ವಿವೇಕಾನಂದ ತಾಂತ್ರಿಕ ಮಹಾ ವಿದ್ಯಾಲಯ
VIVEKANANDA INSTITUTE OF TECHNOLOGY
AN INSTITUTE OF JANATHA EDUCATION SOCIETY
Recognised by GOK, Affiliated to VTU & Approved by AICTE, New Delhi.

Index Sheet

SI NO	Particulars	Page Number
1	Year Wise Conference/Book Chapter Details	1
2	Conference/Book Chapter Front Pages-2022-2023	2-4
3	Conference/Book Chapter Front Pages-2021-2022	5-5
4	Conference/Book Chapter Front Pages-2020-2021	6-28
5	Conference/Book Chapter Front Pages-2019-2020	29-34
6	Conference/Book Chapter Front Pages-2018-2019	35-51

27/12/2023

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

3.3.2.1 Total number of Books and Chapters in edited volumes/books published and papers in national/international conference proceedings year wise during the last five years

SI NO	Year	Number
1	2022-2023	01
2	2021-2022	01
3	2020-2021	17
4	2019-2020	05
5	2018-2019	09
	Total	**33**

27|12|2023
Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

Introduction to
C Programming

Dr.Nandini N
Dr V Nagaveni
Dr P Vanajakshi
Dr Ravi Kumar J
Prof. Vani B. A.

INTRODUCTION TO C PROGRAMMING

FIRST EDITION

Authors

Dr. NANDINI .N

Dr. NAGAVENI .V

Dr. VANAJAKSHI .P

Dr. RAVI KUMAR .J

Prof. VANI B. A

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 0__

②

BOOK TITLE : INTRODUCTION TO C PROGRAMMINC

Edition: First - 2023

Copyrights © Authors

Disclaimer

27/12/2023
Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

MQTT based Secure Transport Layer Communication for Mutual Authentication in IoT Network

Shilpa V [a,*], Vidya A [a], Santosh Pattar [b]

[a] Dept of Computer Science and Engineering, Vivekananda Institute of Technology, Bangalore, India
[b] Dept of Information Science and Engineering, BMS Institute of Technology, Bangalore, India

ARTICLE INFO

ABSTRACT

Recent advancements in the communication protocols and the networking technologies have enabled connectivity of a wide range of objects, resulting in the Internet of Things (IoT) network. The protocols like MQ Telemetry Transport (MQTT), as well as Constrained Application Protocol (CoAP) are moderately capable of providing the management of heterogeneous wireless sensor networks even in an environment with very limited bandwidth. In this paper, we develop a lightweight encryption algorithm to obtain reliable secure data transmission between IoT devices. We propose a Secure Reliable Message Communication (SEC-RMC) protocol using Mosquitto MQTT message broker with cryptographic enhancements to offer security services and also provide the mutual authentication in the IoT environment at the transport layer. The proposed scheme decreases the number of messages transmitted between the devices. Also, the authentication scheme provides resistance to DNS hacking, routing table poisoning and packet mistreatment. On comparison with the existing methods, the transmission time has been reduced by 80% in this work.

1. Introduction

The Internet of Things (IoT) includes objects with recognizable characteristics that are associated to the Internet. The diversity of existing devices, such as PCs and networked computers, or 4G-enabled mobile devices, as well as their internet connected nature, make them unique and valuable. The IoT network is defined by the frameworks and organization of interconnected devices. As a result of the advancements in sensor networks, mobile gadgets, wireless devices, networking, and cloud technologies, there has been a revaluation of the capabilities of endpoints that are connected to the internet. In 2025, experts estimate that 50 billion nodes/things will be able to communicate with the internet and be connected [1].

IoT doesn't merely involve connecting devices to the Internet. As machines, appliances, etc., can also be interconnected. The IoT network makes it possible for these objects to converse and exchange information while executing large applications to achieve a common goal. In various developments scopes, from a minute single object to a large collection of dissimilar objects, the characteristics as well as the deployment process keeps on changing.

One of the important characters among these are the transmission and security of the data. The rapid evolution of the communication protocols has augmented the growth of the IoT network for communication as well as other such computing applications. Thus, there is a need for a secure and reliable data communication technique that can be achieved based on an efficient routing protocol [2–7]. The routing scheme has to handle the following issues.

- Reduce irrelevant and duplicate data during data transmission.
- Avoid data loss near the receiver end.
- Select a secure and reliable path from source to destination.

In this paper, we propose a Secure Reliable Message Communication (SEC-RMC) protocol. It works on the principles of generating and communication of the data based on publisher/subscriber model. The SEC-RMC protocol is lightweight and secured. It works on top of the MQTT Protocol as shown in Fig. 1.

The major contributions of the paper are as follows.

- IoT nodes are initially separated into the network using MQTT pub/sub. Next, In Mosquito MQTT, a node is selected and an event is detected.
- Getting distance and node in/out degrees by using the private key of the publisher and the subscriber topic.
- The proposed method minimizes the chance of packet mishandling over the network, as the Mosquitto MQTT broker routes around malicious nodes.

KeAi
CHINESE ROOTS
GLOBAL IMPACT

MQTT based Secure Transport Layer Communication for Mutual Authentication in IoT Network [☆]

Shilpa V [a,*], Vidya A [a], Santosh Pattar [b]

[a] Dept of Computer Science and Engineering, Vivekananda Institute of Technology, Bangalore, India
[b] Dept of Information Science and Engineering, BMS Institute of Technology, Bangalore, India

ABSTRACT

Recent advancements in the communication protocols and the networking technologies have enabled connectivity of a wide range of objects, resulting in the Internet of Things (IoT) network. The protocols like MQ Telemetry Transport (MQTT), as well as Constrained Application Protocol (CoAP) are moderately capable of providing the management of heterogeneous wireless sensor networks even in an environment with very limited bandwidth. In this paper, we develop a lightweight encryption algorithm to obtain reliable secure data transmission between IoT devices. We propose a Secure Reliable Message Communication (SEC-RMC) protocol using Mosquitto MQTT message broker with cryptographic enhancements to offer security services and also provide the mutual authentication in the IoT environment at the transport layer. The proposed scheme decreases the number of messages transmitted between the devices. Also, the authentication scheme provides resistance to DNS hacking, routing table poisoning and packet mistreatment. On comparison with the existing methods, the transmission time has been reduced by 80% in this work.

1. Introduction

The Internet of Things (IoT) includes objects with recognizable characteristics that are associated to the Internet. The diversity of existing devices, such as PCs and networked computers, or 4G-enabled mobile devices, as well as their internet connected nature, make them unique and valuable. The IoT network is defined by the frameworks and organization of interconnected devices. As a result of the advancements in sensor networks, mobile gadgets, wireless devices, networking, and cloud technologies, there has been a revaluation of the capabilities of endpoints that are connected to the internet. In 2025, experts estimate that 50 billion nodes/things will be able to communicate with the internet and be connected [1].

IoT doesn't merely involve connecting devices to the Internet. As machines, appliances, etc., can also be interconnected. The IoT network makes it possible for these objects to converse and exchange information while executing large applications to achieve a common goal. In various developments scopes, from a minute single object to a large collection of dissimilar objects, the characteristics as well as the deployment process keeps on changing.

One of the important characters among these are the transmission and security of the data. The rapid evolution of the communication protocols has augmented the growth of the IoT network for communication as well as other such computing applications. Thus, there is a need for a secure and reliable data communication technique that can be achieved based on an efficient routing protocol [2–7]. The routing scheme has to handle the following issues.

- Reduce irrelevant and duplicate data during data transmission.
- Avoid data loss near the receiver end.
- Select a secure and reliable path from source to destination.

