Securing Mobile Adhoc Network from Black Hole Attacks

MANETs are in-secure and vulnerable to attacks as it lacks a central trusted authority. Providing security to such a network becomes an essential task and forms the basis of the proposed work. The proposed system makes an attempt to secure MANETs using route validation and cryptographic techniques.

One of the most crucial, and primary concerns in today's times is to be able to detect an attacker at its initial stages. This also forms a focus point in our system, where our aim is to prevent such attacks by detecting them, preventing network degradation. The novelty of the proposal system is the use of cryptographic techniques for improving the security, along with reverse-AODV for reducing path fail correction and machine learning concepts for validation of results.

Many of the existing malware detection techniques proposed by the researchers were either executed on machine independent platform, or on an available dataset with machine dependent approaches. This gap has been addressed in the existing proposal, where in machine learning is used with self-generated data-set, to eliminate contingent problems.

The proposed system includes such a network, that is designed to be free from *black hole attack*s. Results justifying this system were generated using classifier tools that were trained along with the obtained dataset. For secured communication, an *elliptical curve cryptographic algorithm* is applied to reverse ad-hoc on-demand distance vector with *reverse multiple route replies* that have been generated from the destination to the source node.

An investigation to ensure the correct delivery of data can be done by diverting the traffic through the shortest alternative secured path is theorized for the detection.

Fahmina Taranum