RSINER: Randomised Selection Of Intermediate Nodes For Efficient Routing In MANET

Mr.Madhusudhan H , Ms.Arudra A

Abstract : MANET Mobile Ad Hoc Network is equipped for each and every device in the network to maintain the information required for the proper route that does not create the traffic issues. One such issues can raise to forming the proper path from one device to the other. Usual way of routing in MANET is followed by hop-by-hop way of fashion or the route can be formed by considering the anonymity location in the network. This both way of route is easily vulnerable for accessing the data from the third party. Where in ,the hop-by-hop fashion always consider the same node for each and every time to transfer the data which can be easily opened for attack. Where as the anonymity location route for data transfer does not provide the security as well as protection and privacy between the two devices. And hence to overcome this we introduce RSINER were it partition the network in to zones consisting of different nodes and one node from each zone acts as a relay node and start to transmit the data to the other zone ,where as the node in the opponent zone also consists of relay node that accepts the data. But the existing routing and anonymity protocols does not provide any sort of security or the protection to the relay node which is transmitting the data henceforth RSINER overcomes this complexity by offering the verification and confirmation for both the devices at two end and henceforth provides the high efficient route which drops the high cost required for data transmission.

Index Terms--Mobile ad hoc network, routing protocol, anonymity location, relay node.

---

1 INTRODUCTION

1.1What is Mobile Ad Hoc Network?

Mobile Ad Hoc Network is a self-configuring infrastructure less network of mobile devices connected by wireless. Each device in MANET is free to move independently in any direction and will therefore change its link to other devices frequently. Each must forward the traffic which is unrelated to its own use and hence forth passing the same information to the near by router. A Mobile Ad-hoc Network (MANET) is a collection of independent mobile users that communicate over relatively bandwidth and power constrained wireless links. As the nodes in a MANET are mobile, the network topology may change rapidly and unpredictably The network is decentralized which means that all network activity including route discovery, topology discovery, delivering messages and route maintenance must be executed by the nodes themselves, i.e. the nodes should be capable of performing the routing functionalities. Examples of such networks include building survivable, dynamic .

- *Mr.Madhusudhan H, MTech Student in Rajiv Gandhi Institute Of Technology,Dept Of CSE,Bangalore,India.*
- *Ms.Arudra A, Assistant Professor in Rajiv Gandhi Institute Of Technology,Dept Of CSE,Bangalore,India*

1.2 The Basic Concept

And efficient communication for emergency or rescue operations, disaster relief efforts and military networks. With the passage of time and increase in the use of MANETs, many security flaws in the routing protocols have been cited. This has motivated people in the Internet Engineering Task Force (IETF) to form a separate group to deal with this specific problem i.e. the MANET group of IETF, and some new routing protocols have been proposed under this group that take special care of security aspect of MANETs. These secure routing protocols do their job to acceptable extent and there can not be any compromise to the security a protocol provides, but we should also evaluate the routing protocols on the basis of performance metrics such as bandwidth utilization, round trip time, power consumption and overhead of security extensions etc. This can be useful in scenarios where we want to transmit some public information in very quick time. An example can be of an emergency relief network. In such a network we would surely be concerned with the privacy or secrecy of the information but we will be more concerned with the efficient and in time delivery of the messages. These kind of scenarios motivate us to evaluate routing protocols in the networking context rather than in security context. I n this paper we are implementing the shortest cost for traffic avoidance that are mainly possible with respect to route fashion.We are keen implementing more techniques on providing security and protection for the sender and receiver end with respect to verification and clarification scheme.

In this paper we are overcoming the security and the protection concern for MANET where in with the existing

routing protocols there is not much precise solution obtained for this concern .The basic concept behind this paper is to partition the network in to zones. this network consisting of about n- number of nodes that are precisely present in the particular zone and this zone consists of one random node where this random node will act as a relay node to transmit the data from one device to the other device .no matter how much safely the data has been received to the second device hence forth we are implementing the verification and confirmation scheme for this operation. where a data in the relay node will hide the data(encrypt) and the same data will be received(decrypt)at the second device.At this instance we are very much clear that data has been received to the second device(destination) but how to know that data has been sent from sender only and how to know that data has been received with the receiver only?.as a solution to this we are implementing the key generation function where in once when sender sends the data a random key will be generated from it and also at the other end the same key should be derived by the receiver if he needs to take that data, hence forth giving the confirmation for both the end.