In this paper, we propose a Secure Reliable Message Communication (SEC-RMC) protocol. It works on the principles of generating and communication of the data based on publisher/subscriber model. The SEC-RMC protocol is lightweight and secured. It works on top of the MQTT Protocol as shown in Fig. 1.

The major contributions of the paper are as follows.

- IoT nodes are initially separated into the network using MQTT pub/sub. Next, In Mosquito MQTT, a node is selected and an event is detected.
- Getting distance and node in/out degrees by using the private key of the publisher and the subscriber topic.
- The proposed method minimizes the chance of packet mishandling over the network, as the Mosquitto MQTT broker routes around malicious nodes.

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

FTRAT: Fault-Tolerant Routing Based on Aggregation Tree to Improve the QoS in Wireless Sensor Networks

P. Manasa, K. Shaila, and K. R. Venugopal

Abstract Wireless sensor network is one of the effective communication fields due to its capability of performing functionalities such as sensing, aggregation and other computational activities. Cluster formation among the deployed sensor nodes has shown to be an effective method in saving life of the network. Cluster head selected supervises other nodes in the network and plays a vital role in data transmission. Since cluster head is responsible of monitoring the whole cluster, so cluster heads are more crucial in the network. If defective cluster head is present in the network, transmission in the network will be worst hit. In the proposed work, the network failure due to defective cluster head can be overcome by considering backup cluster head in the network. Flawless cluster member node energy is coordinated to form the backup cluster head. Aggregation tree formation among the cluster head and backup cluster head in case of cluster head failure in the network helps to improve QoS by adopting beneficiary path from cluster head to the sink.

Keywords Aggregation tree · Backup cluster head · Cluster head · Quality of service (QoS) · Routing and wireless sensor networks

1 Introduction

Wireless sensor networks (WSNs) frequently update to sink node by monitoring the deployed sensor devices. Routing of data from sensor to sink is carried out productively by adopting effective routing methods. Effective routing methods like

P. Manasa (✉)
Research Scholar, Department of Electronics and Communication Engineering, VTU-RC, Vivekananda Institute of Technology, Bengaluru, India

K. Shaila
Professor, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru, India

K. R. Venugopal
Vice-Chancellor, Bangalore University, Bengaluru, India

Logistic and Tent Map Encrypted Image Steganography in Transformation Domain using DWT-LSB Technique

Shashikiran B S
Research Scholar
VTU-RC, Department of Electronics
and Communication
Vivekananda Institute of Technology,
Bengaluru, India
shashikiran.bisileri@gmail.com

Shaila K
Professor
Department of Electronics
and Communication
Vivekananda Institute of Technology,
Bengaluru, India
shailak17@gmail.com

Venugopal K R
Vice Chancellor
Bengaluru University
Bengaluru, India

Abstract - **The data confidentiality in an image is predominant in digital-world and outstretching the importance. Steganography and Cryptography are generally used for securing information. The security level is enhanced by encrypting the secret image using dual chaotic system models to generate random encryption sequences using Logistic and Tent map in proposed algorithm. The encrypted image is inserted into another image in transformation domain using DWT-LSB steganography techniques. Proposed method is robust and providing high information security with a good SSIM and PSNR for encryption process and embedding process respectively.**

Keywords— Cryptography, chaotic system, Logistic, PSNR, SSIM, Steganography, Tent Map.

I. INTRODUCTION

The commercialization and continuous development of digital technology has reformed the processing of secret data for protection and security. Everything is headed in the direction of smart epoch driven by digital world intending to have data at finger tips. Each second approximately millions of data exchanged over the internet in different forms such as, text, audio, video or image. Information in images are effervescent and visually striking than data represented in text. personal and sensitive data or data related to defense or medical data or documents related to an organization need to be secured from unauthorized person when it is circulated and shared across internet.

Steganography [1] is a technique to hide data into multimedia without leaving any noticeable falsification. Cryptography [2] is a process of protecting data from unauthorized persons using codes such that only intended person can decode the protected data. With the expeditious growth in digital technology and network technology, digital images have become imperative medium for data storage and transmission. Ensuring the indemnity of information plays significant role. If the information is stolen from an industry or an organization, it will have immense deprivation. Cryptography and steganography techniques can encrypt and embed data, even if the data is stolen, unauthorized person cannot recover the real data. Steganography means protected and covered writing and is originated [3] from Greek words 'Steganos' means covered or protected and 'graphia' means writing. Ssteganography methods used for embedding information are text, image, audio and video steganography. However, different types of steganography mentioned can be combined to secure the secret data [4]. Image steganography is a predominant digital steganography used in various applications. Cryptography falls into two categories, symmetric-key cryptography uses the same key for both encryption and decryption, asymmetric-key cryptography where different keys are used. With the rise in usage of image for data or information sharing, image encryption expedited lot of demand in digital world. Numerous cryptographic and steganographic algorithms are developed and are in widely used. With the development of encryption and embedding algorithms, counter attacks are also advanced and hence securing data from unauthorized person is a recursive development with new steganography and cryptography methods. The conventional encryption process such as, AES, DES, blowfish algorithms are suitable for encrypting text data but, these algorithms turns out to be deficient when used for image encryption due to intrinsic characteristics of image like high redundancy, strong correlation and so on. Steganography happens to be better for securing the image by embedding in another image. Integrating steganography with cryptography results in high security for data.

Chaotic theory [5] concerns deterministic models whose behavior can be predicted for a while and then appears to become random. The chaotic system [6] has better properties in data encryption since chaotic systems are sensitivity to control parameter and initial value condition. Chaotic system has some complex properties and pseudo randomness that used in generation of secured and robust encryption algorithms. Chaotic system includes, Logistic map, Arnold Cat map, Lorenz, Henon map, Tent map and other models. The attractiveness of developing chaotic models in implementation of crypto systems is due to fact that a chaotic model is characterized by: (a) High sensitivity to control parameter and initial condition. (b) Randomness and unpredictability. (3) ease for implementation.

DWT [7] is used to reshape the spatial domain information in to transformation domain information. When a DWT is performed on image it is decomposed into 4 sub bands called LL-Approximation band, LH-Horizontal band, HL-Vertical band and HH-Diagonal band. Approximation band contains the most significant features of an image. Rest three bands contains less information of the image that can be utilized for inserting secret information.

Proposed work is focused towards providing security to an information by encrypting and inserting secret image data into cover image. Many algorithms are in place to provide

SN

Cross Layer Design for Wi-Fi Sensor Network Handling Static and Dynamic Environment Using Local Automate Based Autonomic Network Architecture

K. N. Sanjay[1] · K. Shaila[1] · K. R. Venugopal[2]

Abstract

In social activities with shared Wi-Fi needs to accommodate large number of users and effectively handle congestion. These are critical issues due to the presence of larger density nodal activity at nearby access points involving inter-technology interference. An interference involves a statistical approach in monitoring access points with its received errors. The received errors vary with frame reception at their fields like PHY, MAC headers and payloads. Local automate-based Autonomic Network Architecture a cross layer approach algorithm is proposed to channelize a frame reception and can effectively avoid inter-technology interference. This results in P2P communication at initial stages and can accommodate multiple mobile devices with varying signal strengths. The algorithm is deployed for a dynamic environment along with static clusters. The throughput of the entire network is increased by 20% because of identifying multiple nodes with lesser latency avoiding congestion.

Introduction

The deployment and its popularity of Wireless Sensor Network provides users to think beyond its timeliness. The classification of WSN starts from few meters to several kilometers. With higher distance coverage Wireless Fidelity(Wi-Fi) is among the one with good reliability features in practical applications. Wi-Fi operating rages from 900MHz, 2.4 GHz, 3.6 GHz, 4.9 GHz, 5 GHz, 5.9 GHz and 60 GHz bands. The 2.4 GHz is considered as it can be found in most of the industrial applications handling a larger density of nodes. The process looks simple if the area is not set as a constraint

in using Wi-Fi. The collision and congestion can be easily avoided with larger space and high bandwidth compared to UWB, Bluetooth or even ZigBee [1–5].

