ISSN: 2321-7782 (Online)

Volume 2, Issue 11, November 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Review on High Anonymity Protection Using ALERT Protocol for Mitigation Routing Attacks in MANETS

Pooja P. Borekar[1]
M.E. Student
Department of computer Engineering
Dr.D.Y.Patil School of Engineering & Technology
Savitribai Phule Pune University
Pune – India

Nilav Mukherjee[2]
Assistant Professor
Department of computer Engineering
Dr.D.Y.Patil School of Engineering & Technology
Savitribai Phule Pune University
Pune – India

Abstract: An anonymous communication method in MANETS is mostly classified into three type's reactive methods (on-demand), proactive methods and anonymous routing method. Further reactive routing method 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. Whereas Mobile Ad Hoc Networks (MANETs) uses various anonymous routing protocols to provide anonymity protection to data, sources and destination. However, existing anonymous routing protocols depends upon either hop-by-hop encryption or redundant traffic which results into increase in cost and low anonymity protection to sources, destination, data and routes. Hence to offer a very high anonymity protection, Anonymous Location-based Efficient Routing protocol (ALERT) is proposed. Basic idea behind ALERT is to dynamically partition the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. Experiments and simulation results have proved that ALERT provides route anonymity protection that to at lower cost compared to other anonymous routing protocol. 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.

Keywords: Mobile -Ad-Network, Anonymity Routing Protocols, Zone Partitions.

I. INTRODUCTION

In the last 10-15 years, research in various aspects of mobile ad-hoc networks (MANETS) has been very active, motivated mainly by allegedly important and numerous applications in law enforcement, military and emergency response scenarios. MANET is self-configuring, self-organizing and infrastructure less network which consist of number of mobile nodes connected without wires. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission. A mobile ad hoc network is an autonomous collection of mobile devices (laptops, smart phones, sensors, etc.) that communicate with each other over wireless links and cooperate in a distributed manner in order to provide the necessary network functionality in the absence of a fixed infrastructure.

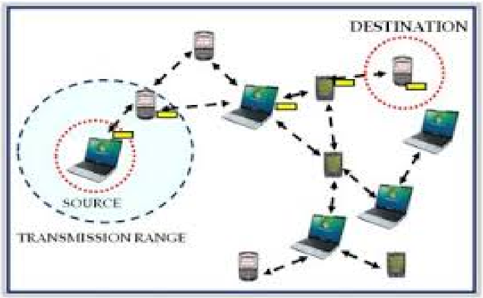

Fig 1: Overview on MANET.

The vital characteristic of MANET is that the dynamic nature of its constellation which might be often modified attributable to the unpredictable quality of nodes.

Furthermore, every mobile node in MANET plays a router role whereas transmission knowledge over the network. Anonymity is the state of being not identifiable8 within a set of subjects, the anonymity set. Anonymous means to hide or to be unknown to outside world. Anonymous communication methods, try to prevent traffic analysis attacks by hiding nodes' identities from outside observers. Anonymity is an important part of the overall solution for truly secure Mobile Ad-hoc Networks (MANET), especially in certain privacy-vital environments. In MANET it is very important to provide anonymity to location, identity and routes. Early routing protocols were based on either hop-by-hop encryption or redundant traffic, but these results into high cost, high traffic and low anonymity. A mobile computer is associated with environment of constrained resources. Although these constraints are becoming less noticeable with recent technological advances, the portability of a mobile computer will always induce constraints when com-pared to non-mobile computers.

