Modification in the Kerberos Assisted Authentication in Mobile Ad-hoc Networks to Prevent Black Hole Attack

Abstract

MANET is the self-configuring type of network in which the mobile nodes can leave or join the network when they want. MANET is decentralized type of network, no central controller is present. Due to their unique features mobile ad hoc networks can be deployed anywhere round the clock. This posed the remedial venture to large number of attacks like replay attack, fabrication, eavesdropping etc Kaman provides secure solution to the problem of secure channel establishment, secure exchange of session keys and prevention of nodes identity forgery. In this paper, we reviewed the Kaman; Kerberos assisted Authentication in Mobile Ad hoc Network and added the concept of timers in KAMAN to solve the problem of black hole attack that aroused when Kaman protocol is embedded into large network AODV, on-demand routing protocol had been used to select secure shortest path between the nodes.

References

- Asad Amir Pirzada and Chris McDonald,"Kerberos Assisted Authentication in
Mobile Ad-hoc Networks
- C. Siva Ram Murthy, B. S. Manoj, 2007 "Ad Hoc Wireless Networks, Architectures and Protocols";
- Georgios Kambourakis, Elisavet Konstantinou, "Efficient Certification Path Discovery for MANET”;
- Govind Sharma, Manish Gupta (2012), "Black Hole Detection in MANET Using AODVRouting Protocol”;
Modification in the Kerberos Assisted Authentication in Mobile Ad-hoc Networks to Prevent Black Hole Attack

- Irshad Ullah, Shoaib UR Rehman, 2010 "Analysis of Black Hole attack On MANETs Using different MANET Routing Protocols";
- Kamarularifin Abd. Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Mitigation of Black Hole Attacks for AODV Routing Protocol";, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA Malaysia, Shah Alam, Selangor, Malaysia.

Index Terms

Computer Science
Networks

Keywords
Black hole  Mutual Authentication  Secure server  MANET  KAMAN.