IJCAT International Journal of Computing and Technology, Volume 1, Issue 5, June 2014
ISSN : 2348 - 6090
www.IJCAT.org

MART: Multipath-Based Anonymous Routing Protocol in MANETs

Thejaswi D T

Computer Science and Engineering Department, Shree Devi Institute of Technology
Mangalore, Karnataka, India-574142

Abstract -Rapid development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. To offer high anonymity protection at a low cost, we propose a Multipath-based Anonymous Routing proTocol (MART) in MANETs. This protocol uses multipath routing to route packets through multiple paths, which form a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Thus, it offers anonymity protection to sources, destinations and routes. It also effectively counters intersection and timing attacks. The protocol is simulated using Network Simulator-2 and performance of the protocol is evaluated based on the average throughput and end to end delay.

Keywords **- MANET, Multipath Routing, Source Anonymity, Destination Anonymity, Route anonymity**

1. Introduction

Mobile Adhoc Network (MANET) is a collection of independent mobile nodes that can communicate to each other via radio waves. These networks can work at any place without the help of any infrastructure. The dynamical nature of the network topology increases the challenges of the design of routing protocols in such ad hoc networks. The nodes in these networks usually have a limited storage and low computational capabilities. They heavily depend on other nodes and resources for data access and information processing. But MANETs are much more vulnerable to attacks than wired network. This is because of the reasons like open medium where eavesdropping is easier than in wired network. Also dynamically changing network topology, implying that mobile nodes come and go from the network, may allow any malicious node to join the network without being detected. Routing strategies play an important role in the minimization of energy consumption during the data transmission. Thus, a reliable network topology must be assured through efficient, secure and anonymous routing protocols for these Ad Hoc networks. Mobile Ad Hoc Networks(MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. However, existing anonymous routing protocols relying on either hop-by-hop encryption or redundant traffic, either generate high cost or cannot provide full anonymity protection to data sources, destinations, and routes. The high cost exacerbates the inherent resource constraint problem in MANETs especially in multimedia wireless applications. To provide high anonymity protection (for sources, destination, and route), a Multipath-based Anonymous Routing Technique (MART) in MANET's is proposed here. MART adopts Multipath Routing thus forming a non-traceable anonymous route. Specifically, in each routing step, a data sender or forwarder applies Multipath Routing in order to provide a non-traceable anonymous route. This protocol is also resilient to intersection attacks and timing attacks.

2. Literature Survey

Mobile Ad Hoc Networks (MANETs) use anonymous routing protocols that hide node identities and/or routes from outside observers in order to provide anonymity protection. The existing anonymous routing protocols rely either on hop-by-hop encryption or redundant traffic. The packet coding [2] method aims to thwart generic attackers. Make the packets, and their headers, change at each hop to reduce traceability. But its usage is limited to high-bandwidth networks. ANODR [1]realizesroute anonymity and location privacy. But it suffers from computationally intensive route discovery process and also it is sensitive to node mobility. Ariadne [3] provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptographic operations. But a high amount of traffic is inevitably incurred in broadcasting. MASK [4] thwarts malicious

traffic analysis by passive adversaries. But is not designed for a hierarchical anonymous routing framework. Anonymous Geo-Forwarding in MANETs through Location Cloaking [5] solves the problem of destination anonymity for applications in mobile ad hoc networks where geographic information is ready for use is addressed. This technique only focuses on destination anonymity. Discount Anonymous On Demand Routing for MANET [7] achieves source anonymity and routing privacy. The aforementioned properties are achieved at the cost of reduction of some privacy guarantees. ALERT [6] was designed with a purpose to provide high anonymity protection (for source, destination and route) with low cost. ALERT is not completely bulletproof to all attacks. ALERT needs to be enhanced further in an attempt to thwart stronger, active attackers.

3. MART: Multipath-Based Anonymous Routing Protocol

MART can be applied to network models with static nodes and dynamic nodes. Consider a MANET deployed in a large field where geographic routing is used for node communication in order to reduce the communication latency. The location of a message's sender may be revealed by merely exposing the transmission direction. Therefore, an anonymous communication protocol that can provide untraceability is needed to strictly ensure the anonymity of the sender when the sender communicates with the other side of the field. Moreover, a malicious observer may try to block the data packets by compromising a number of nodes, intercept the packets on a number of nodes, or even trace back to the sender by detecting the data transmission direction. Therefore, the route should also be undetectable.

