SENTHAMARAI

INTERNATIONAL CONFERENCE ON NEW HORIZON IN IT ICNHIT'18

Organized by

DEPARTMENT OF COMPUTER APPLICATIONS

SENTHAMARAI COLLEGE OF ARTS AND SCIENCE

(Approved by Govt.of Tamil Nadu and Affiliated to Madurai Kamaraj University)

VHS Garden, Vadapalanji, Palkalai Nagar, Madurai - 625 021

INTERNATIONAL CONFERENCE ON New Horizon in IT ICNHIT'18

© DEPARTMENT OF COMPUTER APPLICATIONS

ISBN: 978-93-87102-89-7

First Edition: 2018

All rights reserved. No part of this book may be reproduced, stored in a retrieval system or transmitted, in any form or by any means, mechanical, photo copying, recording or otherwise, without prior written permission of the author or publisher.

Publisher
SHANLAX PUBLICATIONS
61, 66 T.P.K. Main Road,
Vasantha Nagar,
Madurai - 625003
Tamil Nadu, India

Ph: 0452-4208765,
Mobile: 7639303383
email: publisher@shanlaxpublications.com
web: www.shanlaxpublications.com

CONTENT

WIRELESS PROTOCOLS AND LIGHTWEIGHT AUTHENTICATION

B.Chandirika,
chandirikab@gmail.com
Head & Associate Professor, Department of MCA, FatimaCollege

B.Usha,
USHABHAKTHA@gmail.com
Assistant Professor, Department of MCA, FatimaCollege

Abstract

Wireless Sensor Network stands as one of the most emerging technologies combining together sensing, computational capability and communication into minute devices proceeding towards whole new world of simplicity. Many of cloud computing applications like that in health sector include collection of data by sensors and then sending it wirelessly to cloud. WSN acts as a mediator between the real physical world and the virtual world. In this paper, we report some of the current trends, challenges and security issues with wireless sensor network. Leap protocol offers many security benefits to WSNs. LEAP only employs one base station and always assumes that it is trustworthy. In this paper, intensive research was undertaken on LEAP protocols, finding out its security drawbacks and limitations. A solution has been proposed in order to overcome the security issues faced in implementing this protocol whilst employing more than one base station. The performance of the proposed solution has been evaluated and simulated to provide a better network performance.

Key Words: *Wireless Sensor Network, LEAP, Authentication*

Introduction

A wireless sensor network (WSN) is a collection of spatially distributed autonomous sensors to examine present atmospheric and physical such as temperature, pressure, etc. and to cooperatively pass the data gathered through the network to a main centralized point [1]. A WSN in its simplest form can be defined as a collection of sensing devices (nodes) that can sense the environment, process data and communicate the information gathered from the monitored field wirelessly to a centralized point (sink) that can use it locally, or it is connected to other networks through a gateway. A wireless sensor network is composed of large number of dispersed autonomous devices which uses sensors to monitor physical or environmental changes in a geographical area, process this data and report the changes to a centralized point through a wireless communication network. Wireless technology has propagated the use of sensor networks in many applications. Sensor networks join small sized sensors and actuators with general purpose computing components [2].

A sensor node or a mote is a node which gathers information from fields performs some processing on that information and propagates this information with other connected nodes in the network. Gateways are the mediators that interface Motes with computers, personal digital assistants (PDAs), Internet and existing networks and protocols. Gateways may be considered as a proxy for the sensor network on the Internet. Application Manager is the software that connects to the gateways via some communication media like Internet or satellite link. Sink can be accessed by the user via communication link such as internet or satellite communication. Location of sink is mainly near the sensor field or well-equipped