Chapter 10
Security and Privacy in Mobile Ad hoc Social Networks

Mohamed Amine Ferrag
University of Badji Mokhtar – Annaba, Algeria

Mehdi Nafa
University of Badji Mokhtar – Annaba, Algeria

Salim Ghanemi
University of Badji Mokhtar – Annaba, Algeria

ABSTRACT

In this chapter, first, the authors briefly introduce the two new systems "MASN-OLSR" (Mobile Ad Hoc Social Networks with OLSR) and "MASN-AODV" (Mobile Ad Hoc Social Networks with AODV). Then they choose wormhole and black hole attack methods, because they are not completely solved, especially in a setting where MASN is used as OLSR or AODV routing protocol. The authors give a definition of the wormhole and black hole attacks on an ad hoc network using OLSR or AODV as routing protocol and then examine the various existing proposals in the literature to overcome this attack. With an analysis of these methods, they then determine the advantages and disadvantages of each of these new systems.

INTRODUCTION

Since their introduction, the wireless local area networks have attracted the interest of professionals, faced with the needs of mobility and network connectivity to their organization. 802.11 networks, standardized by the IEEE in 1997, has rapidly become until, in some cases, replace traditional wired networks like Ethernet. Since their arrival on the market, the steady evolution of their performance and lower their cost of acquisition helped accelerate their dissemination.

The IEEE 802.11 provides two modes: infrastructure mode and ad hoc mode. Infrastructure mode, also called cellular mode, uses a topology built around fixed access points. The latter is responsible for managing exchanges between mobile nodes located in their area transceiver. Multiple

DOI: 10.4018/978-1-4666-4691-9.ch010

access points can be interconnected by a backbone network, called the distribution system to provide connections to a larger number of nodes or increase the space of node mobility. Ad hoc mode, it establishes an exchange point to point between two mobile nodes. If two nodes do not share the same areas transceiver, a direct connection is impossible. In this case, the intermediate nodes are used to establish a path between the source and destination nodes. These networks, whose architecture evolves according to the movement and appearance of nodes are called MANET (Mobile Ad hoc NETwork) or spontaneous networks (M.A. Ferrag 2012).

In some contexts, users can benefit from the features of MANET to exchange information. A frequently cited example, in civil and military, is an ad hoc network formed by the interconnections between moving vehicles. In the industrial networks catch (Sensor Networks) can form a MANET to adapt to different environments. But many other situations of everyday life are adapted to the use of MANET. We consider, for example, a network created for the purposes and duration of a meeting of participants from different organizations, or created a network between students and their teacher in a classroom for the duration of a course.

There are primarily two types of routing protocol in ad hoc networks. The reactive routing protocols (AODV, DSR) that initiates the search for a route when trying to reach a destination that is not contained in the routing table. The proactive routing protocols (OLSR, FSR) that maintain regularly update the information in the routing table with route discovery requests. Note that the hybrid algorithms exist. They then make use of both protocols under different conditions.

Two types of algorithms used to maintain accurate routing tables. This is the distance vector algorithms and link state. In general, the route discovery is as follows. When a node wants to transmit a message to another node it broadcasts a route request different denominations according to the protocols. The road was then built as and when his discovery to the recipient once attached can return a message back to sender. The road is then set and the actual data exchange can take place. In the absence of authentication, confidentiality, integrity, etc. Ensuring the smooth running of these protocols, network stability can be greatly compromised.

The issue of privacy is almost solved but major gaps remain in terms of routing protocols. For this reason, the subject of this chapter focuses on the security of routing protocols in MASN. We chose both OLSR and AODV routing protocol because they are most widely used in ad hoc community.

MASN (Mobile Ad Hoc Social Networks) is inherited from the MANET (Mobile Ad Hoc Networks). So the attacks which exist in MANET necessarily exist in MASN. The design consideration for MANET made a number of differences with the traditional centralized networks, namely:

1. Dynamic Topology
2. Resource Constraints
3. Low Cost
4. Limited Physical.

MANET is subject to a number of attacks. For example, an attacker in the MANET may not be willing to route packets to other nodes. On the other hand, more sophisticated attacks against MANET routing can disrupt the route discovery. In addition, they may interfere with maintaining ride disobedient routing protocols. Blackhole Attack, Byzantine Attack, Wormhole Attack , and Spoofing Attack are illustrations of various threats for MANET. For the purposes of group communication security, cryptography has been integrated in MANETs. Among the most popular techniques, symmetric and public key infrastructure (PKI).

First in this chapter, we briefly introduce the two routing protocols OLSR and AODV then the two new systems MASN- OLSR (Mobile Ad Hoc