A malicious observer may also try to detect destination nodes through traffic analysis by launching an intersection attack. Therefore, the destination node also needs the protection of anonymity. In this work, 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 assumptions below apply to both inside and outside attackers:

1. Capabilities: By eavesdropping, the adversary nodes can analyze any routing protocol and obtain in- formation about the communication packets in their vicinity and positions of other nodes in the network. They can also monitor data transmission on the fly when a node is communicating with other nodes and record the historical communication of nodes. They can intrude on some specific vulnerable nodes to control their behaviour, e.g., with denial-of-service (DoS) attacks, which may cut the routing in existing anonymous geographic routing methods.
2. In-capabilities: The attackers do not issue strong active attacks such as black hole. They can only perform intrusion to a proportion of all nodes. Their computing resources are not unlimited; thus, both symmetric and public/private key cannot be brutally decrypted within a reasonable time period. Therefore, encrypted data are secure to a certain degree when the key is not known to the attackers.

3.1 Anonymous Routing

Anonymity is a property of network security. An entity in a system has anonymity if no other entity can identify the first entity, nor is there any link back to the first entity that can be used, nor any way to verify that any two anonymous acts are performed by the same entity.

3.1.1 The Adversary

There are many kinds of adversaries:

1. The receiver or the target-site
2. End servers, other users
3. Eavesdroppers
   - Global – e.g. ISP, backbone administrator
   - Partial – e.g. in a cable Internet system, all the users use the same channel and can get everyone's messages (encrypted), so an eavesdropper can perform a traffic analysis of another user.
   - Local – e.g. system administrator
4. Active attackers – an individual or a group, local or global, that can cause worse damage than just listening.

3.1.2 Types of Anonymity Protection

1. Sender anonymity: the receiver (and others) cannot know who sends the message.
2. Receiver anonymity: servers in the message path cannot know to whom the message is designated.
3. Unlinkabiliity of sender and receiver: Linkability is the possibility to link between different actions in the Internet. For example, if a specific IP address appears in several transactions, then it can be concluded that there is a connection between those transactions.
4. Publisher anonymity (broadcast).

5. Information anonymity
6. Client anonymity (in client-server systems).

Naively, there is no privacy on the Web. Browsers advertise IP address, domain name, organization, referring page, platform (OS, browser) and which information is requested. The information is available to end servers, local system administrator, and other third parties. Cookies are another violation of privacy. This motivates for the requirement of an Anonymous Routing Protocol.

3.2 Multipath Routing

Multipath routing is the routing technique of using multiple alternative paths through a network, which can yield a variety of benefits such as fault tolerance, increased bandwidth, or improved security. In a mobile wireless network, multipath routing provides an effective way to recover from frequent network failures, balance load and energy resources among network nodes, and allow more secure and resilient data transmission. In an ideal network, a source always knows how to reach the destination, and the network connection is always reliable. In a wireless mobile network, or an ad hoc network, a source needs to update the location of the mobile destination and intermediate nodes constantly, and network connections may break frequently due to the changing network topologies and unreliable wireless connectivity.

Routing is a major challenge in wireless mobile environment. Mobility renders standard Internet routing methods inappropriate. Typically, ad hoc networks operate on wireless links with limited bandwidth and transmission range, and the nodes constituting the network often operate off batteries, placing a further premium on efficient operations. Clearly, handling mobility demands protocols that have higher resiliency in the face of rapidly changing network topologies. Such resiliency can be achieved by using multipath routing solutions, which create several redundant routes for a source-destination pair. If one route fails, a backup route will still be available.

Combined with on-demand approaches, multipath routing can handle mobility efficiently by tracking intermediate nodes and destinations only when necessary. The combined approach offers a greatly reduced route recovery time when a main route fails. In the context of ad hoc networking, all the classical applications of multipath routing still apply, but ad hoc multipath routing provides additional benefits. First, in a mobile environment, a pre-established route is likely to break often, and reducing the failure recovery time by having standby alternative routes can significantly affect the QoS perceived by end users. Alternating paths to transmit information can also spread the energy use among network nodes and prolong the battery life for the ad hoc network as a whole.

