International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10977-10983

http://www.ripublication.com

Secured Key Generation In Manet

Kunal Sharma A[1], D Siddharth[2] and Dr. S.Prayla Shyry[3]
[1]Student, Computer Science and Engineering, Sathyabama University, Chennai, India, (kunal46@live.com)
[2]Student, Computer Science and Engineering, Sathyabama University, Chennai, India,(siddharthfeb14@gmail.com)
[3]Asst.professor Computer Science and Engineering, Sathyabama University, Chennai, India, (suja200165@gmail.com)

Abstract

Communications of various and many sorts need to be secure and authentic. A network should be able to disable and protect off attacks from unauthorised users, as most applications of the mobile ad hoc networks (MANET) are used in unfriendly or attack-prone environment. In this paper, it is discussed about the key generation in MANET.

Introduction

A mobile ad hoc network (MANET) supports a number of applications. The applications which are used here run in adversary environments. Thus, non identification and unlink ability needs to be provided to the network. Mobile ad hoc networks (MANET) are generally open to security threats and unknown user due to inherent characteristics of such networks, for instance open wireless medium. A network can be under attack from inside as well as outside the network. The activities or traffic of a network can be observed by passive observation of the network, even if the communication is encrypted. Moreover, the nodes inside a network cannot be trusted always since a valid node may be captured by attackers and become malicious.

Anonymity is defined as the state of being unidentifiable within a set of objects. In mobile ad hoc networks (MANET), the requirements of anonymous communications can be described as a combination of non identification and unlink ability. Non identification means that the identities of the source and destination nodes cannot be revealed to other nodes. Unlink ability means that the route and traffic flows in the source and in the destination nodes cannot be recognised or the two nodes source and destination cannot be unlinked.

Related Works

D. Kelly et al proposed using anonymous on-demand routing protocols. Similar to the ad hoc routing, there are two categories: topology-based and location-based. We compare the protocols in terms of the key distribution assumption, node anonymity in route discovery, and packet authentication. Our observations are summarized as follows. [1]

C.Perkins et al described the routing protocols are designed to work in different scenarios.AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services SDAR, AnonDSR, MASK, and D-ANODR have problems in meeting the un-identifiable and unlink ability. The node IDs in a neighbourhood and along a route are possibly exposed in SDAR and AnonDSR, respectively. The plain node IDs are used in the route request of MASK and D-ANODR. [2]

D. Johnson et al used among many some of the protocols adopt additional authentication schemes to sign the routing packets, including A3RP, RAODR, USOR, and PRISM. Note that, although MASK provides neighbourhood authentication, it cannot sign the routing packets. RAODR deploys a master key mechanism, which cannot provide the anonymity, traceability, and enforceability that are supported by a group signature. A3RP and USOR adopt a group signature and use secure hash functions to map the keys and node pseudonyms along a route.[3]

J. Kong proposed that when it comes to topology based on demand routing , centralization and decentralization techniques are used. The major issues in the presently used techniques in MANETS is the consumption of resources by route discovery packets. Flooding is the most widely used technique that helps discover the path to broadcast a route request . After the path discovery comes a secure key management system for MANTES. This key management system does not rely on a centralized authority for generating and distributing keys. This in group based MANETS, group leaders generate keys , maintain them and also distribute in their groups a secure manner. To allow a node for enter a group challenge response protocol is used. This protocol lets the group leader authenticate the incoming node and lets it enter the group. This leads to the detection of any modification in the RREQ.[4]

M. Gerla et al based on the topology based routing protocols are source - initiated (Reactive on-demand) and Table driven (pro - active)

The source initiated protocols represent a class of routing protocols in which the source requests as the destination for a route and the route is then created.

The various mechanism in this protocol are Dynamic source Routing (DSR) followed by ADHOC on demand distance vector.

Pro-active routing protocols is the 2nd topology based protocols. It always routes from each and every node.

It uses DSDV technique, one of the earliest ADHOC routing protocols , optimised link state routing (OLSR) and also clustered gateway switch with routing (CGSR) from the practitioners point of view a very careful analysis of the scenario and is need are requested which acts as serious problem.[5]

Implementations

This paper presents the design of Authenticated Anonymous Secure Routing AASR protocol. Considering the nodal mobility, the paper takes the on-demand ad hoc routing as the base of our protocol, including the phases of route discovery, data transmission, and route maintenance. In the route discovery phase, the source node broadcasts an RREQ packet to every node in the network. If the destination node receives the RREQ to itself, it will reply an RREP packet back along the incoming path of the RREQ. In order to protect the anonymity when exchanging the route information, the paper redesign the packet formats of the RREQ and RREP, and modify the related processes.