1.3 Advantages and Disadvantages of MANETs

Advantages

- It requires less time to form the network
- MANET can be used as Temporary Network
- MANET is Multi-hop network with Autonomous Terminal and dynamic network topology.
- These networks can be set up at any place and time.
- Cost Estimation is very less
- This can be developed where there is less telecommunication infrastructure

Disadvantages

- Challenges in MANETs Initial Routing before attack
- Challenges in MANETs Data Packets Initial Routing before attack
- Challenges in MANETs• Data packets received in one place of the network and replay them in another place Attacker can attack the Routing Algorithm
- Challenges in MANETs most packets will be routed to the Attacker The Attacker can drop packets or forward packets to avoid detection

2 Literature Survey

In literature survey we are going to discuss some of the existing technique related to MANETs

a)X.Wu [1] Position service is essential for position-based ad hoc routing algorithms, which have proved to have decent network performance. As private information, node positions are valuable for attackers to locate their targets. Therefore, a secure position service system is needed. In this paper, a distributed secure position service system, named DISPOSER, is proposed and evaluated. A number of trusted servers are distributed in the network. Each node has a virtual home region (VHR). Servers residing in a node's VHR handle the position service regarding to the node, such as position update and position retrieving. DISPOSER keeps the position information private and prevents the position from being misused by a compromised user for tracing purposes. A region-based local broadcast approach has been designed to reduce the control overhead for information distribution within a VHR. Mechanisms for improving system robustness have been proposed. Analytical results show that while DISPOSER meets the security requirements, it achieves a high system robustness at a relatively low control overhead. One approach for obtaining a destination's position is broadcasting. The source broadcasts the position request in the network. When the destination receives the request, it replies the source with its most updated position. The approach is simple, yet the tradeoff is the overwhelming control overhead especially in a large network. It is shown in Reference [5] that broadcast may cause a so-called broadcast storm problem as the ad hoc channel is mostly used for transmitting redundant messages

b)Y-C Hu ,D.B.Johnson and A.Perrig [2] An ad hoc network is a collection of wireless computers(nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this paper, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol (DSDV). In order to support use with nodes of limited CPU processing capability, and to guard against Denial-of-Service (DoS) attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is

robustagainst multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

c)Z.Zhi and Y.K. Choong [3] Due to the utilization of location information, geographicad hoc routing presents 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. Routing design presents the main interest of research in mobile ad hoc networks. Existing ad hoc routing protocols could be roughly classified into two categories: topologybased and location-based(which we call geographic routing in our study). Topology-based routing [6, 13, 12] uses network-wide flooding to find a route or uses link information to perform packet forwarding. Geographic routing [7, 3, 1] utilizes only location information to perform packet forwarding, which evidently improves the routing performance. While geographic routing brings about exciting performance improvement, it raises an important issue about location privacy. In order to make a localized routing decision location information has to be present in packets, and must be accessible to all the nodes along the path towards the destination. Inevitably, malicious nodes with eavesdropping capability are given the access to those location information as well. Consequently, potential tracking of personal activity to derive sensitive information poses severe threat

d) Sk.Md.M.Rahman,M.Mambo,A.Inomato,and E.Okamoto [4] 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, 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. Also position information of routing nodes is very sensitive data in MANETs where even nodes not knowing either other establish a network temporarily. Therefore we propose a new position-based routing protocol which keeps routing nodes anonymous, thereby preventing possible traffic analysis. To this end, a time variant Temporary Identifier Temp ID is computed from time and position of a node and used for keeping the node anonymous. Only the position of a destination node is required for the route discovery, and Temp ID is used for establishing the route for sending data: a receiver hand shake scheme is designed for determining the next hop on-demand with use of the Temp ID. We evaluate the level of anonymity and performance of our scheme. The analysis shows that the proposed scheme ensures the anonymity of both route and nodes and the robustness against the target-oriented attack and several others. Also our scheme is applicable to networks with any density of nodes.

e)K.E Defrawy and G.Tsudik [5]

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. Unlike most networks, where communication is based on long-term identities (addresses), we argue that the locationcentric communication paradigm is better-suited for privacy in suspicious MANETs. To this end, we construct an on-demand location-based anonymous MANET routing protocol (PRISM) that achieves privacy and security against both outsider and insider adversaries. We analyze security, privacy and performance of PRISM and compare it to alternative techniques. Results show that PRISM is more computationally efficient and offers better privacy than prior work.

f) Z.Zhi and Y.K Choong[6]

