Chapter 11

Intrusion Detection and Tolerance in Next Generation Wireless Network

Deshraj Ahirwar
UIT RGPV, India

Kirti Raj Bhatele
UIT RGPV, India

P. K. Shukla
University Institute of Technology, India

Prashant Shukla
SIRT RGPV, India

Sachin Goyal
UIT RGPV, India

ABSTRACT

Organizations focuses IDPSes for respective purposes, e.g. identifying problems with security strategies, manually presented threats and deterring individuals from violating security policies. IDPSes have become a necessary technique to the security infrastructure of approximate each association. IDPSes typical record information interrelated to practical events, security administrators of essential observed events and construct write up. Many IDPSes can also respond to a detected threat by attempting to thwart it succeeding. These use several response techniques, which involve the IDPS restricting the attack, changing the security environment or the attack's content. Sensor node should diverge in size from a shoebox down to the small size, although functioning "motes" of genuine microscopic dimensions have to be formed. The cost of sensor nodes is variable, from a few to thousands of dollars, depend on the complexity of the sensor nodes. Size and cost constraints on sensor nodes represent in corresponding constraints on resources such as energy, memory, computational velocity and communications bandwidth. The arrangement of the WSNs alters itself from a star network to efficient multi-hop wireless mesh network. The proliferation technique between the hops of the network can be routing or flooding.

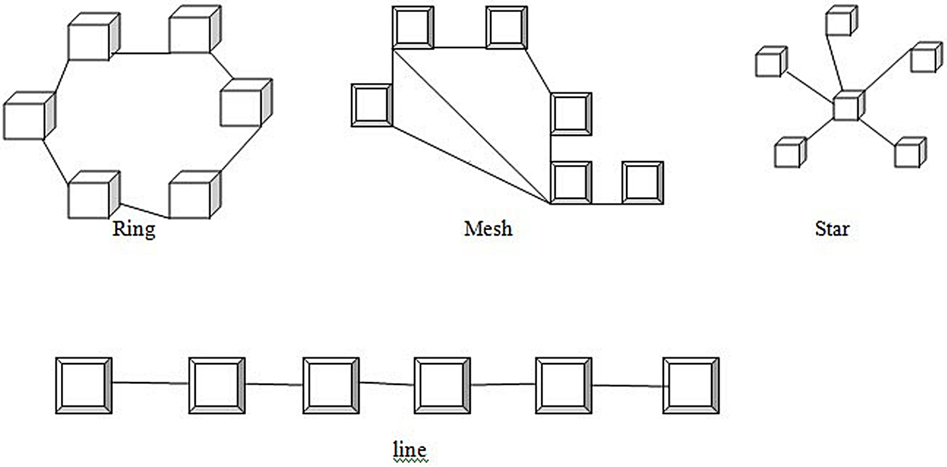
DOI: 10.4018/978-1-4666-8687-8.ch011

INTRODUCTION

An intrusion detection system is a software application that monitors system activities for malicious policy violations and generates reports to a management station. IDS come up to in a "flavors" and move toward the goal of detecting suspicious traffic in different types. There are network based and host based intrusion detection systems. System should try to stop an intrusion attempt but it is not expected of a monitoring system. Intrusion detection and prevention systems are primarily listening on identifying possible incidents, logging information, and reporting attempts (Scarfone & Mell, 2007). A wireless sensor network of spatially distributed autonomous sensors to test environmental conditions, for example temperature, sound, pressure, etc. and to cooperatively pass data through the network to prime location. Modern networks are bi-directional. Development of wireless sensor networks was aggravated by military applications such as battlefield surveillance; presently networks are second-hand in many industrial and consumer applications, e.g. industrial process monitoring and control, machine health monitoring. The various Topologies is illustrated in Figure 1.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, Node is coupled to one sensors. Sensor network node has typically several parts: a radio transceiver with an internal antenna to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, the embedded form of energy harvesting. Sensor node may fluctuate in size from a shoebox down to the different size, although functioning "motes" of genuine microscopic dimensions to be displayed. The cost of sensor nodes is variable, A few to

Figure 1. Topologies of devices



Related Content