Abstract

An innominate communication method in MANETS is categorized into proactive method, re-active method and anonymous routing method. Re-active routing is further divided into two methods, which includes superfluous traffic and routing hop-by-hop encryption. Whereas MANETs has various choices in respect to anonymous routing protocols, to provide location innominate safety to information, source node and destination node. However, a previous innominate routing protocol fully depends on station by station encryption or superfluous traffic which generates a heavy cost and offer low anonymity protection. Hence to offer a very high innominate protection, S-ALERT is pro-posed. Basic idea behind S-ALERT is to divide the whole network into number of nodes and then allocate each node a unique Id, so that we can differentiate source node and destination node. Followed by dynamic partition of network into zones and then randomly choosing nodes in zones as random forwarder, which forms a non trace-able innominate route. Along with, it also hides the source/destination node among many source/destination, in order to give very high safety to source node and destination node. It is observed that S-ALERT gives better as compared to other protocols. Hence S-ALERT protocol achieves full anonymity protection and that to at very least cost.
Enhancing Privacy Preservation using S-ALERT Protocol to Diminish Routing Attacks in MANETs

- J. Li, J. Jannotti, D. S. J. De, C. David, R. Karger, and R. Morris, "A Scalable
Enhancing Privacy Preservation using S-ALERT Protocol to Diminish Routing Attacks in MANETs


Index Terms

Computer Science

Networks
Keywords