For instance, battery powered mobile computers will always face power constraints relative to their fixed counterparts. Since current technology [17] also allows hardware components to be added or removed while a mobile computer is still powered on, a dynamic element is introduced to the constrained mo-bile computing environment. In such an environment of changing resource constraints, a system within-built addictiveness would either be unable to utilize newly available resources, or would fail because an expected resource is currently unavailable. Clearly, such behavior would make the system unacceptable to a user. In order to address this 2 problem, a mobile computing system must appropriately utilize available resources and alleviate the effects of changes in resource availability. A mobile computing system must also deal with dynamic network connectivity caused by heterogeneous network technologies. For example, fast connectivity of wired networks or wireless networks such as WaveL and may be available indoors, while slower cellular or CDPD connectivity may be available outdoors. Although network and transport protocols for mobile hosts [17, 18] can transparently maintain network connectivity across these technologies, they are mostly tuned to adapt and recover from transient changes in network conditions. These protocols are therefore inadequate to handle the long-term changes in network parameters that characterize connections to a mobile host.

A. MOTIVATION

Consider a scenario in which MANET is being used in battlefield. By analyzing the traffic patterns, enemies can get the original message transmitted which will lead to attacks on our solider by knowing their exact location, even getting the entire message being transmitted/blocked and attack on commander nodes. Also preventing communication from malicious entities and eavesdropping. Hence we must come up with system that provides secure communication by hiding node identities and preventing traffic analysis attacks from outside observers in MANET.

Hence ALERT is used which has various strategy to hide data initiator among a number of initiators to strengthen the anonymity protection of the source. ALERT offers with both privacy and security features, including data integrity, anonymity, tracking-resistance and also offers protection against passive and active insider and outsider attacks.

B. LITERATURE SURVEY

Existing anonymity routing protocols in MANETs can be mainly classified into two categories: hop-by-hop encryption [1], [2], [3], [4], [5] and redundant traffic [6], [7]. Most of this method results in high cost and provide with low anonymity protection. Then followed by ALARM [4] which drawback that it won't provide protection to source and destination. In many traditional mobile network scenarios, nodes establish communication on the basis of persistent public identities. However, in some hostile and suspicious MANET settings, node identities must not be exposed and node movements must be untraceable. Instead, nodes need to communicate on the basis of nothing more than their current locations. In this paper, we address some interesting issues.Arising in such MANETs by designing an anonymous routing framework (ALARM) [4].

It uses nodes' current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with. ALARM takes advantage of some advanced cryptographic primitives to achieve node authentication, data integrity, anonymity and intractability (tracking-resistance). It also offers resistance to certain insider attacks.

Further SDDR [5] won't provide with route protection. All the mentioned protocols have one or the other drawbacks. We want protocol which will provide three anonymity protections like sources, destination and data. Further many routing protocol are based on geographic routing protocols like GPSR (Greedy Perimeter Stateless Routing) [11], [13] which blindly forwards the data to neighbor which is close to it. An Anonymous On-Demand Position-Based Routing in Mobile Ad Hoc Networks [1], due to the infrastructure-less, dynamic and broadcast nature of radio transmissions, communications in mobile ad hoc networks (MANETs) are susceptible to malicious traffic analysis. After traffic analysis, an attacker determines a target node and conducts an intensive attack against it, called target-oriented attack. The traffic analysis and the target-oriented attacks are known as quite severe problems in MANETs, including position-based routing protocols, with respect to the degradation of both throughput and security of the routing.

Anonym zing Geographic Ad Hoc Routing for Preserving Location Privacy [2], due to the utilization of location information, geographic ad hoc routing present's superiority in scalability compared with traditional topology-based routing in mobile ad hoc networks. However, the consequent solicitation for location presence incurs severe concerns of location privacy, which has not been properly studied. In this paper, we attempt to preserve location privacy based on the idea of dissociating user's location information with its identity. We propose an anonymous geographic routing algorithm which includes three components to avoid the explicit exposure of identity and location in communication without compromising the efficiency guaranteed by geographic routing. PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs) [18], mobile ad-hoc networks (MANETs) are particularly useful and well-suited for critical scenarios, including military, law enforcement as well as emergency rescue and disaster recovery. When operating in hostile or suspicious settings, MANETs require communication security and privacy, especially, in underlying routing protocols. This paper focuses on privacy aspects of mobility. Results show that PRISM is more computationally efficient and offers better privacy than prior work.

