ISSN:0975-9646

An Improved and Efficient Multipath Anonymous Routing in MANET

B Usha
M.Tech Student, Electronics and Communication, Guru Nanak Dev Engineering College Bidar, Karnataka, India.

Premala Patil
Assistent Professor, Electronics and Communication, Guru Nanak Dev Engineering College Bidar, Karnataka,India

***Abstract*— unspecified communications are momentous for many applications of the mobile ad hoc networks (MANETs) deployed in opponent environments. The most important necessity on the network is to afford unidentifiability and unlinkability for mobile nodes and their traffics. Eventhough a number of unspecified secure routing protocols have been proposed, the requisite is not completely fulfilled. The existing protocols are susceptible to the attacks of false routing packets or denial-of-service (DoS) broadcasting, still the node identities are protected by pseudonyms. In this paper, I propose new routing protocol, i.e., authenticated anonymous secure routing(AASR) with multipath to assure requirement and defend the attack. In this protocol the route request packets are authenticated by group signature, to protect the prospective active attacks without disclosing the node identities. The key-encrypted onion routing with a route secret verification message, is intended to avoid intermediate nodes from inferring a real destination. Multipath routing allows the founding of multiple paths between a pair of source and destination node in MANET. By using multipath in anonymous routing we can get less end to end delay, less packet loss, more throughput. Simulation results have demonstrated that the proposed AASR protocol is effective with improved performance in multipath routing.**

Key terms-Group signature, Multipath routing, Trap door, Onion routing, Anonymous routing

I. INTRODUCTION

Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network. MANETs have potential use in a wide variety of disparate situations. Such situations include moving battlefield communications to disposable sensors which are dropped from high altitudes and dispersed on the ground for hazardous materials detection. Civilian applications include simple scenarios such as people at a conference in a hotel where their laptops comprise a temporary MANET to more complicated scenarios such as highly mobile vehicles on the highway which form an ad hoc network in order to provide vehicular traffic management.

MANET nodes are typically distinguished by their incomplete power, processing, and memory resources as well as high degree of mobility. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are typically needed for a node to exchange information with any other node in the network.

MANET is a self organized wireless network, due to the fact it has susceptible attacks that can easily damage the whole network; that's why there should be some solutions which works even some of the mobile nodes compromised in the network. It is complicated to afford trusted and secure communications in opponent environments, such as battlefields. On one hand, the opponents outside a network may deduce the information about the communicating nodes or traffic flows by passive traffic inspection, still if the communications are encrypted. On the other hand, the nodes within the network cannot be forever trusted, since a valid node may be captured by enemies and becomes malevolent. As a result, unspecified communications are significant for MANETs in opponent environments, in which the nodes identifications and routes are replaced by random numbers or pseudonyms for defense purpose.

Anonymity is defined as the state of being unidentifiable within a set of subjects. In MANETs, the necessities of unspecified communications can be described as a mixture of unindentifiability and unlinkability [1]. Unindentifiability means that the identities of the source and destination nodes cannot be discovered to other nodes. Unlinkability cannot be predictable the route and traffic flows between the source and destination nodes or the two nodes cannot be connected. The key to implementing the unspecified communications is to enlarge suitable unspecified secure routing protocols. There are many unspecified routing protocols projected in the history. Our focus is the type of topology-based on-demand unspecified routing protocols, which are general for MANETs in opponent environments.

In this work, we focus on the MANETs in opponent environments, where the public and group key can be originally deployed in the mobile nodes. We assume that there is no online security or localization service available when the network is deployed. I propose an authenticated anonymous secure routing (AASR) with multipath to overcome the pre-mentioned problems. It adopt a key-encrypted onion to trace a revealed route and intend an encrypted secret message to validate the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to evade intermediate nodes from modifying the routing packet. General simulations are used to compare the performance of AASR to that of AODV, a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than AODV under the packet-dropping attacks, although AASR experiences additional cryptographic process delay. AASR with multipath routing also we can get more throughputs, less packet loss, less end to end delay.

II. Literature Survey

Different approach are designed in order to get less end to end delay, less packet loss, more throughput. But the Simulation results have demonstrated that the proposed AASR protocol is effective with improved performance in multipath routing.

In paper [2] Privacy and security solutions require today the protection of personal information so that it may not be disclosed to unauthorized participant for illegal purposes. It is a challenge to address these issues in networks with strong constraints such as Ad Hoc network. The security increase is often obtained with a quality of service (QoS) decrease. We propose in this paper a solution that provides at the anonymity, security to Ad Hoc network with a limited impact on QoS. This method could be efficient against some viral attacks. We also give some security proofs of our solution for Ad Hoc networks.