In addition, transmitting encrypted data across multiple routes can significantly reduce the likelihood of man-in-the-middle, replay, and eavesdropping attacks. This property is especially important in mobile environments, since wireless communication is inherently more vulnerable to security failures.

3.3 Protocol Description

3.3.1 Global Overview

A reliable network topology must be assured through efficient, secure and anonymous routing protocols for MANETs. An energy efficient multipath routing protocol can be used to overcome this problem. Multipath routing establishes multiple paths between the source-destination pair. Classical multipath routing has been explored for two reasons. The first for load balancing; the traffic between the source and destination is split across multiple disjoint paths. The second use is to increase likelihood of reliable data delivery. In this work we describe MART, an efficient way in which we can achieve source, destination and route anonymity using multipath routing along with economical utilization of energy. The model proposed in this work uses multipath for data transmission. The Ad hoc On-demand Multipath Distance Vector (AOMDV) [10] multipath routing protocol is utilized for this purpose. The data is propagated using the Greedy technique in multipath scenario.

AOMDV [10] is overridden combined with Greedy Perimeter Stateless Routing (GPSR) to provide anonymity protection. The multiple path is used to send the data in multiple direction. The multipath concept in traditional network is used as a backup path. Here, the concept is overridden to extend the routing scheme for anonymity protection. The greedy techniques describe the selection of next hop, here it reduces the number of hops in reaching the destination. Thus forming a nontraceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthen source and destination anonymity protection. Hence, MART offers anonymity protection to sources, destinations, and routes. It also counters intersection and timing attacks effectively. MART is analysed in terms of anonymity and efficiency. Experimental results exhibit consistency with the analysis, and show that MART achieves anonymity of source, destination and route to greater extent.

3.3.2 Source Anonymity

The source address needs to be masked or hidden for the purpose of anonymity protection of the node initiating the communication with another node (destination). Hash algorithm is used for this purpose. The algorithm works as follows. An initial vector is selected and predefined. The source address is XORED with the initial vector, termed as IV_0.

Source Address (SA) $\oplus$ IV_0 = Hashed value of Source Address

This results in a hashed value of the source address. This value is used during route request and route response stages. During the process of packet transmission, the source address is hashed for every new packet. The source address for the first packet is XORED once with the initial vector. The initial vector XORED with itself gives a new initial vector say IV_1. The second packet is placed with the source address value that is XORED with IV_1. The IV_1 is XORED with IV_0 giving IV_2. This IV_2 is used to XOR the source address and placed in the third packet and so on.

$Packet_1$ :: SA $\oplus$ IV_0
$Packet_2$ :: SA $\oplus$ IV_1
[$IV_0 \oplus IV_0 = IV_1$]
$Packet_3$ :: SA $\oplus$ IV_2
[$IV_1 \oplus IV_0 = IV_2$]
……
……
…….

$Packet_n$ :: SA $\oplus$ IV_{n-1}
[$IV_{n-2} \oplus IV_0 = IV_{n-1}$]

Thus, the procedure hides the source address in every packet, thus concealing from any kind of adversaries (internal or external). The entities eavesdropping or part of the system trying to capture the communication details, can never extract the source address details, as the initial vector chosen is totally a private information. Every packet' source address' hashed value is different from its previous packet and next source address' hashed value. The adversary is also oblivious to the fact of the total count, of source address, being XORED with the initial vector. Every intermediate node is also unaware of the initiator of communication, since it does not have sufficient information as to recognise that the route request or packet coming from the previous node is the source. The outcome of this is high anonymity protection to data initiator of the communication taking place.

3.3.3 Destination Anonymity

The destination anonymity is achieved by applying the SHA-1 [9] hash algorithm and the Message Digest 5 (MD 5) on the destination address. First the destination address is hashed using the SHA-1 [9] hash algorithm. The destination address is hashed with the predefined Initial Vector (IV0).

