



All



ADVANCED SEARCH

Conferences > 2023 7th International Confer... ?

A Novel Trust Value Based Mobile Ad hoc Networks (MANETs) Security

Publisher: IEEE

Cite This

PDF

<< Results | < Previous

Sarumathi R ; Jayalakshmi V All Authors

6 Full Text Views



Alerts

Manage Content Alerts Add to Citation Alerts

Abstract



Document Sections

- I. Introduction
- II. Related Works
- III. Trust Value Based Security Model (TV-AODV) Trust
- IV. Algorithm for TS Model
- V. Example of Mathematical Analysis

Show Full Outline

Authors

Figures

References

Abstract: Mobile ad hoc networks, abbreviated as MANETs, are a type of self-configuring network in which several wireless nodes temporarily set up linkages between each other. Due ... **View more**

Metadata

Abstract:

Mobile ad hoc networks, abbreviated as MANETs, are a type of self-configuring network in which several wireless nodes temporarily set up linkages between each other. Due to the fact that MANET is a dynamic network, navigating it can be exceedingly difficult, and it is also more susceptible to a variety of attacks. Traditional security measures like cryptographic techniques need a significant consumption of resources like memory, speed, and transmission bandwidth in mobile ad-hoc networks and by Such methods make it impossible to identify malicious or flawed behaviour and self-centred nodes that damage the network. In Mobile ad-hoc Networks, trust methods are those that calculate the trust of mobile nodes and, as a result, help to identify malicious, selfish, and malfunctioning nodes Network. In this paper, a Trust Calculation based on nodes properties and recommendations are proposed to calculate trust for mobile Ad-hoc network. The proposed technique is very efficient to detect malicious and selfish nodes in MANET and allows trusted routing by eliminating malicious nodes. The findings of this research demonstrate that the proposed technique has a detection rate that is significantly greater than that of any other trust model used in Mobile ad-hoc networks. Routing protocols utilize trust mechanisms to identify a secure route in an efficient manner.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Metrics
More Like This

Date of Conference: 23-25 February 2023

INSPEC Accession Number: 22927585

Date Added to IEEE Xplore: 04 April 2023

DOI: 10.1109/ICCMC56507.2023.10084006

▼ **ISBN Information:**

Electronic ISBN:978-1-6654-6408-6

Publisher: IEEE

DVD ISBN:978-1-6654-6407-9

Conference Location: Erode, India

Print on Demand(PoD) ISBN:978-1-6654-6409-3

☰ **Contents**

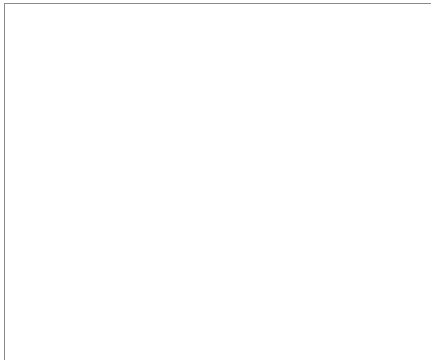
I. Introduction

The Mobile Ad-Hoc Network, also known as MANET, does not have an infrastructure that is pre-defined like the wired network does. During the process of packet relaying, it functions as essentially a self-configuring network in which temporary pathways are established between the nodes. The nodes perform the duties of both a host and a router following are some of the primary properties and characteristics of a MANET[1]: dynamic topology, cooperation, and resource constraints.