Due to the utilization of location information, geographic ad hoc routing presents superiority in scalability com pared 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 pa- per, we attempt to preserve location privacy based on the idea of dissociating users' 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 communica- tion without compromising the efficiency guaranteed by geographic routing. You probably do not care if anyone dis- covers where you were at 10:30a.m. yesterday, but if all of your movements are

recorded every 5 seconds with foot accuracy, you might start to see things differently. In addition, network communications make the observation, propagation and processing of information on-the-fly, and the memory of information can be potentially unlimited. The scale of this problem changes thoroughly Specifically in ad hoc networks.

g) Muthumanickam Gunasekaran1, Kandhasamy Premalatha[8] Security plays a major role in implementing mobile ad hoc networks (MANET) for communication in an adverse environment. This study introduces the concept of anonymity for an informant who identifies and reports anonymously the misbehaviour of the users in the network. The trust-enhanced anonymous on-demand routing protocol (TEAP) is proposed to restrain the misuse of anonymity in two methods. In the first method, a user is revealed as a misbehaving user to other users, if it does not send any cooperative message, upon receiving two warnings. In the second method, if a user attempts to send multiple claims against a particular user for the same reason it will also be termed as a misbehaving user. The TEAP protocol is designed based upon broadcast with trapdoor information is a cryptography concept which is used to detect the misbehaving users anonymously in the network. The simulation results prove the necessity of anonymity in MANET and the effectiveness of this protocol in achieving such anonymity.

3 Existing System

In the existing system the Mobile ad-hoc network have been partitioned in to zones that consists of registered nodes that will to transfer the data from sender to receiver there by avoiding the hop by hop fashion of data transfer or by using the anonymity location to transfer the data from sender to the receiver where in it faces the problem of high cost to reach the destination. Also the existing system leads to traffic congestion problem where in this is over come again by not considering the previous routing fashion(hop by hp, anonymity location),instead it uses one among the node which is present in the zone and that node is called as "relay node" that has randomly selected depending upon the signal strength. This relay node will be completely different from one another across the network, in other words each zone will be consisting of a relay node. Hence the relay node from sender to receiver will come across all the Zone which is present in the network. The existing system assures that the path from sender to the receiver will be different in all the operation ,I,e same path will not be taken from sender to receiver for every operation.

3.1 Disadvantages of existing system

As seen by the experimental facts the existing system clearly describes that apart from portioning of mobile ad hoc network(MANET)and making zones where this zones consisting of set of nodes will randomly select that node as a relay node which is responsible to transmit the data from one zone(sender) to another zone(receiver) is taking place. We are clearly able to analyze that even though the existing system is trying to over come with the problem associated with routing algorithms and anonymity location where the trace of the path from sender to receiver is not detected by third party and hence forth data is delivered to receiver with out any data loss or data modified in the middle, but the major draw back what we are analyzing in this system is that there is no proper guarantee given from sender to receiver weather the data is properly delivered to the receiver means there is no confirmation from both the end telling that who has sent who has delivered, also there is a high possibility of tracing the relay node from the third party(hacker).And this led to our new proposed system that over comes all the draw back associated with existing system.

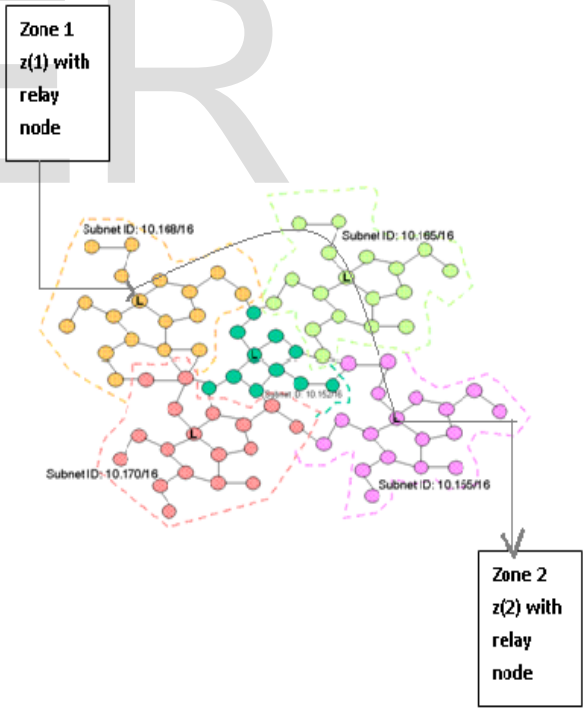

Fig3.1: **Transmission of data from z1 to z2 with out privacy and verification**

4 Proposed System

The proposed system will carry out the same procedures and operation when compared to the existing system where the network consisting of registered nodes and this nodes are grouped in to zones. All among these zones a random relay nodes are selected in order to transmit the data from sender to receiver. But to overcome the drawbacks associated with existing system we are implementing a two new solution for this. In order to authenticate between two zones a common key will be established soon after sending the data(packets) and delivering of data with the respective zones I,e sender and receiver .Also to avoid the data getting misplaced or misuse from the third party in the middle we are encrypting the data throughout the channel till it reaches the receiver and there after decryption takes place and hence forth a ultimate solution can be proposed for these issues

