Tenable On-Demand Steering Protocol in System

T. Saravanan, G. Saritha and R. Udayakumar

1Department of ETC, Bharath University, India
2Department of EEE, Sathyabama University, Chennai, India
3School of Computing Sciences, Bharath University, Chennai, India

Abstract: Security in communication is becoming an essential requirement in ad-hoc networks. Secure communication is decisive due to mobility of nodes and its wireless nature. Various schemes are proposed for stronger privacy protection in Mobile ad-hoc network. These schemes offer unlinkability and anonymity, since no other protocols has a property of complete unobservability. In this paper we made a detailed theoretical study on efficient unobservable routing scheme that provides complete unlinkability and content unobservability for data packets and control packets. The brief analysis is made on some of the existing routing schemes and analyzed the unobservable routing scheme is efficient, it assures high packet delivery ratio and average packet delivery latency.

Key words: MANET • On demand Routing Protocols • Review Analysis • Optimization • Performance Metrics

INTRODUCTION

Mobile ad-hoc networks - A MANET is a type of ad hoc network that can change locations and configure itself on the fly. It is also known as wireless mesh network in which the mobile are connected by wireless link. The independent mobile nodes communicated to each other directly or indirectly through radio waves [1, 2].

Secrecy preserving in mobile ad-hoc networks is more essential than in wired environment because of its both static and dynamic topologies with increased dynamics due to nodemotion or other factors. Comparing with wired networks it is hard to gain the access of the cable and there is no mobility in the network. Providing secrecy preservation in MANET is a very challenging task [3, 4].

In mobile ad-hoc networks, preserving the secret during the communication of nodes in the network are empathize to three terms. They are as follows

- ANONYMITY
- UNLINKABILITY
- UNOBSERVABILITY

Anonymity: In the network, the node are not identifiable which refers to the anonymity. The sender, receiver and intermediate nodes are not known to other nodes.

Unlinkability: The nodes are protected from the outsider.

Unobservability: Data packets from all nodes are similar and they are not distinguishable from other packet.

Secured routing in MANET is accomplished by implementing the above factor in all the nodes of the network. In MANET all the nodes act as the host as well as the routers and nodes are interdependent to each other. Thus secured routing is one of the tor importance for the structure of MANET. The main objective of this paper is to analyze and to have a brief knowledge about various secure on demand routing protocols from different researches papers [5, 6].

Classification of On Demand Routing Protocol:
Classification of on demand routing protocols is based on routing strategy and network structure. On demand routing protocol are source initiated protocols. When the

Corresponding Author: T. Saravanan, Department of ETC, Bharath University, India.
Fig. 2: Classification of Routing Protocols

Fig. 3: Cluster Based Routing Protocol

node needs a route to destination, source will initiate a route discovery process and establish the route. Once the route is established route discovery process is completed and the routine for route maintenance keep tracks the authentic nodes and false nodes. The route remains valid till the destination is reachable or until the route is no longer needed [7, 8].

The classification of on demand routing protocol are based on the routes created and broadcasting the packets. A few on demand routing protocols are Cluster Based Routing Protocol (CBRP), Ad hoc On-demand Distance Vector Routing (AODV), Dynamic Source Routing Protocol (DSR), The Temporally Ordered Routing Algorithm (TORA), Associativity Based Routing (ABR).

Cluster Based Routing Protocols: The nodes are divided into clusters. The cluster are formed on the basis of algorithm and one of node acts as the cluster-head. A cluster-head keeps information about the members of its cluster and also maintains a cluster adjacency table that contains information about the neighboring clusters. When the node enters the cluster it starts its timer and it broadcast the messages [9, 10].

In CBRP, routing is done using source routing. It also uses route shortening that is on receiving a source route packet, the node tries to find the farthest node in the route that is its neighbor (this could have happened due to a topology change) and sends the packet to that node thus reducing the route [11-12]. While forwarding the packet if a node detects a broken link it sends back an error message to the source and then uses local repair mechanism. In local repair mechanism, when a node finds the next hop is unreachable, it checks to see if the next hop can be reached through any of its neighbor or if hop after next hop can be reached through any other neighbor. If any of the two works, the packet can be sent out over the repaired path.

