Chapter 5
IPHDBCM:
Inspired Pseudo Hybrid DNA Based Cryptographic Mechanism to Prevent Against Collabrative Black Hole Attack in Wireless Ad hoc Networks

Erukala Suresh Babu
K.L. University, India

C. Nagaraju
Y.V. University, India

M.H.M. Krishna Prasad
J.N.T. University, India

ABSTRACT

Secure communication is one of the basic requirements for any network standard. Particularly, cryptographic algorithms have gained more popularity to protect the communication in a hostile environment. As the critical information that is being transferred over the wireless adhoc networks can be easily acquired and is vulnerable to many security attacks. However, several security communication threats had been detected and defended using conventional symmetric and asymmetric cryptographic mechanism, which are too difficult and resource consuming for such mobile adhoc networks. Recently, one of the severe security threats that have to be detected and defend in any type of network topology is blackhole attack and cooperative blackhole. Because of its severity, the black hole attack has attracted a great deal of attention in the research community. Comprehensively the results of the existing system conclude that the black hole attack on various mobile adhoc networks is hard to detect and easy to implement. This paper addresses to detect and defend the blackhole attack and cooperative blackhole attack using hybrid DNA-based cryptography (HDC) mechanism. Moreover, the proposed method upsurge the security issue with the underlying AODV routing protocol. Eventually, This Hybrid DNA-based Cryptography (HDC) is one of the high potential candidates for advanced wireless ad hoc networks, which require less communication bandwidth and memory in comparison with other cryptographic systems. The simulation results of this proposed method provide better security and network performances as compared to existing schemes.

DOI: 10.4018/978-1-7998-1763-5.ch005

1. INTRODUCTION

There is a necessity to design and develop a secure wireless mobile ad hoc network (SWMANETs), particularly useful for battlefield applications in order to perform security-sensitive operations. Unlike wireless network with fixed infrastructure that makes use of access points to communicate, a MANET is an infrastructure less network does not require any centralized administration. however, network elements of these networks are needed to be deployed rapidly with reasonably low cost. One of the primary concerns of these networks requires resilient security service, which are more vulnerable to limited physical insecurity of mobile nodes, as these nodes are disposed to attacks. These attacks are performed in both reactive and proactive routing protocols, which can roughly be relegated into two major categories such as active and passive attacks (Konate, K., 2011; Gopi, A. P et al., 2015 ; Kumar, S. A et.al 2015). The malicious nodes pretend to be as a trusted router by advertising the spurious service requests to disrupt the normal routing operation and to deny the services to authorized nodes, which leads to a DOS attack. In active attack, the malicious router originates the attack by modifying the information in the network. The black hole attack is one such type of active assaults that can be performed against both reactive and proactive routing protocols. To be more specific, each black hole node impersonates the source and destination node by sending an imitated path request to the destination node and imitated path reply to the source node that was taking place in route discovery phase to claim that, it has the optimal route information. Finally, the black hole node consumes the packet, and simply drops the packets, that reduce the network performance *as shown in figure-1.* On the other hand, under the context of information and network security domain, it is necessary to provide an unbreakable cryptosystem to protect the data that we transmit over the network; Open Systems Interconnection (OSI) security architecture provided a systematic security solution for different layers of networks. In the routing layer of the OSI model, it is essential to design a secure protocol that can defend the black hole attack and cooperative black hole attack against on-demand routing protocol (Osathanunkul, 2011; Dasgupta, 2012). More importantly, the security services such as authentication, data confidentiality, nonrepudiation and data integrity services must be incorporated into these on-demand routing protocols.

The following are some of the challenging issues to secure against black hole attack and cooperative black hole attack. The first challenging issue is to secure the routing protocols against the black hole attack. This problem has not properly addressed in most of the existing secure routing protocols or if addressed, there are very expensive in terms of bandwidth and limited computational capabilities. The second challenging issue is to defend the black hole attack against adhoc routing protocols that dynamically changes the topology, (i.e., what kind of key management and authentication schemes are needed? Unlike of Wireless networks, MANET cannot use any certificate authority (CA) server).The third challenging issue is the existing secure routing protocols may not efficient or feasible to scale, as these protocols produce heavy traffic load and requires intensive computations.

This paper mainly addresses all the above issues using hybrid DNA based cryptographic mechanism to defend and detect a black hole attack and cooperative black hole attack against AODV routing protocol. We call this protocol, as Secure Routing Protocol using Hybrid DNA-based Cryptography (SRP-HDC) that establishes cryptographically secure communication links among the communicating mobile nodes.

The rest of the paper is as follows. Section-II specifies the related work that had proposed a large class of ad-hoc routing protocols and attacks against MANET in the literature. Section-III enumerates the hybrid cryptosystem that prevents the collabrative black hole attack against on-demand routing protocols by authentication and encryption mechanism. Section-IV presents the detection mechanism