Anonymous Geo-Forwarding in MANETs through Location Cloaking [11], in this paper, we address the problem of destination anonymity for applications in mobile ad hoc networks where geographic information is ready for use in both ad hoc routing and Internet services. Geographic forwarding becomes a lightweight routing protocol in favor of the scenarios. 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.

In response to provide high protection and that to at low cost we propose an Anonymous Location-based and Efficient Routing Protocol (ALERT) [9]. ALERT offers with both privacy and security features, including data integrity, anonymity, tracking-resistance and also offers protection against passive and active insider and outsider attacks. Basic idea behind ALERT is to dynamically partition the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which form a non traceable anonymous route. Along with, it also hides the initiator/receiver among many initiators/receivers so as to provide high anonymity protection to source and destination. In all Anonymous Location-based Efficient Routing protocol provide protection to sources, destinations, and routes.

In summary, the contribution of this work includes:

a) Anonymous routing

b) Resilience to intersection attacks and timing attacks

c) Low cost

II. PROBLEM DEFINITION AND SCOPE

A. *PROBLEM STATEMENT*

Existing anonymous routing protocols generate high cost. It cannot provide full anonymity protection to data sources, destinations, and routes. 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.

To propose an Anonymous Location-based Efficient Routing protocol (ALERT) this offers

- High anonymity protection at a low cost,
- Anonymity protection to sources, destinations, and routes,
- Strategies to effectively counter intersection and timing attacks.

B. *GOALS AND OBJECTIVES*

- To offer high anonymity protection at a low cost.
- To provide anonymity protection to data, sources, destination and routes.
- To hides the initiator/receiver among many initiators/receivers.
- To offer with features of security, data integrity, privacy, anonymity and tracking – resistances.
- Resilience to intersection attacks and timing attacks.
- And there by provide secure and faithfully communication in MANETs.

III. EXISTING SYSTEM

Preserve location privacy based on the idea of dissociating users' location information with its identity. Scheme consists of three main components: anonymous neighbor table (ANT), anonymous greedy forwarding (AGFW), and anonymous location service (ALS).Position-based routing protocol which keeps routing nodes anonymous, thereby preventing possible traffic analysis. Evaluate the level of anonymity and performance. ALARM [4] uses nodes' current locations to securely disseminate and construct topology snapshots and forward data. ALARM provides both security and privacy features, including node authentication, data integrity, and anonymity.

Disadvantages:

1. Existing anonymous routing protocols generate high cost.
2. It cannot provide full anonymity protection to data sources, destinations, and routes.
3. 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.
4. It cannot protect the location anonymity of destination and no route anonymity.

IV. PROPOSED SYSTEM

Now assume the entire network area is generally a rectangle in which nodes are randomly disseminated. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT [15], [16].

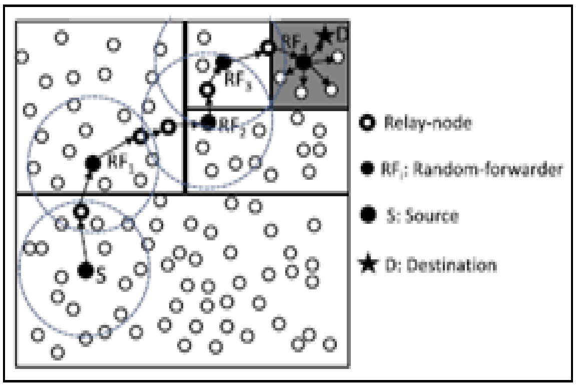

Fig 2: Routing among zones in ALERT

As shown in the upper part of Fig. 1, given an area, we horizontally partition it into two zones A1 and A2. 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. Then call this partition process hierarchical zone partition. ALERT [9] 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) [11], [13], thus dynamically generating an unpredictable routing path for a message.