Ad hoc On-Demand Distance Vector Routing: It is a reactive routing protocol, meaning that it establishes a route to a destination only on demand. In contrast, the most common routing protocols of the Internet are proactive, meaning they find routing paths independently which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route.
request packet. As the route reply packet traverses back
to the source the nodes along the path enter the forward
route into their tables. If the source moves then it can
reinitiate route discovery to the destination [15, 16]. If one
of the intermediate nodes move then they moved nodes
neighbour realizes the link failure and sends a link failure
notification to its upstream neighbors and so on till it
reaches the source upon which the source can reinitiate
route discovery if needed.

**Dynamic Source Routing Protocol:** The Dynamic Source
Routing Protocol is a source-routed on-demand routing
protocol. A node maintains route caches containing the
source routes that it is aware of. The node updates entries
in the route cache as and when it learns about new routes
[11, 17].

The two major phases of the protocol are: route
discovery and route maintenance. When the source node
wants to send a packet to a destination, it looks up its route
cache to determine if it already contains a route to the
destination. If it finds that an unexpired route to the
destination exists, then it uses this route to send the
packet. But if the node does not have such a route, then
it initiates the route discovery process by broadcasting a
route request packet. The route request packet contains
the address of the source and the destination and a
unique identification number [18]. Each intermediate
node checks whether it knows of a route to the
destination. If it does not, it appends its address to the
route record of the packet and forwards the packet to its
neighbors. A route reply is generated when either the
destination or an intermediate node with current
information about the destination receives the route
request packet [Johnson 96]. A route request packet
reaching such a node already contains, in its route record,
the sequence of hops taken from the source to this node.

**Associativity Based Routing:** ABR defines a new metric
for routing known as the degree of association stability.
It is free from loops, deadlock and packet duplicates. In
ABR, a route is selected based on associativity states of nodes. The routes thus selected are liked to be
long-lived. All node generate periodic beacons to signify
its existence [19]. When a neighbor node receives a
beacon, it updates its associativity tables. For every
beacon received, node increments its associativity tick with respect to the node from which it received the
beacon. Association stability means connection stability
of one node with respect to another node over time and
space. A high value of associatively tick with respect to
a node indicates a low state of node mobility, while a low
value of associativity tick may indicate a high state of
node mobility. Associativity ticks are reset when the
neighbors of a node or the node itself move out of
proximity. The fundamental objective of ABR is to find
longer-lived routes for ad hoc mobile networks. The three
phases of ABR are Route discovery, Route reconstruction
(RRC) and Route deletion.

The route discovery phase is a broadcast query and
await-reply (BQ-REPLY) cycle [4]. The source node
broadcasts a BQ message in search of nodes that have a
route to the destination. A node does not forward a BQ
request more than once. On receiving a BQ message, an
intermediate node appends its address and its
associativity ticks to the packet.

**Analysis of Secured Efficient On Demand Routing
Protocols:** A survey is made on several on demand
routing protocols of MANETs and analyzed them for its
fast delivery rate and secured transmission. Due to the
nodes mobility in the network the security is important for
each individual nodes. In an attempt to enhance security
in MANETs many researchers have suggested and
implemented new improvements to the protocols and
some of them have suggested new protocols. Some of
the protocols are analyzed not only to improve the fast
transmission and also to increase the speed in the packet
transmission [20].

**Related Work:** In this section, we analyse a brief
description of secured on demand routing protocols in
MANET. These following protocol uses Public key
cryptosystem for providing security in the nodes and data
packets [8].