In paper [4] Multipath routing allows the establishment of multiple paths between a pair of source and destination node in mobile ad hoc network. It is typically proposed in order to increase the reliability of data transmission or to provide load balancing and has received more and more attentions. In this paper, we present a multipath source routing protocol with some QoS guarantee. During the routing discovery, the source node firstly checks whether it has the routing information to the destination node. If not, it begins to broadcast RREQs to its neighborhoods and finally to the destination. From the received RREQs, the destination node can construct a certain topology for network and the path that is maximally disjoint from the shortest delay path is selected as our desirable routing. Simulation results show that comparing with traditional unipath routing scheme, the proposed protocol can greatly increases the packet delivery rate and extend the life-span of network.

In paper [3] 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.

III. Methodology

A.Trapdoor: In cryptographic functions, a trapdoor is defined on a one-way function between two sets .An information gathering mechanism in which intermediate nodes may add information elements, such as node IDs, into the trapdoor is called global trapdoor. By the use of pre-established secret keys certain source and certain destination nodes can release and reclaim the elements. An anonymous end-to-end key agreement between the source and destination can be potential by the use of trapdoor.

B. Onion Routing: This is a mechanism to provide secret communications over a open network. The interior of an onion with a exact route message can be locate by the source node. Every forwarding node adds an encrypted layer to the route request message, during a route request phase. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it with the route back to the source. The intermediate node can confirm its role by decrypting and removing the outer layer of the onion. Thus finally an anonymous route can be established.

C. Group Signature: This method can afford authentication with no troubling the anonymity. Each member in a group may contain a pair of group public and private keys that are issued by the group trust authority (i.e., group manager). The member can generate its own signature by its own private key, and that signature can be confirmed by other members in group without enlightening the signer’s identity. The tracing of the signer’s identity and repeal the group keys can be done only by the group trust authority.

D. Multipath Routing: Multipath routing allows the founding of multiple paths between a pair of source and destination node in mobile ad hoc network. It is usually projected in order to raise the reliability of data transmission or to provide load balancing and it allow additional secure and resilient data transmission.

Attacks on the ad hoc networks can be broadly categorized as Passive Attacks and Active Attacks.
I. Passive Attacks - The main aim of passive attackers is to steal the important information from the targeted networks. Attackers do not disturb the normal network functioning like inducing false packets or dropping packets. They simply become a part of the network but continuously keeps an eye on the network traffic thus in turn violating the message confidentiality restriction. Since they do not initiate any malicious activity to disturb the normal functioning of the network, it becomes very difficult to identify such attacks. Examples of such types of attacks are traffic analysis, traffic monitoring and eavesdropping.
II. Active Attacks - Active attackers interfere with the network traffic like reason for congestion, propagation of incorrect routing information etc. Due to their active participation, their detection and prevention can be done using suitable prevention algorithms. Examples of passive attacks include modification attack, impersonation, fabrication and message replay.

IV. Implementation

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours. NS2 is an object oriented simulator written in OTcl and C++ languages. While OTcl acts as the frontend (i.e., user interface), C++ acts as the backend running the actual simulation.

Due to its flexibility and modular nature, NS2 has gained constant popularity in the networking research community since its birth in 1989. Ever since, several revolutions and revisions have marked the growing maturity of the tool, thanks to substantial contributions from the players in the field. Among these are the University of California and Cornell University who developed the REAL network simulator, the foundation which NS is based on. Since 1995 the Defence Advanced Research Projects Agency) supported development of NS through the Virtual Inter Network Tested project currently the National Science Foundation has joined the ride in development. Last but not the least, the group of researchers and developers in the community are constantly working to keep NS2 strong and versatile.

A. Basic Architecture of NS2

NS2 provides users with executable command ns which take on input argument, the name of a Tcl simulation scripting file. Users are feeding the name of a Tcl simulation script (which sets up a simulation) as an input argument of an NS2 executable command ns. In most cases, a simulation trace file is created, and is used to plot graph and/or to create animation. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (Otcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events (i.e., a frontend). The C++ and the OTcl are linked together using TclCL. Mapped to a C++ object, variables in the OTcl domains are sometimes referred to as handles.

