Abstract

The advent of mobile and miniature devices in wireless technology gives rise to new paradigm called Mobile Ad-hoc Network (MANET). MANETs are self-maintaining, self-administered dynamic network. MANETs are vulnerabilities in the MANET due to its intrinsic characteristic that make it insecure against various security threats. The black hole attack is forthcoming among them that are launched on AODV protocol. In these attacks, a malicious node disrupts data transmission by sending false routing information containing very high sequence numbers. To deal with these attacks, we proposed an incentive mechanism that protects network against this attack. This mechanism is integrated into route decision making process of the AODV protocol to defend the black-hole attack.

References

- R. H. Jhaveri, &quot;MR-AODV: A Solution to Mitigate Black-hole and Gray-hole
A Fortify Approach to Secure AODV Protocol against Black Hole Attacks

Attacks in AODV Based MANETs; Third International Conference on Advanced Computing & Communication Technologies, Pp. 254-260.
- Rajesh Yerneni and A. K. Sarje &quot;Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks;&quot; ICCCNT©2012, pp. 248-252.
- Kamarularifin Abd Jalil et. al. &quot;Securing Routing Table Update in AODV Routing Protocol;&quot; IEEE conference on Open Systems, 2011, pp. 116-121.
- Jaspal Kumar et. al. &quot;Effect of Black Hole Attack on MANET Routing Protocols;&quot; I. J. Computer network and Information security, April 2013, pp 64-72.

Index Terms

Computer Science       Security
Keywords
   AODV   Black hole attack   Gray-hole attack   security   sequence number.