A Novel Routing Protocol for Providing Anonymity in MANET
Vignesh S¹, Sudhakar K²

¹ (P. G. Scholar, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India)
² (Assistant Professor, Department of Computer Science and Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamilnadu, India)

ABSTRACT: Mobile Ad Hoc Networks (MANETs) using anonymous routing protocols hidden node identity and external routes having anonymity protection. Anonymous routing protocols use either hop-by-hop encryption or redundant traffic, which generates more cost or without providing full anonymity protection to the data source and destination. It has more cost and increase for naturally resource constraint problem in MANETs particularly in multimedia wireless applications. High anonymity protection at a lower cost, we propose an unsigned Location-based competent Routing protocol. It dynamically partitions the network field into different zones and randomly chooses nodes in various zones as intermediate relay nodes, it also non traceable. It's based on counter intersection and timing attacks. It performs better route anonymity. It has self configuring infrastructure less networks. In future, the Random forwarder node replication attack will be also eliminated. To consider this attack, set up server will assign the key for each random forwarder node is generated by using the polynomial bivariate key generation scheme. The key wrapping algorithm used to protect the key from the adversary. In this paper, one way hash chain algorithm is used for key wrapping.

Keywords: Random forward, Anonymity, Routing protocol, key wrapping, non traceable, bivariate key.

1. INTRODUCTION

Fast development of Mobile Ad Hoc Networks (MANETs) excited numerous wireless applications that can be used in a wide number of areas. It has self-organizing and independent infrastructures, uses such as communication and information sharing, Nodes in MANETs are problem with harmful entities that aim to involve and analyze data and traffic analysis of communication or or attacking routing protocols.

Anonymity may not be a requirement in civil oriented applications and critical in the military. Consider a MANET stoped in a battleground. Anonymous routing protocols provide secure communication by hidden node identity and traffic analysis attack is prevented in outside viewer. Anonymity in MANETs includes the identity and the location anonymity of data sources, destinations as well as route anonymity. Same and site anonymity of sources and destinations means it is difficult to possible for other nodes to obtain the real identities and correct locations of the sources and destinations. Anonymity routing protocols have two types of hop-by-hop encryption and redundant traffic.

It was partitioned network into different zones and randomly select node, which are non traceable anonymous route. Forwarder node partitions in network separate two zones. Random selection of node other zone into next relay node uses GPRS algorithm for sending data in relay nodes.

2. RELATED WORK

We address some interesting issues arising in such MANETs by designing an anonymous routing framework. It uses nodes’ current locations to construct a secure MANET map. We consider what it takes to provide secure communication in hostile and suspicious MANETs. To this end, we construct a framework for Anonymous Location-Aided Routing in MANETs which demonstrates the feasibility of obtaining, at the same time, both strong privacy and
strong security properties. By privacy properties we mean node anonymity and resistance to tracking whereas, security properties include node or origin authentication and location integrity.

First define stricter requirements on the anonymity and security properties of the routing protocol in mobile ad-hoc networks. Following that, we propose the Anonymous Secure Routing (ASR) protocol that can not only protect the privacy of nodes and routes, but also ensure the security of discovering routes. Afterwards, detailed analysis is given to show that ASR can ensure anonymity and security of the routing protocol against known passive and active attacks.

2.1 MODELS OF ATTACK AND NETWORKING

The network model has different models for simulating the movement of nodes such as a random way point model and group mobility model. The routing performs a user to node communication in order to reduce communication latency. The message location of the sender is used to identify the transmission direction. Therefore, a communication protocol, which is untraceable is required to severely ensure the anonymity. The sender when the communication of sender with the other side of the field. A harmful observer will try to chunk the data packets by compromising a different number of nodes, interrupt the packets on a number of nodes, or even mark out back to the sender by detecting the direction of data transmission.

If the routes are not detectable, the harmful observer will not be able to find destination nodes through traffic analysis to launch an intersection attack. The destination of a node is made anonymous and powerful nodes pretend to be genuine nodes and insert packets to the network, according to the critical results from their eavesdropped packets.

2.2 ZONE PARTITIONING

Zone partition having randomly selected nodes. It refers to two zones such as upper left and bottom-right coordinates of zones. Horizontally partition the network area into two zones Z1 and Z2. We then vertically partition zone Z2 to Z2 and Z3. If the horizontal partition split into two zones. The partition having a number of zones continuously for horizontal and vertical process.

![Zone partitioning nodes](image)

Fig. 1 Zone partitioning nodes

Every data source or forwarder to execute zone partition in horizontal. It first to check destinations are in the same node. If the zones are divided into alternatively horizontal and vertical direction. It cannot be same process is to be repeated. MANET has rectangular and K number of nodes. The ‘k’ nodes are distributed by the density $p$ in the MANET. The rectangular area is divided into a number of zones.
\[ H = \log_2 \left( \frac{\rho G}{k} \right) \]

Here \( G \) is the size of the entire network area. Given an S-D pair, the partition pattern in the ALERT varies depending on the randomly selected Temporary Destinations and the order of horizontal and vertical division, which provides an improved anonymity defense. The nodes of each Zone are colored to differentiate the node partition. The Random Forwarder (RF) node is obtained using the random function and hence routing takes place.

### 2.3 SELECTION OF RANDOM FORWARDER NODE

The routing is performed from source to destination, usually using the relay nodes in any network. In ALERT, a Random Forwarder Node is selected in each zone using which routing is done to the destination.

