South Asian Journal of Science and Technology

Open Access Full Text Article 152(2025) 117-122 DOI: 10.26524/sajet.2025.15.12

Path Mechanism in a WSN by means of Discriminative authentication Based Opportunistic Routing

[1]J.Jensya, [2]B.Subhashri

[1]Assistant Professor, [2]PG Scholar-First Year, Department of Computer Science and Engineering, Nandha College of Technology, Perundurai , Tamilnadu , India.

Corresponding author.
Correspondence: B.Subhashri

Article info
Received 5th December 2024 Received in revised form 21 March 2025
Accepted 1 May 2025

https://sajet.in/index.php/journal/article/view/327

Abstract
Wireless sensor networks (WSNs) have been developed in the Internet of Things (IoT) and play an important role to provide a wide range of applications through sensors, such as smart home, traffic management, smart grids and environment monitoring.
To promise reliable data delivery, existing works exploit geographic opportunistic routing with multiple candidate forwarders in WSNs. However, these approaches suffer from Denial of Service (DoS) attacks, in which a large number of invalid data are delivered to receivers to disturb normal operations of WSNs. This project proposes a selective authentication-based geographic opportunistic routing (SelGOR) to defend against the DoS attacks, satisfying the requirements of authenticity in WSNs.
By analyzing statistic state information (SSI) of wireless links, SelGOR leverages an SSI-based trust model to improve the efficiency of data delivery. Unlike previous opportunistic routing protocols, SelGOR ensures data integrity by developing an entropy-based selective authentication algorithm, and is able to isolate DoS attackers and reduce the computational cost.

1. INTRODUCTION

Wireless sensor networks (WSNs) have been developed in the Internet of Things (IoT) and play an important role to provide a wide range of applications through sensors, such as smart home, traffic management, smart grids and environment monitoring [1], [2]. A wireless sensor network contains some receivers/sinks and a number of distributed sensor nodes which collaboratively collect and transmit data to perform a variety of missions. Built upon WSNs, providing reliable data delivery is usually expected for IOT-based applications. As one of the traditional routing protocols, geographic routing is an attractive choice with regard to dynamic wireless links, since it does not need to establish and maintain paths from source nodes to sinks. Therefore, the combination of geographic routing and opportunistic routing has been referred to as geographic opportunistic routing. Existing geographic opportunistic routing approaches can achieve high reliability over wireless links. Suffer from serious Denial of Service (DoS) attacks. Malicious attackers may deliberately send a large number of invalid data with illegitimate signatures to sinks, aiming to waste the network resources and disrupt the normal operations of WSNs. In particular, opportunistic routing aggravates DoS attacks that invalid data can be reliably delivered to receivers with multiple candidate forwarders, which will be validated by our theoretical analysis and experiment results in the latter part of this paper. To defend against such attacks, we need a security authentication scheme, which can guarantee that data packets are sent from legitimate sensor nodes, and they are not sourced or modified by attackers during transmissions.

2. System Analysis

All the existing system approaches are carried out. In addition, trust worthy factor based routing is also considered. In on-demand routing protocols, it is argued that if a node has monitored a route reply (RREP) packet then it must have monitored its corresponding route request (RREQ) packet. The cross-correlation between RREP and RREQ monitored packets with respect to a source and destination pair reveals the behavior of nodes in the MANET.

Similar cross-correlation can also be established with route error (RERR) and RREQ control packets. Further, by monitoring the acknowledgment (ACK) and DATA packets received and forwarded by a node that is destined to some other node can lead to conclusive information about that node. Similar cross-correlation can also be established with DATA packets and RREP control packets. Such cross-correlation from the monitored traffic is instrumental in detection of malicious nodes by the monitor in MANET.

3. Features of The Common Language Runtime

The common language runtime manages memory; thread execution, code execution, code safety verification, compilation, and other system services these are all run on CLR.

- Security
- Robustness
- Productivity
- Performance

4. Security

The runtime enforces code access security. The security features of the runtime thus enable legitimate Internet-deployed software to be exceptionally feature rich. With regards to security, managed components are awarded varying degrees of trust, depending on a number of factors that include their origin to perform file-access operations, registry-access operations, or other sensitive functions.

5. Robustness

The runtime also enforces code robustness by implementing a strict type- and code-verification infrastructure called the common type system(CTS). The CTS ensures that all managed code is self-describing. The managed environment of the runtime eliminates many common software issues.

