Literature Survey

**#1 DSR Routing Protocol in Wireless Ad-hoc Networks: Drop Analysis**

A Mobile Ad Hoc Network (MANET) is a network consisting of a collection of nodes capable of communicating with each other without aid from a network infrastructure. Each node participating in the network works both as host and a router and must therefore is willing to forward packets for other nodes. For this purpose, a routing protocol is needed. The most important characteristics of MANET is the dynamic topology, nodes can change position dynamically therefore a need of a routing protocol that quickly adapts to topology changes. In this paper for experimental purpose, Investigators considered 150m x 150m, 250m x 250m, 350m x 350m, 450m x 450m, 550m x550m, 650m x 650m & 750m x 750m terrain area and illustrate the Drop packet analysis using DSR protocol parameters for wireless network scenario. The *Dynamic Source Routing* protocol, a simple as well as an efficient routing protocol is designed particularly for use in multi-hop wireless ad hoc networks, allows the network to be entirely self-organizing and self-configuring, without the requirement of any presented network infrastructure or the administration. All aspects of the protocol work entirely *on-demand*, permitting the routing packet overhead to scale *automatically* to only which needed to respond to various changes in the different routes currently in use.

**#2. ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Adhoc Networks**

In hostile environments, the enemy can launch traffic analysis against interceptable routing information embedded in routing messages and data packets. Allowing adversaries to trace network routes and infer the motion pattern of nodes at the end of those routes may pose a serious threat to covert operations. We propose ANODR, an anonymous on-demand routing protocol for mobile ad hoc networks deployed in hostile environments. We address two closely related problems: For *route anonymity*, ANODR prevents strong adversaries from tracing a packet flow back to its source or destination; for *location privacy*, ANODR ensures that adversaries cannot discover the real identities of local transmitters. The design of ANODR is based on “*broadcast with trapdoor information*”, a novel network security concept which includes features of two existing network and security mechanisms, namely “broadcast” and “trapdoor information”. We use simulations and implementation to validate the effectiveness of our design.

**#3** An Efficient Anonymous Routing Protocol for Mobile Ad Hoc Networks

Providing anonymous routing in mobile ad hoc networks (MANET) has been a hot issue for the purpose of security and privacy concerns. But there are very few have been done about providing a valid method to detect malicious node and providing a trustworthy protection over whole network. In this paper, we introduce a localized trust management which can primarily remove malicious nodes, and propose an efficient anonymous routing protocol by node that participates in the protocol encrypts entire message with trust key and says Hello to its ancestor within expiration time. It makes malicious node can be detected and isolated from the network. In this way, a anonymous and secure route path can be established in a hostile environment. Meanwhile, it is able to efficiently against the Denial-of-Service (DoS) attack.

**#4. An Secure Anonymous Group Communication in Mobile Ad-Hoc Networks**

Secure group communication with efficient self-organizing key agreement and key establishment is essential to distributed applications in mobile ad-hoc networks (MANETs). In this paper, we propose a Secure Anonymous Routing Protocol (SARP) which is able to provide confidentiality service and non-repudiation service simultaneously. SARP based on Group signature and ID-based cryptosystem for ad hoc networks. The design of SARP offers strong privacy protection completes unlinkability and content unobservability for ad hoc networks. In the proposed scheme, all group members contribute their own public keys to negotiate a shared encryption public key, which corresponds to all different decryption keys. By using the shared public key and the respective secret key, confidentiality and non-repudiation can be obtained, respectively. Both are essential to secure group communication in MANETs. Compared with the exiting anonymous routing schemes for multiple recipients. Accordingly, it is quite suitable to secure group communication in self-organizing, distributed and resource-constrained MANETs.

**#5. MASK: Anonymous On-Demand Routing in Mobile Ad Hoc Networks**

The shared wireless medium of mobile ad hoc networks facilitates passive, adversarial eavesdropping on data communications whereby adversaries can launch various devastating attacks on the target network. To thwart passive eavesdropping and the resulting attacks, we propose a novel anonymous on demand routing protocol, termed MASK, which can accomplish both MAC-layer and network-layer communications without disclosing real IDs of the participating nodes under a rather strong adversary model. MASK offers the anonymity of senders, receivers, and sender-receiver relationships in addition to node unlocatability and untrackability and end-to-end flow untraceability. It is also resistant to a wide range of attacks. Moreover, MASK preserves the high routing efficiency as compared to previous proposals. Detailed simulation studies have shown that MASK is highly effective and efficient.