The sensor network data with large density nodes in a smaller area with lesser collisions and congestion is considered. The use of Wi-Fi includes both static and dynamic environments. While in a smaller network including 5–15 nodes can be made dynamic. One such example is Wi-Fi Hot-spot using cellular phones. While with industrial applications are concerned it involves Wi-Fi stations with routers and larger number of nodes in a wide spread environment. The support by each level of design in a combined static and dynamic environment if fulfilled at a certain level based on strength of a signal and receiving nodes capability.

The data transfer rate differs from node to station level. Capturing the various strengthen in signal and transmitting at a required data rate requires user attention. To fill this gap between a various data rate operation a local automate based autonomic network architecture is proposed [6]. Local automate chooses nodes, routers based on their probability of occurrence.

The architecture provides modeling information and processing is task driven with the collaborative neighborhood.

✉ K. N. Sanjay
   sanjaykenkar@gmail.com

[1] Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bangalore, India

[2] Bangalore University, Bangalore, India

The 2nd International Workshop on Statistical Methods and Artificial Intelligence
IWSMAI'21
March 23 - 26, 2021, Warsaw, Poland

Designing WiMAX Static Environment using Local Automata based Autonomic Network Architecture for Wireless Sensor Networks

Sanjay K N[a,*], Shaila K[b], Venugopal K R[c]

[a]Research Scholar, VTU-RC, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru
[b]Professor, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru
[c]Vice Chancellor, Bangalore University, Bengaluru

Abstract

Smart grid applications requires network availability with lesser dark spots. The available qualitative requirements with dynamic nodes, static stations and routers need to be validated without collisions. This can reach to back-haul network with reachability of specific nodes and routers in Wireless Sensor Network. One method of solving the issue is to use local automate based environment for dynamic nodes. Advanced with static environment configuring address agnostic feature could bridge the gap between static and dynamic environments. The multicast probabilistic model using LA-ANA is proposed with quantified metrics in MAC layer to avoid congestion and dark spots in Wireless Sensor Networks. Thus, increasing throughput and fault tolerance levels with 10-15% supporting unicast and multicast delivery.

1. Introduction

The challenging area with significant ubiquitous computing for low cost networking platform are required using WiMAX. The mesh capability available in WiMAX helps user in forming multi-hop networks. The capacity is limited with varying coverage area and density of nodes. This also includes deployment and self-healing potential in resolving with suggested multiple routing paths. This attract various hardware and software constraints in handling static and dynamic network nodes. The entire network consists of nodes, routers and stations. Thus, channel with multimedia

* Corresponding author. Tel.: +0-000-000-0000 ; fax: +0-000-000-0000.
  E-mail address: sanjaykenkare@gmail.com

Improved Packet Delivery for Wireless Sensor Networks Using Local Automate Based Autonomic Network Architecture in a ZigBee Environment

K. N. Sanjay[1,2(✉)], K. Shaila[2], and K. R. Venugopal[3]

[1] Department of Electronics and Communication Engineering, VTU-RC, Vivekananda Institute of Technology, Bengaluru, Karnataka, India
sanjaykenkare@gmail.com
[2] Vivekananda Institute of Technology, Bengaluru, Karnataka, India
[3] Bangalore University, Bengaluru, Karnataka, India

Abstract. A low cost, low power personal area network is formalized by IEEE 802.15.4 standard ZigBee Wireless Sensor Network. The most common way to construct a WSN using ZigBee is to use tree type network topology. This leads to large amount of energy consumption because of congestion in network. The node failures in a network topology, results in reconstructing the route of existing structure. Thus, a Local automate based autonomic network architecture is deployed at the MAC layer of ZigBee protocol. The architecture considers previous occurrences of probabilities of nodes and learns their behavior during transmission. This record an active state of each node, that inturn reduces congestion when neighboring node failure occurs. Simulation results provide 20% increase in unicast and multicast delivery rate. Finally, throughput of an entire network in a larger density dynamic environment increases.

Keywords: Autonomic network architecture (ANA) · LACAS · Local automate (LA) · Wireless Sensor Network · ZigBee

1 Introduction

With the expanding modernity of remote correspondences and detecting advances, different sensor-based applications, like industrial robots and electro-mechanical mechanization, creates enormous monetary and social implications. The potential for much more prominent effect has broad investigations on WSNs with ZigBee standards. This determines the industrial system and application layers for detecting information delivery rate [1–3].

The process requires backbone network with static environment and related nodes that are mobile. These nodes rely on the available power supply. Normally, traffic information is overheard to the cluster of a tree and its responsibilities in considering larger

ORIGINAL RESEARCH

SN

SDAFPS: Secure Data Aggregation using Fuzzy Judgement, Pattern Category and SHAP Contribution

S. Reshma[1] · K. Shaila[2] · K. R. Venugopal[3]

Abstract

Secure data aggregation intends to reduce redundant data transmission and malicious node interference in the network. Therefore, designing secure data aggregation protocol is a crucial task in WSNs. In this paper, we have proposed a *Secure Data Aggregation using Fuzzy Judgement, Pattern Category and SHAP Contribution* (SDAFPS) protocol. The SDAFPS protocol involves three main phases. In the first phase, the protocol controls the topology with the selection of efficient aggregator node in every interval. The second phase uses category pattern code generation and utilization concept to reduce data size and to aggregate data. Finally, in third phase, the aggregated data are encrypted using partial equation of SHAP contribution and decrypted with SHAP contribution equation. The decrypted data are verified with dataset preserved at the sink node. The SDAFPS protocol is implemented using NS2 Simulator tool and performance of proposed protocol is compared with existing protocol and validated 18% improvement in network lifetime, 10% minimized End-to-End Delay and 14% improvement on Packet Delivery Ratio over protocol.

Keywords Data aggregation · End-to-end delay · Fuzzy judgement · Network lifetime · Packet delivery ratio · Pattern category · SHAP contribution

Introduction

In recent days, Wireless Sensor Network is emerging in a rapid manner in different fields, namely environment monitoring, military surveillance, health care industries, etc., [1–4]. WSN is composed of several tiny sensor nodes which are limited resource self-conscious devices. The resource restriction leads to various challenging issues via. security, data aggregation, congestion, etc. There are various secure data aggregation algorithms in WSNs. The data sensed from various sensor nodes are aggregated and forwarded to the destination [5, 6]. The aggregated data are protected from several intruders such as Denial-of-Service attack, blackhole attack and worm-hole attack [7]. The unbalanced distribution of transmission load in the network causes shorter network connectivity and drains sensors energy which leads to energy hole problem [8]. The efficient routing algorithm in [9] minimizes energy consumption and number of hops during data transmission.

Several existing algorithms focus on topology control to maximize network lifetime in WSNs. These algorithms are categorized as power control [11] and cluster head selection [12]. In [13] the energy consumption for data transmission is reduced by minimizing data size.

