ABSTRACT

An Ad Hoc network is a network connection which is built based on a session of communication between devices. The Ad Hoc network does not require a router or a base station to support the communication between the devices. The Ad Hoc network, which is used for mobile communication is called Mobile Ad hoc Network (MANET). When the devices are enabled with mobility, the session may not hold good and hence the communication may hand-off, this can be overcome with MANET. Basic MANET characteristics are mobility, dynamic topology, limited bandwidth, autonomous and infrastructure less. The technical challenges in MANET are secure fault tolerant routing with energy constraints. The research work proposes a secure fault tolerant routing mechanism to build an efficient system for mobile communication. In addition, the research work comes with a new specialized delay tolerant approach for drop off the delay in communication due to reconstruction of path after the route discovery. The delay tolerant approach considers the delay between different hops of the route and considers many factors in data streaming.

The overall work is categorized as Cluster based fault tolerant routing with error reporting protocol, Delay tolerant multi variant quality driven approach for multimedia information and secure multipath routing for MANET with dynamic trust calculation.

Fault tolerance is the ability of a system to provide its services/functions even in the presence of faults. Due to the fault prone nature of MANETs and since they are deployed in hostile environment, it is required that the MANET should provide its functions even in the presence of node or path failures. Hence, providing for fault tolerance is an important requirement.
of this network. The research work proposes a Fault Tolerant Cluster based AODV Routing protocol with error reporting mechanism (CAODVERR) that works for MANET. The function of the proposed protocol is to typically send error messages to the source of the data packets whenever a data packet along the route path is discarded. It also provides a Control message which can be used to find alternate active neighbors of a node in order to continue its process. This protocol provides alternate paths called as backup path for fault tolerance. The CAODVERR protocol consists of two important tasks namely, Cluster based Routing and Error Reporting. In this protocol, backup route is provided for all nodes in the network. Whenever a node receives a Route Reply (RREP) packet, it stores the route to the destination in the routing table.

Another proposed work is delay tolerant mechanism for multimedia data streaming to reduce the time redisCOVERS the route and route selection phase when fault occurs. This delay tolerant is specifically helpful in multimedia data streaming to select the path which supports high quality data streaming.

The method counts the number of hops and delay between hops, traffic, and bandwidth to perform efficient data streaming. The method calculates the delay approximation in available path while reconstruction including fault tolerant. Then based on the quality needed, the method performs route selection with the proposed routing mechanism called Delay Tolerant Quality Driven Routing (DQDR). The entire approach has been split into number of stages namely Route discovery and construction as given in fault tolerant approach, delay approximation in back up selection and multi variant quality driven route selection.

Third work is about secure multipath routing for MANET with dynamic trust calculation. In some existing systems, initially the trust of the nodes is calculated and routing is carried based on that. After that, sometimes
the trusted nodes energy may reduce or that node is considered for routing because of not in communication path. So, in the proposed system the fault tolerant routing may provide the nodes involved in the routing phase. From that, the trust of the nodes is calculated and routing will be reconstructed as secure multipath routing. The reliability of node is assessed in this model, which is utilized with an attacking prevention system to agreeably distinguish and disconnect the vindictive nodes from the system. At long last, a trusted way is acquired in view of the trust esteem. A dynamic trust-based receptive steering convention named Ad-hoc on interest Dynamic Trusted Multipath Distance Vector (AODTMDV) is utilized for directing as a part of MANETs. Tests have been carried out in the research work to analyze the current trust model and the outcomes demonstrate that the proposed model enhances the security of system by distinguishing the gatecrashers adequately to lessen false alert rate.