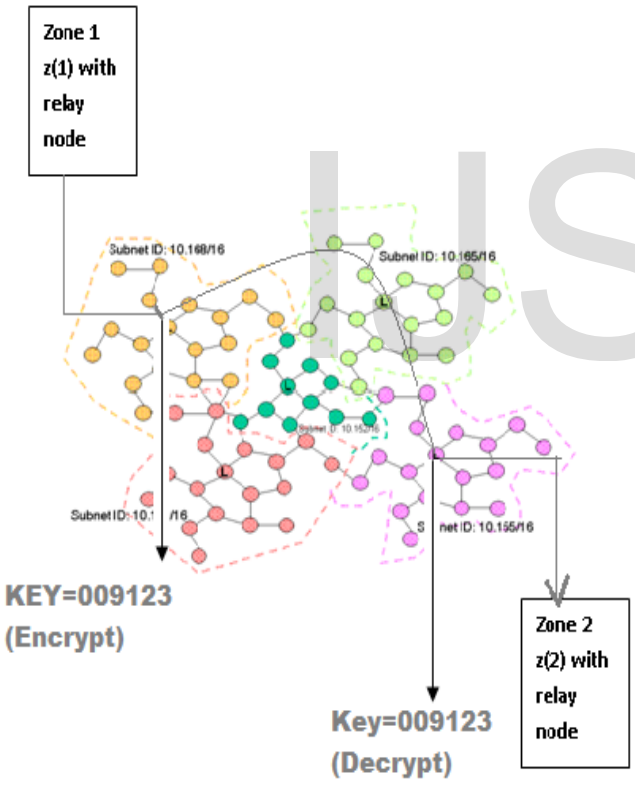

Fig4.1 :**Showing data transmission from one zone to another With verification(same key) and privacy(encryption, decryption)**

4.1 Advantages of proposed system

To overcome the disadvantage of existing system the proposed system gives a solution for the same. The main advantage of the proposed system is that even if the verification key gets fail either from one end the data wont be shared between the zones and appropriate error message will be prompted. During the encryption and decryption procedures if the node is getting treated with the third party a replica of the data will be taken by that node and it will re alter the position of the decrypting location.

5 Conclusion

To conclude MANET is a infra structure less network were in the mobility of the nodes plays a vital role for the data transmission from one end to the other end>hence proper care should be driven in such a way that these data transmission during the propagation should not create any abrupt termination of the data flow. This mean that a proper partition of the network should be carried out through out the operation. Not only the partition should play a major role even the parameters like routing, traffic congestion, tracing of anonymity location etc should also be taken in point. But the major concern for the network like authentication ,authorization and verification for any network should be defined and we have come across such criteria to end with the reliable and dynamic robust mobile ad hoc network.

6 References

1. Xiaoxin Wu*,† DISPOSER: distributed secure position service in mobile ad hoc networks

2. Yih-Chun Hu David B. Johnson Adrian Perrig SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks

3. Zhou Zhi School of Computer Engineering Nanyang Technological University Singapore Yow Kin Choong School of Computer Engineering Nanyang Technological University Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy

4 Sk. Md. Mizanur Rahman Graduate School of Systems and information Engineering, University of Tsukuba, Japan Atsuo INOMATA Japan Science and Technology agency, Research Institute of Science and Technology for Society, Japan Masahiro MAMBO Graduate School of Systems and information Engineering, University of Tsukuba, Japan Eiji OKAMOTO Graduate School of Systems and information Engineering, University of Tsukuba, Japan An Anonymous On-Demand Position-based Routing in Mobile Ad Hoc Networks

5 Karim El Defrawy and Gene Tsudik∗ Donald Bren School of Information and Computer Science University of California, Irvine
PRISM: Privacy-friendly Routing In Suspicious MANETs (and VANETs)

6 Zhou Zhi School of Computer Engineering Nanyang Technological University Singapore Yow Kin Choong School of Computer Engineering Nanyang Technological University Anonymizing Geographic Ad Hoc Routing for Preserving Location Privacy

7 Muthumanickam Gunasekaran1, Kandhasamy Premalatha2 TEAP: trust-enhanced anonymous on-demand routing protocol for mobile ad hoc networks