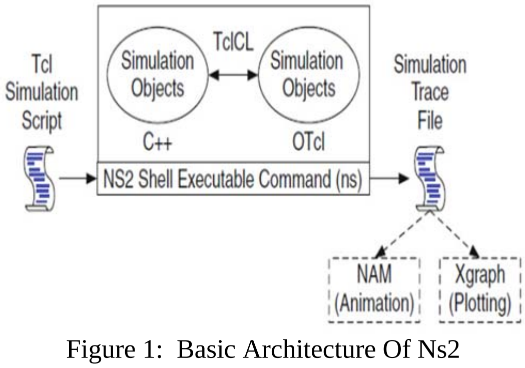

Figure 1: Basic Architecture Of Ns2

Conceptually, a handle (e.g., n as a Node handle) is just a string (e.g., _o10) in the OTcl domain, and does not contain any functionality. Instead, the functionality (e.g., receiving a packet) is defined in the mapped C++ object (e.g., of class Connector). In the OTcl domain, a handle acts as a frontend which interacts with users and other OTcl objects. It may define its own procedures and variables to facilitate the interaction. Note that the member procedures and variables in the OTcl domain are called instance procedures (instprocs) and instance variables (instvars), respectively. NS2 provides a large number of built-in C++ objects. It is advisable to use these C++ objects to set up a simulation using a Tcl simulation script. However, advance users may find these objects insufficient. They need to develop their own C++ objects, and use an OTcl configuration interface to put together these objects. After simulation, NS2 outputs either text-based or animation-based simulation results. To interpret these results graphically and interactively, tools such as NAM (Network AniMator) and XGraph are used. To analyze a particular behavior of the network, users can extract a relevant subset of text based data and transform it to a more conceivable presentation.

B Performance Analysis

- ***Throughput:*** Throughput is the percentage number of packets successfully reaching the destination over communication channel. The throughput is measured in terms of bits per second.
- ***Packet loss:*** Packet loss is the difference between number of packets sent or transmitted by number of packets received. Packet loss is proportional to packet drop.
- ***End-to-end delay:*** It indicates the time lapse between the source nodes and destination nodes in the network**.**

V. Simulation Results

1.Throuhput comparison under malicious nodes

when the number of malicious nodes increases, the average throughput of three protocols decreases obviously. Since AASR has the ability to detect the packet dropping attack, it outperforms AODV.

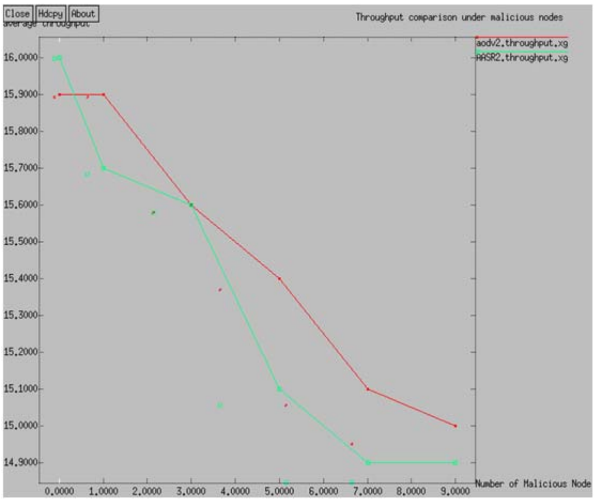

Figure 2: Throughput comparison under malicious node

2. end-end delay under malicious nodes

Here we can see the same result. AASR achieves less loss ratio than AODV in average. End to end delay is shown in graph 2 Since AODV is blind to the malicious attacks and takes no additional actions, its delay does not vary in the presence of different numbers of malicious nodes. Since AASR spend time in the security processing in their route discovery, their delays are much higher than AODV.