**Anonymous On Demand Routing (ANODR) Protocol:**
ANODR protocol in mobile adhoc networks works to
deploy the hostile environments. This protocol is
proposed for two problems (i) Route anonymity and
(ii)Location privacy. The design of this protocol is based
on the broadcasting and trapdoor information. These two
design approaches are mainly for existing network
and security mechanism. From the study of this
protocol it provides unlinkability and partial
unobservability. The route anonymity is implemented for
untraceable route discovery. This is implemented for
anonymous route discovery and an different approach for
route anonymity. The location privacy is designed for
unlinkability. The nodes identity and its location are not
identified by other nodes.
**Drawbacks:** The performance of Anonymous On Demand Routing (ANODR) protocol is low when compared to other protocols due to the mobility of nodes in the network. This protocol ensures unlinkability and partial unobservability. The node intrusion is avoided but the nodes and intermediate node are viewed by the eavesdropper.

**Anonymous Secure Routing (ASR) Protocol:**
Anonymous Secure Routing (ASR) protocol defines requirements on the anonymity and security properties of the routing protocol in Mobile ad-hoc networks. ASR provides additional security by implementing the anonymous node identity and secured route discovery from both the active and passive attacks. From the analysis it shows ASR provides anonymity and satisfy the requirement of security in the mobile ad-hoc networks. The identity privacy, location privacy and anonymous route discovery are the approaches to design the anonymous secure routing. The nodes identity and the location of the nodes are unknown to other nodes and the location of the nodes is also not known to other nodes. Anonymous Route discovery is based on traffic analysis. This protocol ensures the anonymity and security mechanism are achieved and efficiency in performance is achieved compared to the previous protocols.

**Drawbacks:** These methods use some security mechanism which are sometimes having Denial Of Service (DOS) in hop by hop. The Wormhole attacks are possible when there are temporal leashes or the geographical leashes occur. The performance of the routing protocols should be improved when the route changes since it is anonymous. It can have extended functionality in anonymity and security.

**Anonymous Routing Protocol with Multiple Routes (ARMR):** Anonymous routing protocol establishes multiple route using bloom filter in order to decrease the difficulty of traffic analysis and to avoid broken paths due to node mobility. It also creates some fake path to confuse the adversaries and to increase the level of anonymity. This protocol is implemented to anonymity in the mobile ad-hoc network. The anonymity is designed using cryptographic key exchange algorithm and the hash function algorithm. They are implemented as key exchange between the nodes. In addition to the anonymous route discovery which includes route request and route reply, Anonymous fake routes are also made to confuse he intruders in the network. The approach described here are Node identity, Location identity and route identity to identify from fake route. ARMR protocol ensures the anonymity and security in the routes of the network.

**Drawbacks:** The ARMR are vulnerable to DOS attacks. These protocols needs authenticate Route Request to each node. Sometimes a redundant transmission may occur in fake route which will flood the network even though it cannot be obtained by intruders. Hence there is no unlinkability and no unobservability is achieved. The analyzes shows security features does affect the communication and hence it enhanced.

**A Secure Distributed Anonymous Routing (SDAR) Protocol:**
A Secure Distributed Anonymous Routing Protocol (SDAR) proposes a novel distributed routing protocols that assures the security, anonymity, reliability in route establishment. This protocol uses one time private/public key for nodes key exchange. The Protocol works on the trustworthiness of the intermediate nodes for anonymous route establishment with its neighbouring nodes. This protocol proposes three phases (i) Path discovery phase (ii) Path reverse Phase and (iii) Data transfer phase. The main features of this protocol are Non-Source based routing, Non-Source control over route length and Resilience against Path Hijacking. SDAR is secured from passive and active attacks. It can easily identify the malicious code and the trust requirement for a node to qualify the trust value between the nodes. Hence the security is achieved.

**Drawbacks:** SDAR protocol has DOS attack. This protocol achieves security and anonymity and it does not support unlinkability and unobservability.

