrig. Ariadne: A secure on-demand routing protocol for ad hoc networks. In Wireless Networks, vol. 11, pp. 21-38, 2005.

[10] Xiaoxin Wu and Bharat Bhargava AO2P: Ad-hoc On-Demand Position-Based Private Routing Protocol, Computer Science