Contribution: The proposed protocol identified both security and data aggregation issue and designed topology balanced secure data aggregation protocol. The fuzzy judgment matrix is used to control topology to select an appropriate parent node which helps to handle the network disconnectivity issue. In the proposed protocol, category pattern code concept is used to divide the temperature range for regular interval threshold and assigning it instead of forwarding an original temperature. Then, sink handles dataset using SHAP

✉ S. Reshma
   reshnam211@gmail.com

1 Department of CSE, VTU-RRC, Belagavi, Karnataka, India

2 Department of ECE, Vivekananda Institute of Technology, Bengaluru, Karnataka, India

3 Bangalore University, Bengaluru, Karnataka, India

Published online: 10 February 2021

MIPSOE – Markov Integrated PSO Encryption Algorithm for Secure Data Aggregation

Reshma S[a], Shaila K[b], Thippeswamy B M[c], Venugopal K R[d]

[a]Research Scholar, VTU-RRC, Belagavi, Karnataka, India
[b]Professor, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bangalore, Karnataka, India
[c]Professor, School of Electrical Engineering and Computing, Science and Technology University, Adama, Ethiopia
[d]Vice Chancellor, Bangalore University, Bengaluru, Karnataka, India

ABSTRACT:Various clustering algorithm exists in Wireless Sensor Networks concerned on balancing energy utilization. Many research issues deviate towards the formation of clusters based on energy, distance, and another sensor node's resource parameters. In this article, the proposed protocol is composed of two phases. In the first phase, clusters are formed based on Particle Swarm Optimization and Markov's Random Field mathematical calculation. The second phase generates a key, where the secret key is used for encryption technique. The proposed protocol is implemented in the NS2 simulator. When comparing the existing protocol with the proposed MIPSOE protocol it is inferred that there is an improvement in terms of network lifetime, throughput, delay, and packet delivery ratio.

Keywords: Markov Random Field, Particles Swarm Optimization, Wireless Sensor Networks

1. Introduction

The sensor nodes are self-configured and are connected to the internet for communication, which is referred to as the Internet of Things. The Internet of Things is a part of Wireless Sensor Networks. Wireless Sensor Networks are open and unprotected communication channels between sensor nodes. The network is forced to several intruder attacks and also unprotected network sensor nodes are vulnerable to limited battery usage. Therefore, it is necessary to balance energy usage in the network without network disconnectivity.

The existing algorithms [1] LD^{2}FA-PSO designed a lightweight scheme to mitigate Black-hole attack [14], [2] mitigates multi-layer flooding attack and minimizes energy utilization by monitoring residual energy status and [3] detects Sybil attack in large WSNs and reduces false alarm rate. Reduced network clustering and balanced consumption clustering is a process of connecting sensor nodes into one group with one cluster head. There are different algorithms to form a cluster and to elect cluster heads such as LEACH [4], Particle Swarm Optimization [5], GSA [6], and MOEA [7].

These algorithms are a trade-off between energy, latency, and data protection. So, it is necessary to develop a mechanism that should be capable of monitoring energy, delay, and data protection. Therefore, in our work, a protocol is designed in such as to fulfil the constraints of WSNs. The protocol forms cluster with Integrating Particle Swarm Optimization and Markov Random Field concept and protects data with enhanced encryption technique which generates a key based on cluster and energy density.

The Particle Swarm Optimization algorithm searches for the optimal best path based on swarm intelligence. Initially, obtains the basic information about the sensor nodes and the environment and applies fitness function. The global best fitness value is considered to find the similarity of the sensor nodes and forms the clusters using the cosine similarity

MBSR: MIMO Based Sink Relocation for Path Selection in IoT Based WSN

Manasa P[a], Shaila K[b] and Venugopal K R[c]

[a]Research Scholar, VTU-RC, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru

[b]Professor, Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru

[c]Vice Chancellor, Bangalore University, Bengaluru.

Abstract: Wireless Sensor Networks have extended its functionalities by integrating with the Internet of Things and are highly proficient when it is incorporated with other technologies. This demands communication with lesser energy consumption and one such idea of low energy consumption is low energy path selection by a mobile sink node. Path selection requires a good Signal Interference Noise Ratio (SINR) which is calculated for the positioned mobile sink. Thus, a high-quality transmission path is selected by choosing a path to obtain better SINR. MBSR algorithm considers hierarchical clustering schemes and heads are elected to monitor the network. Heads of the clusters communicate to IoT applications using Multiple Input and Multiple Output Dual Antennas. The proposed MBSR scheme utilizes a path optimization technique and finds a suitable path to establish links to end user and real-time environments. The proposed MBSR mechanism employs three phases of execution. *Phase* 1: Cluster Creation, *Phase* 2: SINR Analysis for Path Selection. *Phase 3*: Data transmission to MIMO Devices and in turn forwards to static sinks that connect to end-user using the internet. MBSR improves transmission quality and the proposed scheme is tested for various network parameters to check transmission quality and is compared with existing methodologies.

Keywords: Hierarchical Clustering, IoT, MIMO, Signal Interference Noise Ratio, Wireless Sensor Network.

1. Introduction

Internet of Things (IoT) entrusts the connection of devices to establish communication among various applications. Due to the advancement of technology, WSNs can be easily integrated with other technologies and enable users to access various applications. IoT refers to remote sensing, gathering, and communication of information with the view of establishing a connection between real and computer domain. This provides better opportunities for mankind in accessing valuable resources resulting in effective economic utilization. IoT incorporates various devices for communication establishment from real-world to end-user [1] [2]. The IoT supported WSNs consist of sensing, data collection, accumulation, processing, and a communication unit. Data collection and accumulation of information in IoT devices should consume minimum energy [3].

Clustering in IoT refers to the grouping of IoT devices to collect and accumulate the information. It avoids the extra burden on IoT devices for repeated data transfers. In WSN-IoT, LEACH (Low Energy Adaptive Clustering Hierarchy) and other hierarchical protocols enable designing the routing effectively to achieve the quality of service. Different routing schemes are designed in Cluster Head selection (CH) to reduce the overhead in choosing of CH. Power-efficient routing technologies are in the foremost position for IoT applications. Energy balance in deployed devices helps to prolong the battery life of IoT devices. CHs functioning in the network should always utilize minimum hops to reach the information to sink node [5-6].

619

DMHCET: Detection of Malicious Node for Hierarchical Clustering based on Energy Trust in Wireless Sensor Network

Manasa P
Research Scholar, VKIT
Email: emanasagowda@gmail.com

Shaila K
Professor, VKIT
Email: shailak17@gmail.com

Venugopal K R
Vice Chancellor
Bangalore University

Abstract—**Wireless Sensor Networks are inhibited with the energy consumption and major role plays in improving the network lifetime. The hierarchical cluster zone formation helps in improving its lifetime of the network. The proposed work employs low energy clustering and hierarchical protocols that aims at providing secure path when the network is exposed to malicious attacks and shows improvement in QoS metrics like throughput, Packet Delivery Ratio, Routing Overhead and Network Lifetime**

Index Terms—**Hierarchical Clusters, Malicious attacks, QoS, Routing, Security, Wireless Sensor Networks.**

I. Introduction

Monitoring the information in the field using WSNs consists of arbitrary deployment of sensor nodes. This can examine the surrounding environment and process from monitoring field to the destination. Clustering achieves network's scalability and will lower the quantity of raw data that is communicated to the destination thereby saving the battery life[1]

Motivation: Hierarchical clustering of network is one of the effective ways to enhance the network lifetime of the cluster node. This can be achieved by sharing the monitoring responsibility at different levels in the network. It is highly necessary to follow secure transmission protocol for information exchange in the network[2].

Contribution: To achieve improvement in Network Lifetime, DMHCET protocol is proposed. DMHCET adopts the Hierarchical Clustering methods in the routing techniques. It also provides a secure transmission path, when the network is vulnerable to malicious attacks. This protocol avoids transmission through a node which has lesser energy and via malicious nodes in the network.

Organization: In section II, related work and their drawbacks are discussed. In section III, problem statement of clustering and black hole attack is explained. Section IV gives the detail of proposed techniques and the Network Model. Section V described the proposed DMHCET system. Section VI explains the simulation and section VII explains

and tabulates the obtained results. Finally, in Section VIII conclusions and references are discussed.