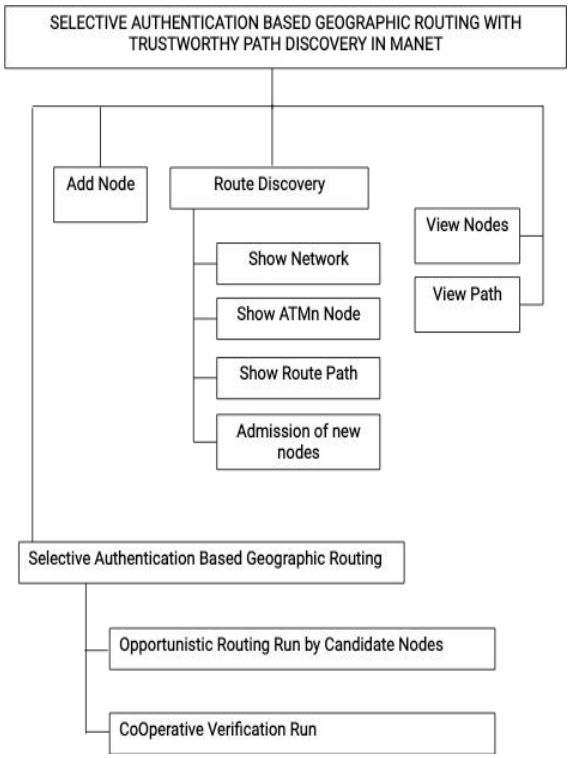
6. Productivity

The runtime also accelerates developer productivity. For example, programmers can write applications in their development language of choice, yet take full advantage of the runtime, the class library, and components written in other languages by other developers.

7. Performance

The runtime is designed to enhance performance. Although the common language runtime provides many standard runtime services, managed code is never interpreted. A feature called just-in-time (JIT) compiling enables all managed code to run in the native machine language of the system on which it is executing. Finally, the runtime can be hosted by high-performance, server-side applications, such as Microsoft® SQL Server™ and Internet Information Services (IIS).

8. System Flow Diagram



9. Route Discovery

(A) SHOW NETWORK
(B) SET ATMn
(C) ROUTE REQUEST (RREQ)
(D) ROUTE REPLY(RREP) AND TRUST REQUEST (TREQ)
(E) TRUST REPLY(TREP)
(F) TRUST EVALUATE (TEVAL)

10.1 Details

Add Node

In this form, the node details are added so that the network can be drawn in route discovery process. The node contains id, isSource node, isATMn node and isDestination node details. All the nodes can be viewed in nodes list.

ROUTE DISCOVERY

(A) SHOW NETWORK

In this form, a network is 'n' nodes is drawn and given as input for the algorithm process. The first node is taken as 'Source Node' and last node is taken as 'Destination Node'.

(B) SET ATMn

The Node with ID '2', '3' or '4' which is immediate right node is taken as ATMn Node. Then Route discovery process continues. For sake of convenience, the node with ID '2' or '4' is randomly chosen as ATMn node.

(C) ROUTE REQUEST (RREQ)

All neighbors of the ATMn are calculated through algorithm step and further forwarding the RREQ message to their neighbors is carried on, until either the destination or an intermediate Mobile Node with a fresh route to the destination and path trustworthiness above PATH THRESHOLD is reached.

(D) ROUTE REPLY (RREP) AND TRUST REQUEST (TREQ)

During the process of sending/forwarding the RREP message, every Mobile Node in the reverse path broadcasts trust request (TREQ) message, shouting for trust value of the nexthop Mobile Node in the upstream from its neighbors. The broadcast is only to one-hop Mobile Nodes

(E) TRUST € REPLY (TREP)

Upon receipt of TREQ message, the neighbors broadcast trust reply (TREP) message with trust value of the upstream Mobile Node in their respective node trust table. The broadcast is only to one-hop Mobile Nodes.

(F) TRUST EVALUATE (TEVAL)

In order to evaluate the trustworthiness of the discovered path, the ATMn of the source Mobile Node unicasts trust evaluate (TEVAL) message to the destination with a FLAG set. The FLAG is set to ensure that its acknowledgment is only from the destination node.

11. Related Work

Internet of Things in Industries: A Survey

AUTHORS

Li Da Xu, Wu He and Shancang Li

In the paper [1] the authors stated that Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID),and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years. In an effort to understand the development of IoT in industries, this paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges.

A main contribution of this review paper is that it summarizes the current state-of-the-art IoT in industries systematically. Index Terms—Big data analytics, enterprise systems, information and communications technology (ICT), industrial informatics, internet of things (IoT), near field communications, radiofrequency identification (RFID), wireless sensor networks (WSNs).

As an emerging technology, the Internet of Things (IoT) is expected to offer promising solutions to transform the operation and role of many existing industrial systems such as transportation systems and manufacturing systems. For example, when IoT is used for creating intelligent transportation systems, the transportation authority will be able to track each vehicle's existing location, monitor its movement, and predict its future location and possible road traffic.

The term IoT was initially proposed to refer to uniquely identifiable interoperable connected objects with radio-frequency identification(RFID) technology[11]. Later on, researchers relate IoT with more technologies such as sensors, actuators, GPS devices, and mobile devices.

Today, a commonly accepted definition for IoT is a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [12].

Specifically, the integration of sensors /actuators, RFID tags, and communication technologies serves as the foundation of IoT and explains how a variety of physical objects and devices around us can be associated to the Internet and allow these objects and devices to cooperate and communicate with one another to reach common goals [13]. There is a growing interest in using IoT technologies in various industries [14]. A number of industrial IoT projects have been conducted in areas such as agriculture, food processing industry, environmental monitoring, security surveillance, and others.