Destination Address (DA) $\oplus$ IV0 = Hashed Value of DA (DA_{hash})

Then MD5 [8] is applied to the hashed value of the destination address (DA_{hash}). This gives a doubly secured destination address value to be placed in the route request and response packets and the data packets.

$$DA_{hash} \xrightarrow{\text{MD5}} (DA_{hash})_{MD5}$$

3.3.4 Route Anonymity

The route to be taken for communicating between two nodes is carried out by the AOMDV [10] multipath routing protocol along with GPSR technique to accomplish route anonymity. The node that intends to communicate, is termed as the source node, with some specific node, termed as the destination node. The source node initiates the process by invoking the AOMDV [10] protocol. AOMDV [10] protocol procedures are carried out instantly. The route request is generated and sent to all the neighbouring nodes within the source node' transmission range or vicinity. This information regarding a node' neighbours is maintained by every node in a MANET. The selection of sending the route request to the next best intermediate node is carried by the GPSR protocol. GPSR protocol selects the next best intermediate node in a way reducing the hop counts to reach the destination, in a broadcasting fashion. This procedure is carried out until destination node reached. Once the destination reached, the route response packets are sent back across all the paths through which route request was received.

The route request once reached the source node, the source gets a list of possible paths or multipath between the source destination pair. The source now transmits the encrypted data packets in the following fashion: The first packet is sent through the first path, the second packet is As with end to end delay, the average throughput is also tabulated for the ten scenarios taken as input to the protocol, with same conditions as mentioned above. The horizontal values in the graph show the file names representing static or/and dynamic nodes with their respective average throughput achieved sent through the second path, the third packet is sent through the third path and so on. On sending the packet through the last available path, but packets are still present to transmit, the next packet in the sequence is sent through the first path

available. And this continues till the last packet is sent. If the number of packets are more than the number of multipath available, some paths may remain never used. Thus resulting in a nontraceable route between route and destination.

4. Performance Analysis

The proposed concept is simulated using Network Simulator-2. The performance evaluation is done on the basis of average throughput and end to end delay. The results show nearly to hundred percent efficiency. The analysis is carried out on the basis of predefined scenarios given as input to the protocol.

4.1 Simulation Setup

Table 4.1 : Simulation Setup

Channel type	Wireless Channel
Radio Propagation Model	Two Way Round
Network Interface Type	WirelessPhy
MAC Type	MAC 802.11
Interface Queue(IFQ) Type	PriQueue
Link Layer Type	LL
Antenna Model	OmniAntenna
Maximum Packet in IFQ	50
Number of Mobile Nodes	5,6
Routing Protocol	AOMDV
Simulation Area(m×m)	500×500

4.2 End to End Delay

There are totally ten scenarios, each one either taking five or six nodes. There are five scenarios of static nodes and five scenarios of dynamic nodes. Static nodes remain fixed during transmission. Dynamic nodes are in mobility during transmission. The packet delivery ratio is calculated, based on which the average end to end to delay is determined. This is tabulated below in the graph. The horizontal values in the graph display the specific file names used to represent static and dynamic nodes and their respective end to end delay achieved. Figure 3.1 shows the end to end delay pertained to both static and dynamic nodes

4.3 Average Throughput

As with end to end delay, the average throughput is also tabulated for the ten scenarios taken as input to the protocol with same conditions as mentioned above. The horizontal values in the graph show the file names representing static and dynamic nodes with their respective average throughput achieved. Figure 3.2 represents the average throughput for static and dynamic nodes.