II. Related Works

SAIMA [3] *et al.*, proposed Mobility-Aware Clustering method for hierarchical network. The problem of node mobility in the clustered network is addressed in this algorithm. MCCA and MHCA create mobility awareness to the nodes by Time scheduling the movement within the network. Centralized hierarchy may overburden some part of the network.

Shoukat [4] *et al.*, describes the commonly found Black Hole Attacks in IOT and WSNs that are based on Hierarchical, trust, multi hop and secure routing. But the methods here are suitable to a particular application. Hence, methodology has to be designed to meet the energy, processing and computation power demands suitable for variety of applications

Mohamed [5] *et al.*, has proposed a method to resist Blackhole attacks on MANET. Blackhole Resisting Mechanism (BRM) is incorporated to resist malicious attacks. This protocol does not use cryptography or authentication mechanisms, instead uses timers and thresholds to identify malicious nodes. This protocol is able to detect and resist the malicious behavior of node within a short time span. Further, black hole attack can be applied as a resisting mechanisms to other reactive protocols.

Guangqian [6] *et al.*, has proposed Routing technique by formation of clusters for movable Sink in WSNs that includes obstacles. Heuristic tour-planning based on spanning graph methods are adopted in this above algorithm. Grid-based techniques are adopted to shorten the scheduling tasks during collection of information from the cluster heads. One such method is spanning graph algorithm that determines the shortest path from source to sink and avoids obstacles.

Salim [7] *et al.*, proposed Secured AODV Routing Protocol addressing the black hole attack in VANET. Unpredictable movement of VANET has caused the network to face the security issues. In this work, efficient method to detect the

Evaluation of mechanical properties of AL7075/Al$_2$O$_3$/B$_4$C based hybrid composite

🛒

Hanumanthe Gowda ✉; S. Harish ✉; G. P. Devaraju ✉

📘 Check for updates

Aluminum Alloy Composites are utilized widely in current years, as it recommends higher mechanical properties than base aluminum alloy. As they have high proportion of strength to density and superior wear protection, it has broad assortment of uses in marine and Automobile. In the present work, a stir casting method is used to fabricate hybrid composites reinforced with Boron carbide with an average mesh size 100μm and Al$_2$O$_3$ of mesh size of 80μm particulates. Optical microscope is used to study the micro structural characterization of the Aluminium hybrid composites. Tensile strength and Hardness of the hybrid composite increased as increasing the particulates of reinforcement.

Topics

Composite materials, Alloys, Materials properties, Mechanical properties, Metal oxides

REFERENCES

1. Amol Mali, S.A Sonawane and Sachin Dombale, *International Journal of Engineering Research and Technology*, 4, 130–133 (2015).

2. P. Talukdar, B. Mallik, S.K. Mukherjee, *Indian Foundry Journal*, 52 (11) 23–34 (2006).

15

Artificial neural network for prediction of mechanical properties of aluminium A356 /Al₂O₃/RHA particulates reinforced hybrid composites 🛒

Hanumanthe Gowda ✉ ; S. Harish ✉ ; G. P. Devaraju ✉

🔖 Check for updates

In this study, the mechanical properties of Aluminium A356 alloy reinforced with particulates Al_2O_3 and RHA particulates were first experimentally examined and then ANN implemented in order to model the mechanical properties including UTS, Percentage elongation and Hardness. The test specimens were machined to ASTM standards and were subjected to artificial ageing and solution heat treatment. The mechanical properties were studied and considerable improvement was observed in double aged with strain /stretching condition. It is also revealed that Artificial Neural Network can be employed for optimizing the process parameters of aluminium alloys.

Topics

Artificial neural networks, Mechanical properties, Metal oxides, Chemical elements, Alloys

REFERENCES

1. Ali Mazahery & Mohsen Ostad Shabani, *Indian Journal of Engineering & Materials Sciences*, 19, 129–134 (2012).

2. G.J. Yuan, J.J. Wu, M.C. Gui, C.G. Li, *Materials Science and*

Winter Collection | Dec

ಡೆಕಾಥಾ಼ನ್ ಮ್ಯೆಸ...

Studies on ruthenium and rhodium complexes containing 6-pyridyl-5,6-dihydrobenzo[4,5]-imidazo[1,2-c]quinazoline and catalytic transfer hydrogenation 🛒

H. G. Bheemanna ✉ ; M. N. Manjunatha; K. S. Mamatha; V. Gayathri

🔖 Check for updates

Reactions of ruthenium(III) chloride and rhodium(III) halides with 6-pyridyl-5,6-dihydrobenzo[4,5]-imidazo[1,2-C]quinazoline in stoichiometric amounts in methanol produced binuclear complexes of the compositions $[RuCl_2(\mu-Cl)(N-N)]_2$ and $[RhX_3(N-N)]_2 \cdot nH_2O$ (n = 0, X = Br or I; n = 1, X = Cl). $[RhI_3(N-N)]_2$ was prepared by stirring a mixture of rhodium trichloride with fifteen fold excess of sodium iodide and the N-heterocycle in methanol. Rhodium halides in 2-methoxyethanol/alcohol reacted with (N-N) in presence of CO to produce complexes of the types $[Rh(CO)_2(N-N)]Cl$ and $[Rh_2Br_2(CO)_2(N-N)]$. The complexes were characterized by elemental analyses, molar conductivity measurements, IR, electronic, ^{1}H- and ^{13}C-NMR spectral studies and by mass spectra. Probable structures have been proposed for the complexes. The complex $[RuCl_2(\mu-Cl)(N-N)]_2$ in DMF was found to reduce nitrocompouds to corresponding amines using formic acid as hydrogen donor.

Topics

Transition metals, Electrolytes, Mass spectrometry, Nuclear magnetic resonance spectroscopy, Organic compounds, Hydrogenation process, Catalysts and Catalysis

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

17
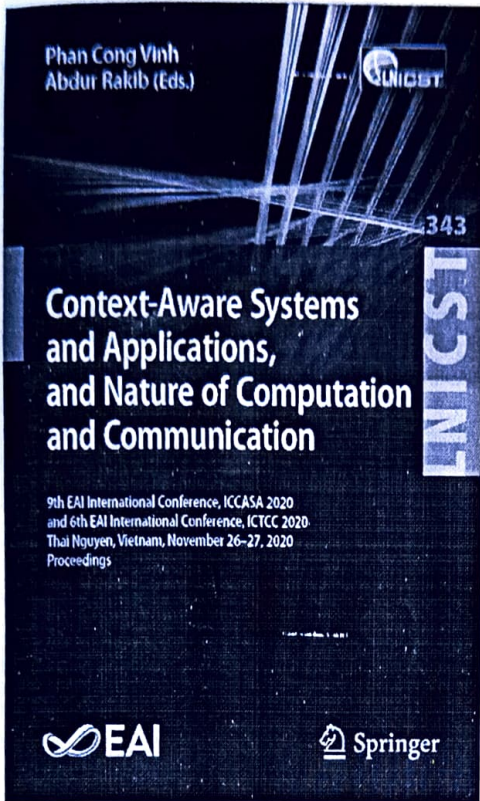
Cite this paper

Shashikiran, B.S., Shaila, K., Venugopal, K.R. (2021). Hybrid Domain Steganography for Embedding DES Encrypted QR Code Using Random Bit Binary Search. In: Vinh, P.C., Rakib, A. (eds) Context-Aware Systems and Applications, and Nature of Computation and Communication. ICCASA ICTCC 2020 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 343. Springer, Cham. https://doi.org/10.1007/978-3-030-67101-3_25

Download citation

.RIS⤓   .ENW⤓   .BIB⤓

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

(18)

19

Hybrid Domain Steganography for Embedding DES Encrypted QR Code Using Random Bit Binary Search

B. S. Shashikiran ✉, K. Shaila & K. R. Venugopal

Cite this paper

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

Phan Cong Vinh
Abdur Rakib (Eds.)

