Patent Search

Invention Title	SECURE DATA TRANSMISSION PROTOCOL FOR IOT DEVICES USING ADAPTIVE SPREAD SPECTRUM TECHNIQUES
Publication Number	39/2025
Publication Date	26/09/2025
Publication Type	INA
Application Number	202521087316
Application Filing Date	14/09/2025
Priority Number	
Priority Country	
Priority Date	
Field Of Invention	COMMUNICATION
Classification (IPC)	H04L0009400000, H04L0067120000, H04L0009080000, H04L0009320000, H04L0009000000

Inventor

Name	Address	Country
Dr. Ahmed Sajjad Khan	Professor, Department of Electronics & Telecommunication Engineering, Anjuman College of Engineering and Technology, Sadar, Nagpur, Maharashtra, India. Pin Code: 440001	India
Mrs. M. Swarnalatha	Assistant Professor, Department of AI, Anurag University, Venkatapur, Ghatkesar- Medchal, Telangana, India. Pin Code: 500088	India
Dr. Mahesh Shyamsunder Darak	Assistant Professor, School of Computational Sciences, Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, India. Pin Code: 431606	India
Mr. Dharavath Veeraswamy	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Dundigal, Medchal-Malkajgiri, Hyderabad, Telangana, India. Pin Code: 500043	India
Mrs. N. Sujata Kumari	Assistant Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, Ranga Reddy District, Telangana, India. Pin Code: 500075	India
Dr. Devathoti Rajendra Prasad	Professor & HOD, Department of ECE, St. Ann's College of Engineering & Technology, Chirala, Bapatla District, Andhra Pradesh, India. Pin Code: 523187	India
Mr. Ch. Rakesh	Assistant Professor, Department of Computer Science & Engineering-AI&ML, GMR Institute of Technology, Rajam, Vizianagaram, Andhra Pradesh, India. Pin Code: 532127	India
Dr. S. Vinod Kumar	Associate Professor, Department of Chemical Engineering, St.Joseph's College of Engineering, OMR Road, Chennai, Tamil Nadu, India. Pin Code: 600119	India
Dr. Ch. Raja	Associate Professor, Department of ECE, Mahatma Gandhi Institute of Technology, Hyderabad, Ranga Reddy District, Telangana, India. Pin Code: 500075	India
Dr. Anandbabu Gopatoti	Professor & Ho D, Department of Electronics and Communication Engineering, Welfare Institute of Science, Technology & Management, Pinagadi, Visakhapatnam, Andhra Pradesh, India, Pin Code: 530047	India

Applicant

Name	Address	Country
Dr. Ahmed Sajjad Khan	Professor, Department of Electronics & Telecommunication Engineering, Anjuman College of Engineering and Technology, Sadar, Nagpur, Maharashtra, India. Pin Code: 440001	India
Mrs. M. Swarnalatha	Assistant Professor, Department of AI, Anurag University, Venkatapur, Ghatkesar- Medchal, Telangana, India. Pin Code: 500088	India
Dr. Mahesh Shyamsunder Darak	Assistant Professor, School of Computational Sciences, Swami Ramanand Teerth Marathwada University, Nanded, Maharashtra, India. Pin Code: 431606	India
Mr. Dharavath Veeraswamy	Assistant Professor, Department of Electronics and Communication Engineering, Institute of Aeronautical Engineering, Dundigal, Medchal-Malkajgiri, Hyderabad, Telangana, India. Pin Code: 500043	India
Mrs. N. Sujata Kumari	Assistant Professor, Department of Computer Science and Engineering, Sridevi Women's Engineering College, Hyderabad, Ranga Reddy District, Telangana, India. Pin Code: 500075	India
Dr. Devathoti Rajendra Prasad	Professor & HOD, Department of ECE, St. Ann's College of Engineering & Technology, Chirala, Bapatla District, Andhra Pradesh, India. Pin Code: 523187	India
Mr. Ch. Rakesh	Assistant Professor, Department of Computer Science & Engineering-AI&ML, GMR Institute of Technology, Rajam, Vizianagaram, Andhra Pradesh, India. Pin Code: 532127	India
Dr. S. Vinod Kumar	Associate Professor, Department of Chemical Engineering, St.Joseph's College of Engineering, OMR Road, Chennai, Tamil Nadu, India. Pin Code: 600119	India
Dr. Ch. Raja	Associate Professor, Department of ECE, Mahatma Gandhi Institute of Technology, Hyderabad, Ranga Reddy District, Telangana, India. Pin Code: 500075	India
Dr. Anandbabu Gopatoti	Professor & Ho D, Department of Electronics and Communication Engineering, Welfare Institute of Science, Technology & Management, Pinagadi, Visakhapatnam, Andhra Pradesh, India, Pin Code: 530047	India

Abstract:

[036] The present invention discloses a secure data transmission protocol for Internet of Things (IoT) devices using adaptive spread spectrum techniques, designed to confidentiality, integrity, and energy efficiency in resource-constrained environments. The protocol integrates lightweight cryptographic mechanisms with adaptive ph security through dynamically generated frequency hopping sequences and session-specific spreading codes. Synchronization between IoT devices and gateways is m using cryptographic timestamping and secure key exchange, enabling interference-resistant and jamming-resilient communication. Additionally, the system incorpora optimization strategies by adjusting transmission power and spreading factors based on channel conditions and battery availability. The invention provides a scalable layered security framework suitable for healthcare, industrial automation, smart cities, and defense applications, significantly enhancing the resilience and sustainabi networks. Accompanied Drawing [FIGS. 1-2]

Complete Specification

Description:[001] The present invention relates generally to the field of wireless communication systems and, more particularly, to secure data transmission protoc Internet of Things (IoT) devices. Specifically, the invention is directed toward methods and systems utilizing adaptive spread spectrum techniques integrated with lig cryptographic mechanisms to ensure confidentiality, integrity, interference-resilience, and energy efficiency in IoT communication networks.

BACKGROUND OF THE INVENTION

[002] The Internet of Things (IoT) has emerged as a transformative technology connecting billions of devices across diverse domains including healthcare, agricultur industrial automation, smart homes, and defense. These devices typically operate with limited computational resources, constrained memory, and low-power energ sources, yet they are expected to transmit sensitive data securely and reliably over wireless networks.

[003] Security in IoT communication is a critical challenge due to the open nature of wireless channels, which makes them vulnerable to eavesdropping, jamming, sp and replay attacks. Traditional cryptographic protocols, while secure in conventional computing environments, are often computationally intensive and unsuitable f lightweight IoT devices.

[004] Spread spectrum techniques, such as Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS), have long been utilized in m and satellite communication systems for their robustness against interference and interception. These techniques inherently increase security by spreading signals wider frequency band, making them harder to detect and jam.

[005] However, existing implementations of spread spectrum methods are typically static, meaning that hopping sequences or spreading codes remain predictable intercepted. This predictability can be exploited by adversaries, leading to vulnerabilities in otherwise secure communication systems.

View Application Status

Department of Industrial Policy and Promotion
Government of India

Terms & conditions (https://ipindia.gov.in/Home/Termsconditions) Privacy Policy (https://ipindia.gov.in/Home/Privacypolicy)
Copyright (https://ipindia.gov.in/Home/copyright) Hyperlinking Policy (https://ipindia.gov.in/Home/hyperlinkingpolicy)
Accessibility (https://ipindia.gov.in/Home/accessibility) Contact Us (https://ipindia.gov.in/Home/contactus) Help (https://ipindia.gov.in/Home/help)

Content Owned, updated and maintained by Intellectual Property India, All Rights Reserved.

Page last updated on: 26/06/2019