



Institutional Sign In

All



ADVANCED SEARCH

Conferences > 2020 International Conference...

SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications

Publisher: IEEE

Cite This

Cite This

PDF

Syeda Mariam Muzammal; Raja Kumar Murugesan; Noor Zaman Jhanjhi; Low Tang Jung All Authors

Export to
Collabratec

Alerts

- Manage
- Content Alerts
- Add to
- Citation Alerts

More Like This

A Survey of IoT Routing Protocols based on Security and Trust Management
 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)
 Published: 2020

Trust Mechanism in IoT Routing
 2018 Second International Conference on Intelligent Computing and Control Systems (ICICCS)
 Published: 2018

Show More

Top Organizations with Patents on Technologies Mentioned in This Article

Abstract

Document Sections

- I. Introduction
- II. Routing In Iot Networks - Rpl
- III. Related Work
- IV. Smtrust–Trust-Based Secure Routing Protocol
- V. Comparison with Existing Models

Show Full Outline ▾

- Authors
- Figures
- References
- Keywords
- More Like This

Downl

PDF

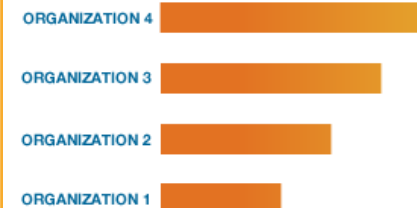
Abstract:With large scale generation and exchange of data between IoT devices and constrained IoT security to protect data communication, it becomes easy for attackers to compromi...[View more](#)

Metadata

Abstract:

With large scale generation and exchange of data between IoT devices and constrained IoT security to protect data communication, it becomes easy for attackers to compromise data routes. In IoT networks, IPv6 Routing Protocol is the de facto routing protocol for Low Power and Lossy Networks (RPL). RPL offers limited security against several RPL-specific and WSN-inherited attacks in IoT applications. Additionally, IoT devices are limited in memory, processing, and power to operate properly using the traditional Internet and routing security solutions. Several mitigation schemes for the security of IoT networks and routing, have been proposed including Machine Learning-based, IDS-based, and Trust-based approaches. In existing trust-based methods, mobility of nodes is not considered at all or its insufficient for mobile sink nodes, specifically for security against RPL attacks. This research work proposes a conceptual design, named SMTrust, for security of routing protocol in IoT, considering the mobility-based trust metrics. The proposed solution intends to provide defense against popular RPL attacks, for example, Blackhole, Greyhole, Rank, Version Number attacks, etc. We believe that SMTrust shall provide better network performance for attacks detection accuracy, mobility and scalability as compared to existing trust models, such as, DCTM-RPL and SecTrust-RPL. The novelty of our solution is that it considers the mobility metrics of the sensor nodes as well as the sink nodes, which has not been addressed by the existing models. This consideration makes it suitable for mobile IoT environment. The proposed design of SMTrust, as secure routing protocol, when embedded in RPL, shall ensure confidentiality, integrity, and availability among the sensor nodes during routing process in IoT communication and networks.

Published in: 2020 International Conference on Computational Intelligence (ICCI)



Date of Conference: 8-9 Oct. 2020

DOI: 10.1109/ICCI51257.2020.9247818

Date Added to IEEE Xplore: 09 November 2020 **Publisher:** IEEE

Conference Location: Bandar Seri Iskandar, Malaysia, Malaysia

ISBN Information:

Contents

I. Introduction

Internet of Things (IoT), as part of the fourth industrial revolution, is emerging in various areas and continuing to expand. Smart devices have been evolved in almost every field of human life. Factories, industries, and governments are adopting autonomous systems to increase efficiency, better production, and overall economic benefits. IoT involvement is further propagating in many other areas like healthcare, energy management, military, agriculture, supply chain and smart cities, aiming to build up a smart world.

Sign in to Continue Reading

Authors	▼
Figures	▼
References	▼
Keywords	▼

IEEE Personal Account

Purchase Details

Profile Information

Need Help?

Follow

CHANGE USERNAME/PASSWORD

PAYMENT OPTIONS

COMMUNICATIONS PREFERENCES

US & CANADA: +1 800 678 4333



[VIEW PURCHASED DOCUMENTS](#)

[PROFESSION AND EDUCATION](#)

[WORLDWIDE: +1 732 981 0060](#)

[TECHNICAL INTERESTS](#)

[CONTACT & SUPPORT](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE Account

- » [Change Username/Password](#)
- » [Update Address](#)

Purchase Details

- » [Payment Options](#)
- » [Order History](#)
- » [View Purchased Documents](#)

Profile Information

- » [Communications Preferences](#)
- » [Profession and Education](#)
- » [Technical Interests](#)

Need Help?

- » **US & Canada:** +1 800 678 4333
- » **Worldwide:** +1 732 981 0060
- » [Contact & Support](#)

[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [Sitemap](#) | [Privacy & Opting Out of Cookies](#)

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2020 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.