LOCATING THE ATTACKER OF WORMHOLE ATTACK ON RPL IN IOT

By

Roshni Hasmukhray Patel
Enrollment No.:140370702549

Guided by

Mr. Rutvik Mehta
M.E(I.T)
Asst. Prof, IT Department

A **Thesis** Submitted to
Gujarat Technological University
In Partial Fulfillment of the Requirements for
The Degree of Master of Engineering
In **Computer Engineering**

May – 2016

Computer Science and Engineering Department
Parul Institute of Engineering & Technology
P.O: Limda, Ta.: Waghodia, Dist.: Vadodara

Locating the Attacker of Wormhole Attack on RPL in IoT

Submitted by

Roshni Hasmukhray Patel

Supervised by

Mr. Rutvik Mehta

M.E. (IT), Assistant Professor,

Parul Institute of Engineering and Technology,

Limda, Waghodia, Vadodara

ABSTRACT

Internet of Things (IoTs) offers capabilities to identify and connect worldwide physical objects into a unified system. As a part of IoT, serious concerns are raised over access of personal information pertaining to device and individual privacy. Internet of Things consists of devices which are limited in resources like battery powered, memory and processing capabilities etc. For this a new network layer routing protocol is designed. This routing based protocol may undergo several kinds of attacks. Honeypots provides a platform for studying the methods and tools used by the intruders, thus deriving their value from unauthorized use of their resources. This enhancement plays an active role in analyzing and detecting the wormhole attack. In this research work new approach is proposed, which helps to dynamically detect the Wormhole attack and helps to prevent it.