**On-Demand Anonymous Routing (ODAR) Protocol:**
On-Demand Anonymous Routing protocol proposes anonymity and complete unlinkability. This protocol approach defines the network, anonymity and bloom filter. It uses diffie-Hellmann algorithm to generate a long term public key. Key Server that generates the public key. The key is distributed between the nodes and the route is discovered with shared key. The node identity, forwarding node identity and route identity are anonymous. Hence the different level of anonymity are made. The performance of ODAR compared with AODV and a control overhead is achieved with public key exchange system.
<table>
<thead>
<tr>
<th>Routing Protocols</th>
<th>Metrics</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANODR</td>
<td>Traceable ratio, Average End-to-end delay</td>
<td>Increased Normalized control bytes</td>
</tr>
<tr>
<td>ASR</td>
<td>Traffic analysis</td>
<td>Increased anonymity</td>
</tr>
<tr>
<td>ARMR</td>
<td>Number of nodes flow</td>
<td>Increased communication efficiency</td>
</tr>
<tr>
<td>SDAR</td>
<td>Trustworthy anonymity</td>
<td>Increased Security and Reliable path Selection</td>
</tr>
<tr>
<td>ODAR</td>
<td>Delivery ratio, Number of Control packets</td>
<td>Improved control Overhead and reliable</td>
</tr>
<tr>
<td>MASK</td>
<td>Normalized routing load, Packet delivery ratio, Average packet delay</td>
<td>Improved packet delivery, partial delay</td>
</tr>
</tbody>
</table>

**Drawbacks:** The protocol achieves the anonymity and complete unlinkability but not the unobservability. It is vulnerable to Man in the middle attack.

**MASK Protocol:** MASK protocol is proposed for anonymous communication based on the cryptographic key exchange. The phases of protocol are anonymous neighborhood authentication, anonymous route discovery and anonymous data forwarding. It provides strong sender and receiver anonymity. It serves as a lightweight routing protocol. The performance of MASK protocol proves a secure anonymous communication compared to AODV.

**Drawbacks:** MASK protocol provides anonymity, unlinkability and partial unobservability. The analysis on the protocol shows that security is achieved but it has a DOS attack and timing analysis attack.

**Usor Protocol:** Unobservable Secured On demand Routing Protocol that satisfies all the features such as Anonymity, Unlinkability and Unobservability. It uses public key cryptosystem for secure key exchange. The algorithm used for key generation is elliptic curve discrete log problem (ECDLP) and the bilinear Diffie-Hellman problem (BDH).

It uses group signature scheme and ID based scheme for pairing. It has security strength as same of 1024 bit RSA algorithm. The phases of protocol are Anonymous key establishment, Privacy-preserving route discovery and unobservable data packet transmission. This protocol avoids the collision attack and Sybil attack. From the brief analysis the USOR protocol has a strong security, complete unlinkability and content unobservability.

**Optimization of Energy Efficiency in MANET:** An important goal of on demand routing protocol is to ensure the secured communication with anonymity, unlinkability and unobservability. Various on demand routing protocols have been analyzed and metrics that have been used to determine efficient secure routing is discussed below.

**Performance Metrics:** We calculate performance according to the following metrics [18]:

**Delay Time:** The time taken to receive the packets.

**Average End-to-end Delay:** The Averaged over all data packets from the sources to the destinations.

**Average Packet Delivery Ratio:** It is the ratio of the number of successful packets to the total number of packets sent.

**Average Packet Delay:** It is the ratio of sum of the number of successful packets from sender to receiver to the total number of successful transmission. The average packet delay is measured in seconds [19-24].

**CONCLUSION**

A Mobile Ad-Hoc Network (MANET) is a self organizing network with wireless links. Due to moving nature in the network, security is becoming a challenging task in on demand routing protocols. The protocols designed for secured routing uses several techniques and various cryptographic algorithms. In this paper, we analyzed and classified various on demand routing schemes and each has its own features. The analysis show that most of the protocol has its key feature anonymity. Hence the Unlinkability and Unobservability are achieved by few protocols. It is difficult to compare these protocol directly since it has different assumption and different goals. With the three key feature such anonymity, unlinkability and unobservability a secured communication is provided in on demand routing protocol of Mobile ad-hoc networks.

**REFERENCES**