Steps:

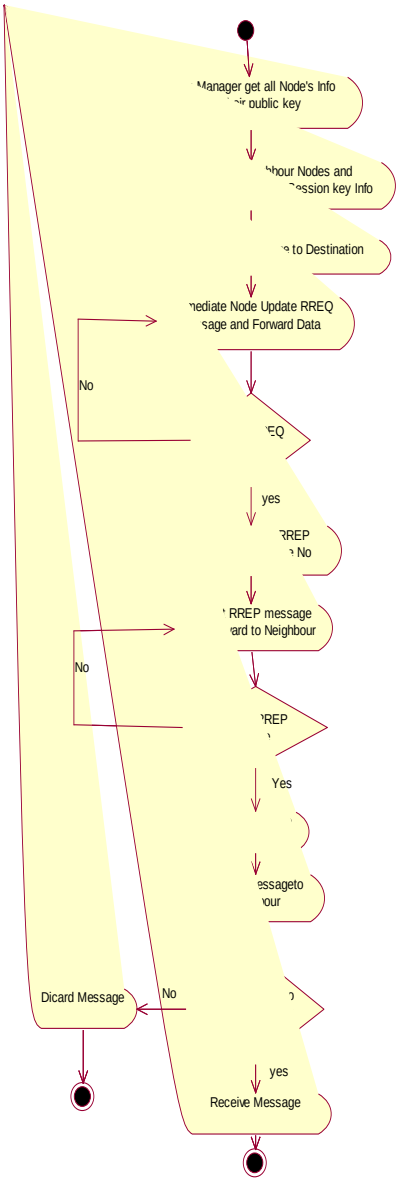
- **Anonymous Route Request**
- **Anonymous Route Reply**
- **Anonymous Data Transmission**

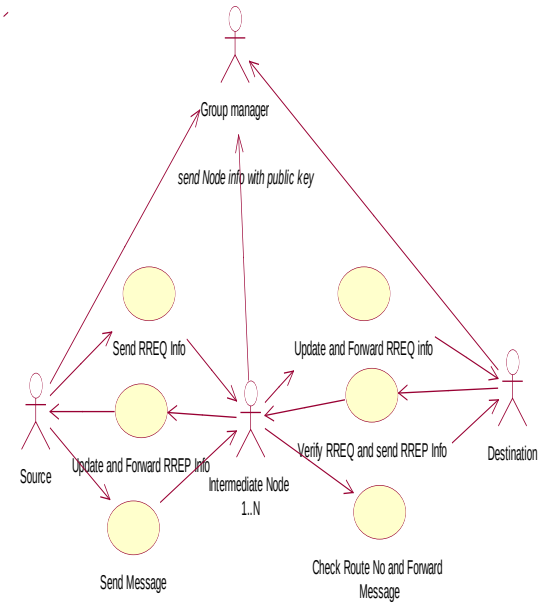
Anonymous Route Request

The source node sets up the core of an onion with a specific route message. During a route request phase, each forwarding node adds an encrypted layer to the route request message. The source and destination nodes do not necessarily know the ID of a forwarding node. The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established.