EAI/ICST

343

LNICST

Context-Aware Systems and Applications, and Nature of Computation and Communication

9th EAI International Conference, ICCASA 2020
and 6th EAI International Conference, ICTCC 2020
Thai Nguyen, Vietnam, November 26–27, 2020
Proceedings

21

Improved Packet Delivery for Wireless Sensor Networks Using Local Automate Based Autonomic Network Architecture in a ZigBee Environment

K. N. Sanjay, K. Shaila & K. R. Venugopal

Cite this paper

Sanjay, K.N., Shaila, K., Venugopal, K.R. (2021). Improved Packet Delivery for Wireless Sensor Networks Using Local Automate Based Autonomic Network Architecture in a ZigBee Environment. In: Vinh, P.C., Rakib, A. (eds) Context-Aware Systems and Applications, and Nature of Computation and Communication. ICCASA ICTCC 2020 2020. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 343. Springer, Cham. https://doi.org/10.1007/978-3-030-67101-3_24
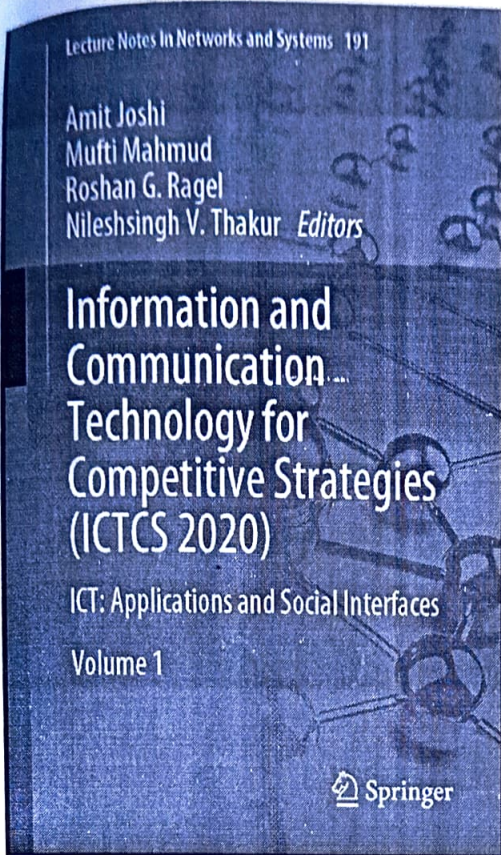
Download citation

.RIS ⭳   .ENW ⭳   .BIB ⭳

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

(23)

Cite this paper

Download citation

.RIS ⤓   .ENW ⤓   .BIB ⤓

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

(24)

25

Conference paper

FTRAT: Fault-Tolerant Routing Based on Aggregation Tree to Improve the QoS in Wireless Sensor Networks

P. Manasa, K. Shaila & K. R. Venugopal

Conference paper · First Online: 27 July 2021

913 Accesses

Cite this paper

Download citation

RIS ⬇   ENW ⬇   BIB ⬇

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

26

Energy Concerned Clustering Mechanism to Ensure Reliable Data Transmission in Wireless Sensor Network

Original Research · Published: 08 May 2021

Volume 2, article number 266, (2021)   Cite this article

SN Computer Science

Aims and scope

Submit manuscript

P. Manasa ✉, K. Shaila & K. R. Venugopal

Cite this article

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 07¿

27

ORIGINAL RESEARCH

SN

Minimal Block Knight's Tour and Edge with LSB Pixel Replacement Based Encrypted Image Steganography

B. S. Shashikiran[1] · K. Shaila[1] · K. R. Venugopal[2]

Abstract

The data security of an information is predominant in the digital world and gaining lot of importance. Cryptography and steganography are widely used in providing security to an information. In the proposed algorithm, the image encryption and steganography are performed using Knight's move in the game of chess called Knight's Tour Algorithm. Minimum block or square required for a knight's tour to reach all the squares is 5×5 block. The 5×5 blocks' pattern generated is used for image encryption. The encrypted image is then embedded into another image and block shuffling is performed to obtain a crypto-stego image. Proposed algorithm is robust and provides high data security with a good PSNR and SSIM.

Keywords Cryptography · Crypto-Stego · Knight's tour · PSNR · SSIM · Steganography

Introduction

The incessant development and popularization of digital technology has changed the processing of secret images. The entire world is moving towards smart era driven by digital technology and all information is accessible at finger tips. Every second, more than a million information is exchanged across the internet in different formats, such as text, audio, image or video. Information in the image is sparkling and visually attractive than text information. Sensitive, personal information or defense information related to a country or medical information or documents related to an organization need to be protected from trespassers when it is distributed and shared over internet.

The recursive root cause analysis is carried out on trapping and attack of information by trespassers and data protective techniques are improved with new security algorithms. There are many effective techniques that are available to protect the data from unauthorized access like cryptography and steganography. Image files are extensively used nowadays due to its high capacity and easy accessibility and protecting these image files are the top priority. Many cryptography, steganography and crypto-steganography algorithms are developed.

Chess is a game of adaptive strategy and intelligence. Each move of pieces in the chess ends with some pattern by the end of game. The pattern of each pieces has encouraged many combinatorial puzzles. The most interesting and popular patterns are obtained from Knight's Tour and Eight Queen puzzle.

Knight's tour [1–3] is an arrangement of moves of a knight on a chess board such that knight visits each square just once. If the knight tops on a same square where it started, then it is called closed tour, otherwise it is open. The knight's tour problem has become the mathematical puzzle and motivated open thoughts for many image processing and pattern-based research work. The moves of knight in chess game are very tactical to end the game with possible win. Knight's tour is not restricted only for a chess board size 8×8, but it can be extended for any size $M \times N$. To obtain a solution for Knight's tour, minimum size of the board should be 5×5. Figure 1a shows one of the patterns generated by knight's tour on 8×8 board and Fig. 1b shows one of the patterns generated by knight's tour on 5×5 board.

✉ B. S. Shashikiran
shashikiran.bisileri@gmail.com

[1] Department of Electronics and Communication Engineering, Vivekananda Institute of Technology, Bengaluru, Karnataka, India

[2] Bangalore University, Bengaluru, Karnataka, India

28

An Energy Efficient Threat Free Protocol (ETP) for Data Transmission in Wireless Sensor Networks

Publisher IEEE   Cite This   PDF

All Authors

R   <   C   🔔

Cite This

                                      ✕

Plain Text	BibTeX	RIS	Refworks

✅ Citation & Abstract   📋 Copy

R S , S K and V K R , "An Energy Efficient Threat Free Protocol (ETP) for Data Transmission in Wireless Sensor Networks," *2019 IEEE 16th India Council International Conference (INDICON)*, Rajkot, India, 2019, pp 1-4, doi 10 1109/INDICON47234 2019 9030284

Abstract Data security and energy efficiency is the most exacting issue in Wireless Sensor Networks (WSNs) In this paper, we propose a protocol for secure and energy efficient data transmission between the source and the destination This protocol involves Cluster Head Selection (CHS) phase and Secure Data Transmission (SDT) phase First, CHS phase elects an efficient aggregator node based on localization, then the sensed data is forwarded to the Cluster Head (CH) and CH aggregates data In turn, SDT phase focused on providing security to aggregated data Thus, the proposed protocol, ETP utilizes the node's resource parameter uniformly, which in turn improves Network Lifetime and maximizes Throughput Rate The ETP is simulated using the NS2 simulator and compared with Fuzzy C-Means centroid algorithm and a secure aggregation protocol implemented using SAR(Secure Aware Ad hoc Routing Routing) The time complexity of ETP protocol is $O(m2\ n)$