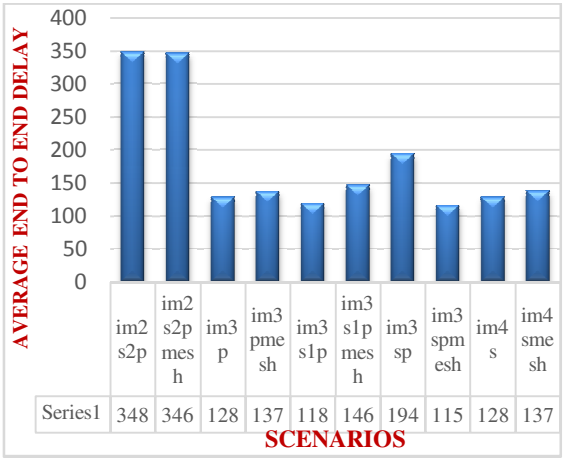

Figure 4.1: End to End Delay Static and Dynamic Nodes

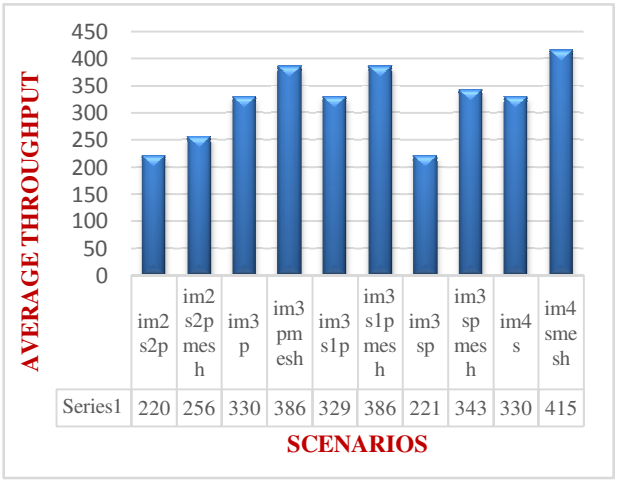

Figure 4.2: Average Throughput Static and Dynamic Nodes

5. Conclusions and Future Work

The Multipath-based Anonymous Routing protocol (MART) provides an anonymous routing technique that produces efficient results in accomplishing the aforementioned anonymity of source, destination and route, using the concept of multipath routing, that is traditionally used for the purpose of load balancing and fault tolerance in networks. The basic usage of multipath routing is overridden to achieve the purpose of the protocol. AOMDV [10] protocol is used to achieve multipath routing, used specifically for route anonymity, thus

forming non-traceable route. The source and destination anonymity achieved using hash algorithms and MD5 [8]. The analysis shows good result.

The proposed system depends on the existing multipath protocol AOMDV [10]. The dependency on AOMDV [10] incurs overhead of route request and route response. Thus the future work would be to focus on an independent or a dedicated multipath protocol for achieving source, destination and route anonymity. Another concentration would be to use a higher and still more efficient algorithm instead of SHA-1 [9] hash algorithm.better your paper looks, the better the Journal looks. Thanks for your cooperation and contribution.

Appendix: Abbreviations

MANET: Mobile Adhoc Network
MART: Multipath-based Anonymous Routing protocol
AOMDV: Adhoc On-demand Multipath Distance Vector
GPSR: Greedy Perimeter Stateless Routing
MD5: Message Digest 5
SHA: Secure Hash Algorithm
NS2: Network Simulator 2

References

[1] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.

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

[3] 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.

[4] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[5] 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.

[6] Haiying Shen and Lianyu Zhao, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," in Proceedings of the June 2013 IEEE Transactions on Mobile Computing.

[7] L. Yang, M. Jakobsson, and S. Wetzel, "Discount Anonymous On Demand Routing for Mobile Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[8] R. Rivest, "The MD5 Message-Digest Algorithm", MIT Laboratory for Computer Science and RSA Data Security, Inc.April 1992.

[9] SHA1 Algorithm, Designed by the United States National Security Agency, is a U.S. Federal Information Processing Standard published by the United States NIST.

[10] Mahesh K. Marina and Samir R. Das, "Ad hoc On-demand Multipath Distance Vector routing", Wireless Communications and Mobile computing. Published online in Wiley InterScience.

[11] Rakesh Kumar, Piush Verma, Yaduvir Singh, "Mobile Ad Hoc Networks and Its Routing Protocols", International Journal of Computer, Information Science and Engineering Vol:7 No:8, 2013.

Thejaswi D.T.B.E. Information Science 2009, M.Tech Computer Science and Engineering 2014. Worked as a Trainee Engineer in ABB GISL, Bangalore, from 2009 to 2010. Worked as a Lecturer in Computer Science and Engineering Department of Canara Engineering College, Benjanapadav, Mangalorefrom 2010 to 2011.