Anonymous On-demand Routing

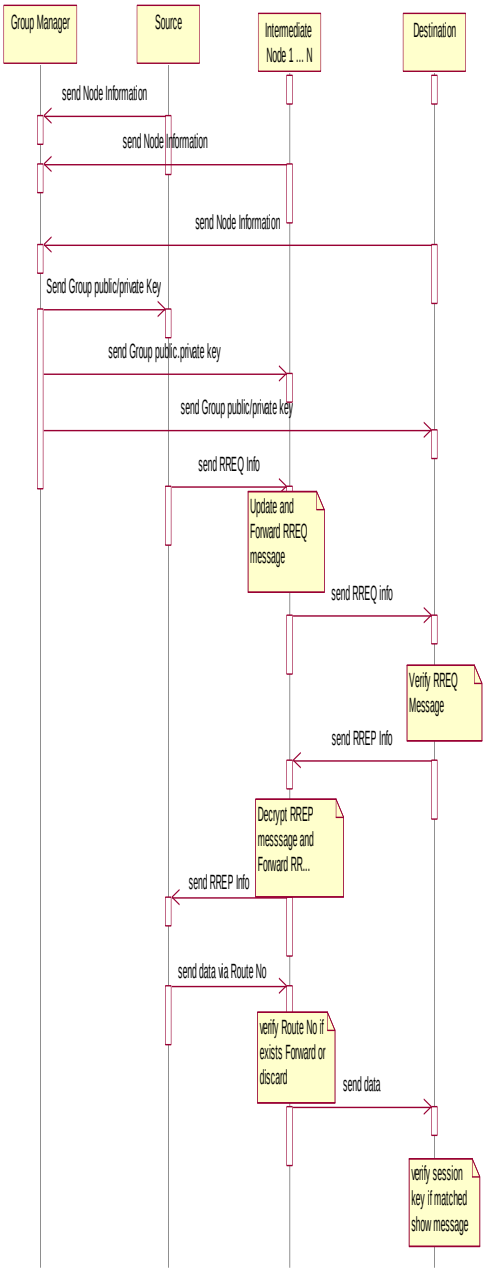
Many anonymous on-demands routing protocols and related to the ad hoc routing. Topology-based and location-based and node identity centric and location centric and the key distribution assumption, node anonymity in route discovery, and packet authentication. The routing protocols are designed to work in different scenarios. AO2P, PRISM, and ALERT are designed for location-based or location-aided anonymous communications, which require localization services. Since ours is for general MANETs, we focus on the topology-based routing rather than location-based routing.


Manager get all Node's Info
ir public key
hour Nodes and
ssion key Info
e to Destination
ediate Node Update RREQ
sage and Forward Data
No
EQ
yes
RREP
No
RREP message
ard to Neighbour
No
REP
Yes
essageto
our
Dicard Message
No
yes
Receive Message



Anonymous Data Transmission

We implement the of AASR protocol. Considering the nodal mobility and to take the on-demand ad hoc routing as the base of our protocol, including the phases of route discovery, data transmission, and route maintenance. In the route discovery phase, the source node broadcasts an RREQ packet to every node in the network. The destination node receives the RREQ to itself; it will reply an RREP packet back along the incoming path of the RREQ. In order to protect the anonymity when exchanging the route information and the packet formats of the RREQ and RREP.


Group Manager
Source
Intermediate Node 1 ... N
Destination
send Node Information
send Node Information
send Node Information
Send Group public/private Key
send Group public,private key
send Group public/private key
send RREQ Info
Update and Forward RREQ message
send RREQ info
Verify RREQ Message
send RREP Info
Decrypt RREP messsage and Forward RR...
send RREP Info
send data via Route No
verify Route No if exists Forward or discard
send data
verify session key if matched show message

Parameter	Value
No of Nodes	
No of Packets	
Packet size	
Arrival of packets	
Link type	
Link	
Querying	
Traffic	
Simulation	
Result	

Results & Discussion

The paper implements the authenticated and anonymous routing protocol for MANETs in adversarial environments. The key-encrypted onion routing with a route secret verification message is designed to not only record the anonymous routes but also prevent the intermediate nodes from inferring the real destination. The paper improves AASR module to reduce the packet delay.

References

[1]. D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila, "Towards a taxonomy of wired and wireless anonymous Networks," in *Proc. IEEE WCNC'09, Apr. 2009.*

[2]. C. Perkins, E. Belding-Royer, S. Das, *et al., "RFC 3561 - Ad hoc On-*Demand Distance Vector (AODV) Routing," *Internet RFCs, 2003.*

[3]. D. Johnson, Y. Hu, and D. Maltz, "RFC 4728 - The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," *Internet RFCs, 2007.*

[4]. J. Kong and X. Hong, "ANODR: Anonymous On Demand Routing with Untraceable Routes for Mobile Ad hoc networks," in *Proc. ACM MobiHoc'03, Jun. 2003, pp. 291–302.*

[5]. J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and on demand Routing scheme against anonymity threats in mobile ad hoc networks," *IEEE Trans. on Mobile Computing, vol. 6, no. 8, pp. 888*–902, Aug. 2007.