Sign in to Continue Reading

Authors	▼
Figures	▼
References	▼
Keywords	▼
Metrics	▼

< Previous | Back to Results



More Like This

Local Flooding-Based on-Demand Routing Protocol for Mobile Ad Hoc Networks

IEEE Access

Published: 2019

Hash-Based Anonymous Secure Routing Protocol in Mobile Ad Hoc Networks

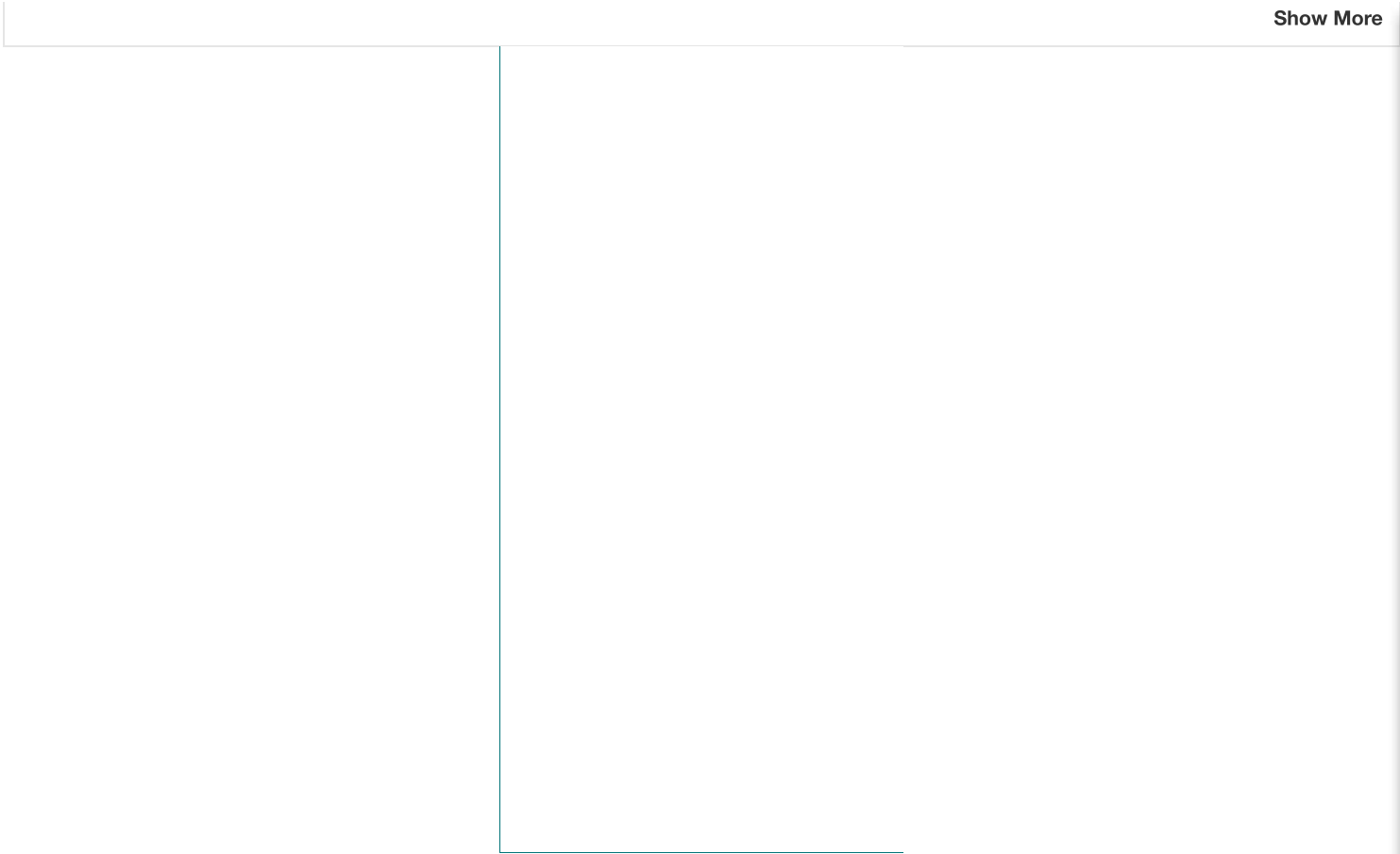
2015 10th Asia Joint Conference on Information Security

Published: 2015

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our Privacy Policy.

Accept & Close

Show More



IEEE Personal Account

CHANGE USERNAME/PASSWORD

Purchase Details

PAYMENT OPTIONS
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

Follow



[About IEEE Xplore](#) | [Contact Us](#) | [Help](#) | [Accessibility](#) | [Terms of Use](#) | [Nondiscrimination Policy](#) | [IEEE Ethics Reporting](#) | [Sitemap](#) | [IEEE Privacy Policy](#)

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

© Copyright 2023 IEEE - All rights reserved.

IEEE Account

- » Change Username/Password
- » Update Address

Purchase Details

- » Payment Options
- » Order History

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close

- » [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 2023 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

IEEE websites place cookies on your device to give you the best user experience. By using our websites, you agree to the placement of these cookies. To learn more, read our [Privacy Policy](#).

Accept & Close