URL https //ieeexplore ieee org/stamp/stamp jsp?tp=&arnumber=9030284&isnumber=9028850

LA-ANA based Architecture for Bluetooth Environment

Sanjay K N
Research Scholar, VTU RC,
Department of Electronics and
Communication Engineering
Vivekananda Institute of Technology,
Bengaluru, Karnataka, India
e-mail:sanjaykenkare@gmail.com

Shaila K
Professor,
Department of Electronics and
Communication Engineering
Vivekananda Institute of Technology,
Bengaluru, Karnattaka, India

Venugopal K R
Vice Chancellor
Bangalore University
Bengaluru
Karnataka, India

Abstract— Wireless Personal Area Network is widely used in day to day life. It might be a static or dynamic environment. As the density of the nodes increases it becomes difficult to handle the situation. The need of multiple sensor node technology in a desired environment without congestion is required. The use of autonomic network provides one such solution. The autonomicity combines the local automate and address agnostic features that controls the congestion resulting in improved throughput, fault tolerance and also with unicast and multicast packets delivery. The algorithm LA based ANA in a Bluetooth based dynamic environment provide 20% increase in throughput compared with LACAS based Wireless Sensor Network. The LA based ANA leads with 10% lesser fault tolerance levels and extended unicast and multi-cast packet delivery.

Keywords— *Autonomic Network Architecture (ANA), Bluetooth, Dynamic Environment, LACAS, Piconet, Stochastic Model, Wireless Sensor Networks.*

I. INTRODUCTION

An abundant application can be found due to advances in micro-sensing technology that led to a considerable volume in the area of Wireless Sensor Networks [1]. One of the short range transmission is Bluetooth [2] technology that uses Time-Division Multiple Access (TDMA) and Frequency Hopping Spread Spectrum (FHSS) for its transmission between nodes. While IEEE 802.11 doesn't make a decent choice as it contains idle listening and collision avoidance making inappropriate for WSNs. As discussed in [3] there exists various advantages and limitations with Bluetooth based-WSNs. Separate channels are used to avoid interference while using Bluetooth within the available radio range. It competes with shared channel in a greater extent [4].

The WSNs applications are completely diverse and are widespread leading to protocols that are always application-driven multilevel specification that involves large amount of sensor activity within a geographical area. This can also involve Heterogeneous network and communication through a sink node. The transmission of Bluetooth is limited with few tens of meters. Hence, there is a requirement of multi-hop routing in designing the dynamic environment with a large spread nodes [5].

Numerous application can be fulfilled using above said networks and few of them are: monitoring the habitats, Health Monitoring, Monitoring Weather, civil construction and others [6]. These applications require data transfers at a bit faster rate and occurs with an unpredictable bursts. Thus, Bluetooth based WSN would be the feasible method for such an environment [7]. For the effective scatternet formation with a multi-hop network in a bluetooth environment is discussed. It acts as a base for involving an Autonomic Network

Architecture in a Bluetooth environment [8]. Thus, to provide various communication opportunities and services for private use is an incredible usage of the wireless personal devices in a heterogeneous networks [9].

In a Bluetooth environment there exist two styles of configuring a network: Piconet forms the basic network unit with one MASTER and several SLAVES and is shown in Figure 1(a) and Scatternet combines an additional piconet and is shown in Figure 1(b). Scatternet is always a multiple piconet configuration and is addressed as PIMP (Participant in Multiple Piconets) that involves bridge nodes with an exceedingly time division manner [9].
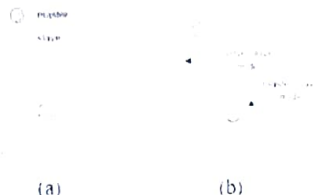

Fig. 1. Representations of (a) Master Node and (b) Master/Slave Node and Slave/Slave Node in Bluetooth Environment.

The master driven time division duplex scheme is employed in Bluetooth with a specific time slots. These time slots are distributed alternatively between Master and Slave in each and every piconet present in a dynamic environment. With autonomicity involvement even and odd slots of time are dedicated with the Master and Slave transmissions [1] respectively. In addition, there exists an inter-piconet scheduler while allocating the piconet scheduling process involving multiple piconets [2]. The ANA architecture consisting of two layers of co-ordination namely, lower task execution layer called the host controller and therefore the application and better task allocation layer with local automate is as shown in Figure 2. The host controller shares between the neighbouring nodes and native automate that differs from existing layered architectures with multi-hop coordination that adopts a reactive method [13].
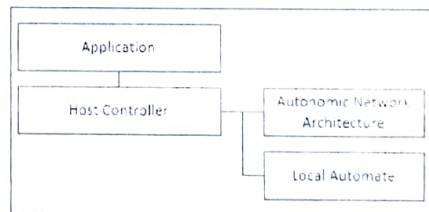

Fig. 2. ANA: Autonomic Network Architecture

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

LA-ANA Based Data Transmission in UWB Tx-Rx

Sanjay K N
Research Scholar, VTU-RC,
Department of Electronics and
Communication Engineering
Vivekananda Institute of Technology.
Bengaluru, Karnataka, India
e-mail:sanjaykenkare@gmail.com

Shaila K
Professor
Department of Electronics and
Communication Engineering
Vivekananda Institute of Technology,
Bengaluru, Karnattaka, India

Venugopal K R
Vice Chancellor
Bangalore University
Bengaluru
Karnataka, India

Abstract— Energy efficiency is the major concern in designing Ultra-Wideband (UWB) based WSNs. In designing the heterogeneous WSNs in a dynamic environment data transmission would be difficult due to the presence of larger density nodes. This problem can be resolved using an autonomic based learning in a MAC Layer of UWB TxRx. In this paper, the process of Local Automate based Autonomic Network Architecture (LA-ANA) is deployed at the MAC Layer of the WSNs. The method learns repeatedly from the previous occurrences and avoids the congestion. The simulation results show an increase in throughput and decrease in energy consumption.

Keywords—Autonomic Network Architecture, Dynamic Environment, LACAS, Ultra Wide-band, Wireless Sensor Networks.

I. INTRODUCTION

Analysis and design of low cost integrated sensing, communicating and computing nodes requires an innovative technology in wireless networking, array processing and microelectronics that are efficient to perform various required collaborative space-time processing tasks. Wireless Sensor Networks finds a significant consideration in the areas of embedded systems, networking, multi-agent systems and pervasive computing [1]. Real-time scenarios like environment monitoring, disaster relief involves the distributive sensing task which is achieved by combining large number of static sensors.

Lots of research and development in wireless extensions are predominantly characterizing the unique functioning of WSNs [2]. The most effective use of every surface of communication protocol is essential and mandatory that demands the requirement using cross-layer design model and combined protocols like Local Automate and ANA. This leads to many newly distributed algorithms and protocols like signal processing, fault tolerant routing protocols that are self-organizing, energy efficient MAC and self-healing sensor network.

In the OSI model, medium access control (MAC) [3] layer is used as glue to thread all the said solutions. The core for proper functioning of any communication system, can be achieved using automata design. The main function of MAC is to coordinate access and transmit it over a medium that are common to several nodes. Within the specific communication range there are chances of interference leading to packet loss and need to be retransmitted. WSNs ranges from small size industry to large scale industrial applications that are scattered because of associated and scheduling delay at MAC layer to the link layer [4-5].

A. Motivation

The assurance of long existance nodes in WSNs with specific energy and complexity of design need to be considered while designing the MAC in active and sleep modes Therefore, in designing the MAC protocols reliability, longevity, fairness, scalability and latency are the primary concern [6].