A. THE ALERT ROUTING ALGORITHM

For ease of illustration, now assume the entire network area is generally a rectangle in which nodes are randomly disseminated. The information of the bottom-right and upper left boundary of the network area is configured into each node when it joins in the system. This information enables a node to locate the positions of nodes in the entire area for zone partitions in ALERT. ALERT features a dynamic and unpredictable routing path, which consists of a number of dynamically deter-mined 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. 3 shows an example of routing in ALERT. Then call the zone having k nodes where D resides the destination zone, denoted as ZD [15]. The shaded zone in Fig. 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.

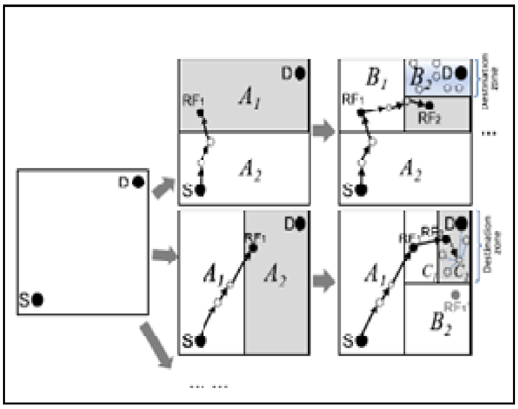

Fig 3: Examples of different zone partitions.

The node repeats this process until it and ZD are not in the same zone. It then randomly chooses a position in the other zone called temporary destination (TD), and uses the routing algorithm to send the data to the node closest to TD [16]. This node is defined as a random forwarder (RF). Fig. 3 shows an example where node N3 is the closest to TD, so it is selected as a RF.

ALERT Algorithm Steps –

- ALERT uses the hierarchical zone partition and randomly chooses a node in the partitioned zone as an intermediate relay node.
- It checks each node as in same zone or different zone.
- And choose the intermediate neighbor node as data forwarder. And checks this step until reach to the destination

Advantages:

- To offers anonymity protection to sources, destinations, and routes.
- It also has strategies to effectively counter intersection and timing attacks.
- To offer high anonymity protection at a low cost.

V. System Architecture

System architecture shows how network is partitions into various nodes like node 1, node 2 …node n. Further it will generate unique ID for source and destination node. This will further help in providing anonymity protection to sources, destination and data [9].

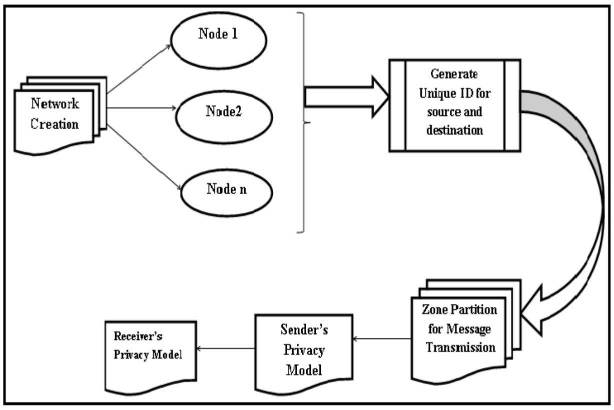
Node 1
Network Creation
Node2
Node n
Generate Unique ID for source and destination
Zone Partition for Message Transmission
Sender's Privacy Model
Receiver's Privacy Model

Fig 4: Architecture for partition of network into zones

System architecture is divided into our modules

a) Node construction

b) Zone Partition

c) Source Anonymity

d) Routing Protocol

e) Destination Anonymity

Let explain each module in short

a) Node Construction:

A node creation is making number of node in the network. We can assign the unique id for each node. Here, unique Id is used for identify the Source and Destination

b) Zone Partition:

Separate source and destination by dynamically partition the network .It will generate an unpredictable routing path for a message. Partition zone in an alternating horizontal and vertical manner. This method is called hierarchical zone partition [13].

c) Source Anonymity:

Strengthens the privacy protection for S and D by the unlinkability of the transmission endpoints and the transmitted data. Lightweight mechanism called “notify and go” is used to hide source by number of neighbors nodes send out packets at the same time as source sending.

d) Routing Protocol:

Routing is the process of information exchange from one host to the other host in a network. Routing is the mechanism of forwarding packet towards its destination using most efficient path. Efficiency of the path is measured in various metrics like, Number of hops, traffic, security, etc [12].