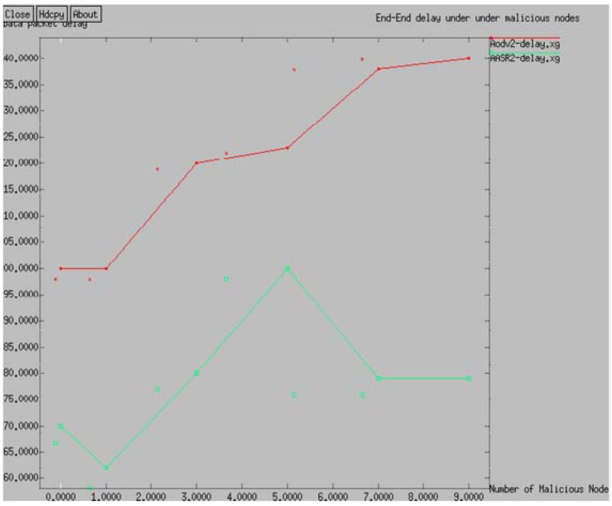

Figure 2: end to end delay under malicious node

Multipath routing graphs

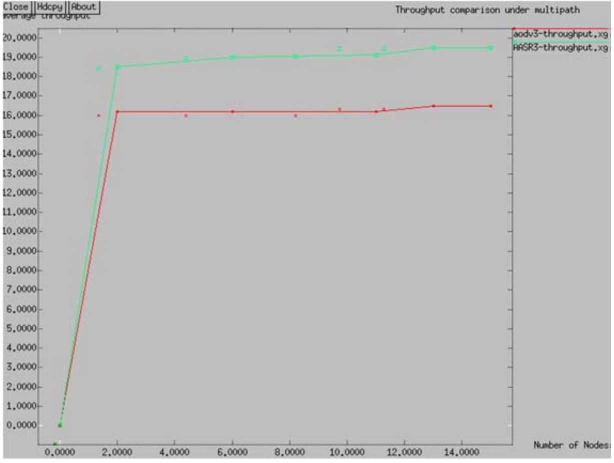

Figure 1: throughput under multipath routing

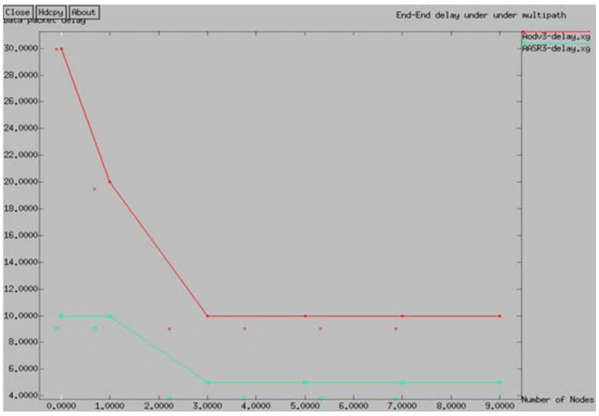

Figure 2: end to end delay under multipath routing

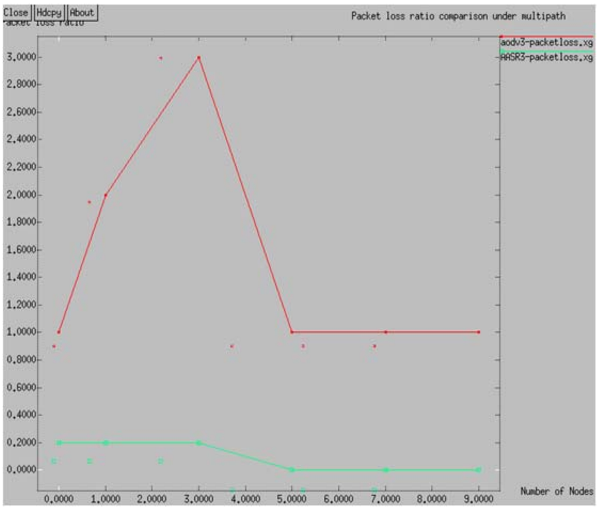

Figure 3: packet loss ratio comparison under multipath routing.

From the above graphs we can observe that the throughput is high, end to end delay is less and packet loss ratio is also less when compare to unicast routing. The performance of AASR protocol is better compare to AODV multipath routing.

VI. CONCLUSION

As compared to AODV, AASR protocol provides higher throughput and lower packets loss ratio in the presence of adversary attacks. It also provides better support for the secure communications that are sensitive to packet loss ratio. By using multipath routing in anonymous we can get less end to end delay, less packet loss, more throughput.

REFERENCE

[1] Wei Liu and Ming Yu, “AASR: Authenticated Anonymous Secure Routing for MANETs in Adversarial Environments” IEEE Transactions on VehicularTechnology,Volume:PP,Issue:99,Date of Publication :21.March.2014

[2] Herv´e Aiache, Fran¸cois Haettel, Laure Lebrun and C´edric Tavernier “Improving Security and Performance of an AdHoc Network through a Multipath Routing Strategy”

[3] Thejaswi D T “MART: Multipath-Based Anonymous Routing Protocol in MANETs” IJCAT International Journal of Computing and Technology, Volume 1, Issue 5, June 2014

[4] Fujian Qin, and Youyuan Liu “Multipath Routing forMobile Ad Hoc Network”2009 International Symposium on Information Processing (ISIP’09) Huangshan, P. R. China, August 21-23, 2009, pp. 237-240

[5] Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng “Anonymous Secure Routing in Mobile Ad-Hoc Networks.

[6] M. G. Reed, P. F. Syverson, and D. M. Goldschlag, “Anonymous Connections and Onion Routing,” IEEE Journal on Selcted Area in Comm., vol. 16, no. 4, pp. 482–494, May 1998.