Meanwhile, the number of IoT publications is quickly growing. The authors conducted an extensive literature review by examining relevant articles from five major academic databases (IEEE

Xplore, Web of Knowledge, ACM digital library, INSPEC, and Science Direct) in order to help interested researchers understand the current status and future research opportunities regarding the use of IoT in industries. Their review focused on both identifying the breadth and diversity of existing IoT research in the industrial areas and highlighting the challenges and opportunities for future researchers.

As a result, they found a large number of journal articles and conference papers related to IoT. For example, they found 306 IoT-related journal articles published from 2009 to 2013 by searching the Web of Knowledge database alone.

12. Conclusion and Future Enhancements

The proposed solution has not only made the feasibility for placement of firewalls to thwart security threats that are common to wireline networks, but also exploited dynamic and cooperative features of MANETs to deal with misbehaving nodes in discovering trustworthy path. The simulation application works well for given tasks in network environment. Any system with .Net framework installed can execute the application. The application reduces the difficulties in the existing system. It is developed in a user-friendly manner. The application is very fast and any transaction can be viewed or retaken at any level. The project provides a best assistance in trust worthy path discovery in MANETs. The following options can be added in future.

In future, cross-correlation of monitored traffic under mobility scenarios can be studied. The developed application can be designed as a web site so that it can be accessed across the platforms. The route discovery application if developed as web service, then many applications can make use of it. The new system becomes useful if the above enhancements are made in future. The new system is designed such that those enhancements can be integrated with current modules easily with less integration work.

In addition, investigation regarding the problem of flooding based on topological information can be carried out. To collect neighborhood topology the network incurs a heavy overhead penalty- it is very costly to collect accurate topology information with node mobility and dynamically changing resources. The aforementioned topology based schemes, in consequence, are limiting in scalability and performance. Flooding scheme based on passive clustering removes such limitations but has some overhead and delay in transmission; it is also complex for implementation. When the number of nodes is more, then the flooding scenario can be avoided by improving the trustworthiness path discovery process.

REFERENCES

1. Alistair Mc Monnies, "**Object-oriented programming in VisualC#. NET**", Pearson Education, and ISBN: 81-297-0649-0, First Indian Reprint 2004.
2. Robert D.Schneider, Jetty R.Garbus, "**Optimizing SQL Server**", Second Edition, Pearson Education Asia, ISBN: 981-4035-20-3
3. Herbert Schildt, "C# 2.0, The Complete Reference, Osborne Complete Reference Series.
4. Meantel, J., "**A Computational Approach to client sever communication**", IEEE Trans. Pattern Analysis and Machine Intelligence, 8:679-714, November 1999.
5. V.S. Suresh kumar "Frequent Pattern Complex query management using FIUT Approach", South Asian Journal of Engineering and Technology, pp: 300-304, issue 204, volume 202, 2018
6. Sureshkumar V S, Chandrasekar A," Fuzzy-GA Optimized Multi-Cloud Multi-Task Scheduler For Cloud Storage And Service Applications" International Journal of Scientific & Engineering Research, Vol.04, Issue.3,pp-1-7, 2013
7. E.Prabhakar,V.S.Sureshkumar, Dr.S.Nandagopal, C.R.Dhivyaa, Mining Better Advertisement Tool for Government Schemes Using Machine learning " , International Journal of Psychosocial Rehabilitation, Vol.23,Issue.4, pp. 1122-1135, 2019

8. Suresh kumar V S ,Thiruvankatasamy S, Sudhakar R, "Optimized Multicloud Multitask Scheduler For Cloud Storage And Service By Genetic Algorithm And Rank Selection Method", Vol.3,Issue.2, pp.1-6, 2014
9. Nandagopal S, Malathi T, "Enhanced Slicing Technique for Improving Accuracy in Crowd Sourcing Database", International Journal of Innovative Research in Science, Engineering and Technology, Vol.3,Issue.1, pp.278-284, 2014
10. V.S. Suresh kumar "E-Farming by means of E-Mandi Process", International Journal of Research and Advanced Development (IJRAD), ISSN: 2581-4451, pp: 55-57, Issue 6, volume 2, 2019
11. Dr.C.R. Dhivyaa, R. Sudhakar, K. Nithya and E. Prabhakar "Performance Analysis of Convolutional NeuralNetwork for Retinal Image Classification", International Journal of Psychosocial Rehabilitation, Vol. 23, no.4, pp.1149-1159,November 2019.
12. V.S. Sureshkumar K. Boobesh , G. Dhatchayan , S. Karthick raja , R. Ajayeswaran" A High-Efficient Joint 'Cloud-Edge' Aware Strategy for Task Deployment and Load Balancing" south asian journal of engineering and technology, Vol. 13, issue no.1, pp. 22-38,November 2024.
13. P.Dhatchana Moorthy, J.Jenshya, V.S Suresh kumar, F.Christopher Jerome, A.S Mahant, N. M Vallarasu. "Early Breast Cancer Detection and Diagnosis Using An Efficient net-Based Predictive System", Second International Conference on Advances in Modern Age Technologies for Health and Engineering Science, 2025.