The Desired Properties of Protocols (For Routing)

- A routing protocol should be distributed.
- Assume routes as unidirectional links.
- Power efficient.
- Consider its security.
- Hybrid protocols can be preferred.
- decrease routing-related overhead
- find short routes

e) Destination Anonymity:

To counter the intersection attacks, in the destination zone broadcast packet to a set of m nodes out of k nodes .the m nodes hold the packet pkt1 until the arrival of the next packet pkt2.Upon receiving the next packet, the m nodes conduct one-hop broadcasting to enable other nodes in the zone to receive the packet in order to hide destination.

VI. Conclusion

In this paper, we have constructed the ALERT framework which supports anonymous location-based routing in certain types of suspicious MANETS. 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 en route. Further ALERT is an optimum solution to intersection attacks. ALERT’s ability to fight against timing attacks is also analyzed. ALERT offers with both privacy and security features, including data integrity, anonymity, tracking-resistance and also offers protection against passive and active insider and outsider attacks. ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs offer with

- Anonymous routing,
- Low cost,
- Resilience to intersection attacks and timing attacks.

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. 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.
6. I. Aad, C. Castelluccia, and J. Hubaux, “Packet Coding for Strong Anonymity in Ad Hoc Networks,” Proc. Securecomm and Workshops, 2006.
7. 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.
8. 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.
9. Haiying Shen, Lianyu Zhao, “ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs,” IEEE Transactions On Mobile Computing, Vol. 12, No. 6, June 2013.
10. 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.
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. 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.
13. 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.
14. 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.
15. T. Camp, J. Boleng, and V. Davies, “A Survey of Mobility Models for Ad Hoc Network Research,” Wireless Communications and Mobile Computing, vol. 2, pp. 483-502, 2002.
16. X. Hong, M. Gerla, G. Pei, and C.C. Chiang, “A Group Mobility Model for Ad Hoc Wireless Networks,” Proc. Second ACM Int’l Workshop Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), 1999.
17. X. Wu, “DISPOSER: Distributed Secure Position Service in Mobile Ad Hoc Networks: Research Articles,” Wireless Comm. and Mobile Computing, vol. 6, pp. 357-373, 2006.
18. K.E. Defrawy and G. Tsudik, “PRISM: Privacy-Friendly Routing in Suspicious MANETs (and VANETs),” Proc. IEEE Int’l Conf. Network Protocols (ICNP), 2008.

AUTHOR(S) PROFILE

Pooja P. Borekar received B.E degree in Computer Science and Engineering in 2013 from MIT-AOE College Savitribai Phule Pune University Pune, Maharashtra, India and pursuing the M.E. degree in Computer Networking from Dr.D.Y.Patil School of Engineering & Technology Pune, Maharashtra, India. She is doing her dissertation work under the guidance of Mr. Nilav Mukherjee Assistant Professor, Dr.D.Y.Patil School of Engineering & Technology Pune, Maharashtra, India.

Prof. Mr. Nilav Mukherjee received B.E degree in Computer Science and Engineering in 2009 from Savitribai Phule Pune University Pune, Maharashtra, India and M.E. degree in Computer Science and Engineering in 2012 from ISM Dhanbad, India. He is currently an assistant professor in the Computer Engineering Department at Dr.D.Y.Patil School of Engineering & Technology Pune, Maharashtra, India.