There is an advantage of using random selection of a forwarder node; anonymity is provided to the route. Each RF node updates its current details as the source details while forwarding the data. The use of random function is implemented during the selection of the Random Forwarder node. The route anonymity due to chance communicate node selection in the ALERT prevents an interloper from intercepting packets or compromising weak nodes.

If the routes between two communicating nodes are constantly changing process, so it is not easy for adversaries in an expect the route of the next packet for packet interception. It has sufficient number of nodes perform in the destination node. The number of random forward having different zone partition. The maximum number of partition for a source and destination pair. RF to be increase and linearly number of partitions increase. Route having higher anonymity production two end point. The zones for random forward having smaller to smaller. The random forward are decrease if the anonymity protection is enhanced which are decrease the speed.

---

**Fig. 2 Random Forward**

### 2.4 ANONYMOUS ROUTING

It same and site anonymity of the source and destination, as well as path anonymity which always takes the direct path. Routing makes the path between an S-D join up not easy to discover by accidentally and energetically selecting the convey nodes. The resultant different routes for transmitting between a given S-D pair make it difficult for an interloper to observe a numerical pattern of transmission.

This is because the RF set changes due to the random range of RFs during the transmission of each packet. Even if a rival detects all the nodes between S and D, this detection with not help in finding the routes for successive transmissions between the same S-D pair.
Fig. 3 Routing Nodes

Since a RF is only aware of its going on node and subsequent node in route, the source and destination nodes with not be differentiate from other nodes en route. Also, the anonymous path between S and D ensures in the nodes on path can not know where the closing stages.

Routing strengthens the time alone protection for S and D by using the unlinkedle communication end points and then transmit data. That is, S and D without be connected with the packets in their contact by adversaries. Routing incorporates the “report and go” mechanism to stop an intruder from identifying which node within the source zone has initiated packets. It also provides k-anonymity to destinations by defeat D among k receivers in ZD. Thus, an eaves dropper can only obtain in turn on ZD, rather than the destination position, from the packets and nodes en route.

2.5 POLYNOMIAL BIVARIATE KEY GENERATION

The bivariate polynomial is generated by using the following equation. The polynomials have the property of $P(a, b) = P(b, a)$.

$$P(a, b) = \sum_{0 \leq i \leq t} c(ij)a^ib^c$$

Where,

$C(ij)$ denotes communication cost

$a, b$ denote the node ID

The identification number is added with each polynomial to differentiate the polynomials. For each node in the MANET, we preload the subset of $n$ polynomials from polynomial pool. For each polynomial share preloaded in a node $m$ is $P(a, b)$.

2.6 REPLICATION ATTACK

The mobile node is captured physically by some adversary. Once it is captured, adversary collects all the credentials like key and identity etc. The attacker can reprogram it and replicate the node in order to replace eavesdrop the transmitted messages or compromise the functionality of the network. These replication attackers are found inside the MANET environment considered. We create replication attackers by using this attack description as a model.

2.7 ROUTING ALGORITHM

The GPSR direction-finding algorithm with a strict node range cannot supply anonymity, since adversaries cannot simply monitor the nodes in the map-reading path. The “network (include id dissemination hops)” generate notably elevated hops per packet than others, which is double of that of ALERT. This result verifies the spectacularly high cost of superfluous traffic for anonymity in network.

3. PERFORMANCE EVALUATION

In this section, we provide untried assessment of the routing protocol, which exhibit steadiness with our diagnostic results. Both prove the bigger recital of high in provide anonymity with low cost of slide. Recall that unsigned routing protocols can be classified into hop-by-hop encryption and disused traffic. We compare Packet with two recently planned anonymous geographic routing protocols: AO2P [10] and protocol [5], which is based on hop-by-hop encryption and unneeded travel, respectively. All of the protocols are geographic steering, so we also compare ALERT with the baseline routing protocol. In GPSR, a packet
is always forward to the node bordering to the destination. Edge forwarding is used to find the hop that is the nearby to the destination. In ALARM, each node sometimes disseminates its own identity to its authentic neighbors and constantly collects all other nodes’ identity. Thus, nodes can build a safe map of other nodes for geographical routing. In routing, each node performs the packet by its key which is verified by the next hop en route. Such diffusion period was set to 30 s in this research. The routing of AO2P is similar to GPSR excepted.

3.1 Actual participating nodes

The symmetric encryption algorithm is GPSR and the open key encrypted. Numbers are generated erratically according to the packet size individual in the paper. Packets are encrypted whenever desirable. The encryption algorithm is single thread, running along with other parts of the experimentation on a 1.8GHz processor out of character symmetric encryption costs several milliseconds while a communal key encryption procedure costs 2-3 hundred milliseconds. We use the following metrics to estimate the routing concert in terms of helpfulness on anonymity protection and effectiveness.

3.1.2 Packet deliver ratio

Number of packet which are delivered in source to destination node. It has randomly and selected into sequence of node reaches. if the node having multicellular and group anonymity process. Forwarded node due to upper and lower zones are divide.

It access the routing due to path from shortest process. If the number of packets are received to the routing algorithm. source and destination having number of random nodes are transmitted. It has sequence number of packets are allowed in the .ion process protect.

Fig. 4 Actual participating nodes

Fig. 5 Packet deliver ratio

CONCLUSION

Various network models with various node group patterns such as chance way point form and cluster mobility model. Consider a MANET deploy in a huge field where geographic routing is used for node statement in organizes to reduce the message latency. An anonymous message protocol that can provide untraceability is needed to stringently ensure the anonymity of the sender when the sender communicate with the other side of the field Protocol further strengthen the anonymity, security of source and destination by defeat the data inventor/receiver among a number of data initiators/ receiver.
REFERENCE


