A REVIEW OF INTRUSION DETECTION SYSTEM ARCHITECTURES IN MOBILE AD HOC NETWORKS

Shafi'i M. Abdulhamid,
Department of Maths/Computer Science,
Federal University of Technology Minna, Niger State.
Shafzon@yahoo.com

ABSTRACT

Mobile ad hoc network (MANET) faces serious security threat due to lack of consideration of security in design and inherent weaknesses. Many intrusion detection techniques as well as preventive measures are in urgent need to protect ad hoc network. This paper reviewed different categories of intrusion detection techniques proposed by different authors. The paper also looked at different types of intruders, the routing protocols in MANET, and then reviewed intrusion detection system architectures as proposed by different authors in past and finally made some recommendations.

Keywords: MANET, Intrusion Detection Systems (IDS) and Anomaly Detection

1

INTRODUCTION

A Mobile Ad Hoc Networks (MANETs) is an autonomous system of mobile host connected by wireless links and forming a temporary network without any pre-existing infrastructure. Each host is directly connected to hosts that are within its range of transmission and reception, and it is free to move randomly in and out of any other host's range. Communication between hosts that are not located in the same coverage range can be realised by establishing a multi-hop route through intermediate hosts that acts as routers when they forward data for others.

The design of MANETs has attracted a lot of attention. The interest in MANETs is driven mainly by their ability to provide instant wireless networking solutions in situations where cellular infrastructures do not exist and are expensive or unfeasible to deploy (disaster relief efforts, battlefields, etc.). Furthermore, because of their distributed nature, MANETs are more robust than their cellular counterparts against single-point failures, and have the flexibility to reroute