Reliability in data transmission can be achieved by considering the congestion into account. Due to congestion energy consumption increases resulting in loss of packets and create unfair and non-reliable flow of packets with the help of intermediate nodes reducing throughput[7]. These issues have to be addressed while designing WSNs for any applications.

B. Contribution

Learning based Autonomic Network Architecture (ANA) is proposed with reliable communication which integrates UWB sensor network with complex dynamic environments at a larger rate between the nodes. Congestion and throughput levels have to be optimized in dynamic environment containing large density nodes within smaller space. Thus, learning based ANA in MAC layer would provide a solution in managing large sensor activity providing an energy efficient data transmission. LA based ANA introduces the function of MASTER/SLAVE to respective nodes even if the nodes are not available in the communication range.

C. Organisation

Section II provides related work. Section III provides implementation of the work. Implementation of the algorithm is discussed in Section IV with the help of flowchart. Section V provides simulation environment and performance metrics used in evaluating the results.

Journal for Manufacturing Engineers and Technocrats

The effects of silicon oxide as an additive with a cotton seed oil biodiesel blend in a CI engine

T. Deepak Kumar[1*], Manjunatha[2], D. K. Ramesha[3]

[1,3]Department of Mechanical Engg., University Visvesvaraya College of Engg., Bangalore University, Bangalore, India

[2]Department of Mechanical Engg., Vivekananda Institute of Technology, Visvesvaraya Technological University, Belgaum, India

ABSTRACT

Experimental investigation was carried out to study the combustion, engine performance and emission characteristics of a single cylinder, naturally aspirated, air cooled, constant speed compression ignition engine, fuelled with five modified fuel blends, Diesel, B20 (Diesel–cotton seed oil biodiesel) and Diesel– cotton seed oil biodiesel –with silicon oxide as a Nano additive with three different concentration 50ppm, 75ppm, 100ppm, and the results are compared with those of neat diesel. The Nano additive was mixed in the fuel blend along with a suitable surfactant by means of an ultrasonicator, to achieve stable suspension. The properties of B20, B20 + silicon oxide fuel blend are changed due to the mixing of cotton seed biodiesel and the incorporation of the with silicon oxide Nano additives. Some of the measured properties are compared with those of neat diesel, and presented. The cylinder pressure during the combustion and the heat release rate, are higher in the B20 + with silicon oxide 100-ppm fuel blend, compared to neat diesel. Further, the exhaust gas temperature is reduced in the case of the B20 with silicon oxide 100ppm of fuel blend, which shows that higher temperature difference prevailing during the expansion stroke could be the major reason for the higher brake thermal efficiency in the case of B20 with silicon oxide 100ppm of fuel blend. The presence of oxygen in the Cotton seed biodiesel and the better mixing capabilities of the nanoparticles, reduce the CO and UBHC appreciably, though there is a small reduce in NO, at full load condition.

1. Introduction

The number of vehicles currently on the road is rapidly increasing. This scenario will create a lot more challenges for the oil supply industries to meet the demand on another side as well as increasing the depletion of fossil fuels day by day. The global warming caused by increased emissions from these vehicles leads to an increase in carbon footprint. To order to meet the demands of vehicle users, fossil fuels are increasingly declining and therefore need a change to alternative energy sources [1]. In addition, the harmful emissions that deteriorate

the atmosphere are created by burning the petroleum-based fuels in a combustion engine. Therefore, due to concerns such as the scarcity of fossil fuels and the rising cost of fossil fuels, the need for the production of alternative fuels has arisen [2]. Bio fuels have certain specific characteristics features such as lower viscosity, better atomization, density, evaporation and net calorific value making them equivalent to diesel [3]. bio fuels are alternative fuels that researchers pay more attention to because of their environmentally friendly nature and their ample availability on Earth [4]. During the implementation of these bio fuels in diesel engines have significant benefits were noted such as major reduction in the engine exhaust pollutants like UBHC, Smoke emissions and CO. Majority of the scientist and researches

*Corresponding author,
E-mail: deepu.doit@gmail.com

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

33

Maximizing the Network Lifetime Using Supervisory Node in Wireless Sensor Networks

Authors:

Manasa Puttaswamy

K Shaila
Vivekananda Institute of Technology, Ba

Venugopal K R
University Visvesvaraya College of Engi

2018-2019

Elliptic Curve Crypto Processor on FPGA using Montgomery Multiplication with Vedic and Encoded Multiplier over GF(2^m) for Nodes in Wireless Sensor Networks

Leelavathi G, Shaila K,
Electronics and Communication Engineering
Research Scholar, VTU-Research Centre,
Vivekananda Institute of Technology,
Bengaluru, India
nisargamodini@gmail.com

Venugopal K R IEEE Fellow
Vice Chancellor
Bangalore University
Bengaluru, India

Abstract—Resource constraint Wireless Sensor Networks requires the fast multipliers that are crucial for data processing. Scalar or Point multiplication, the most important operation of Elliptic Curve Cryptography (ECC) is carried out with Montgomery Multiplication which is implemented using Vedic and Encoded Multipliers. Both the multipliers are designed for basic finite field multiplication operations at lower levels of design that increases the overall performance of the cryptosystem in terms of speed, area, operating frequency and consumption of power. The encoded architecture has low gate count and it decreases the number of partial products in its multiplier architecture. In point doubling and point addition the multiplications are done by Encoded Multiplier and squaring using Urdhva Triyambhagyam Vedic Multiplier. For experimental purpose the crypto system is first implemented with GF (2^8) and expanded to GF (2^{194}). The synthesis result gives that delay of 3.510 nanoseconds for 8 bit point multiplication and 2608 nanoseconds for 194 bit. Upon device utilization it is 432 LUTs for 8 bit and 7455 for 194 bit architecture. The static power utilization for 194 bit is 178.43 mW. The processor with encryption /decryption of 194 bit key and data is implemented selecting low cost optimized Xilinx Spartan 3E XC3S500/ FG320 and Speed Grade of -5 with the IDE tool Xilinx ISE 9.2i. Hardware implementation is performed for GF (2^8) on Spartan 3E with input and output pins availability.

Keywords — *FPGA, Elliptic Curve Cryptography, Encoded Multiplier, Montgomery Multiplication, Public key Cryptography, Urdhva Triyambhagyam, Wireless Sensor Networks.*

I. INTRODUCTION

The major issue in Wireless Sensor Networks (WSNs) with sensor nodes is their controlled resource with respect to cryptographic operations. The sensor capacity in handling the additional computations depends on the cryptographic processes since, it is limited by the usage of power, area and time. Hence, Public Key Cryptography is termed to be most feasible in WSNs by using Elliptic Curve Cryptography (ECC). Compared to RSA cryptosystems Elliptic Curve Cryptography functions as the suitable cryptographic tool due to its smaller key size and security [1][2]. The ECC Cryptosystem is implemented on FPGA for sensor nodes that are used in Wireless Sensor Networks (WSNs) in which nodes are FPGA based [3]. Conventional microcontroller's sensor

nodes do not provide adequate computation power to process public key cryptographic operations [1] [2]. The potentials of FPGAs in sensor node architectures and their applications are explored in [3] [4] [5] with suitable of FPGAs in Wireless Sensor Nodes.

Motivation: Design of multipliers with different multiplication technique to optimize the area and computational time in FPGA design is a challenging task. These multipliers are the basic building blocks of arithmetic logic to enhance the speed of operation. Implementations for hardware applications are habitually designed to achieve an optimal area performance ratio [3]. In order to achieve better hardware efficiency Xilinx is preferred in the design of hardware architecture [6]. More specifically, the challenge is to select an FPGA device that is available at minimal cost, but can afford a maximum number of cryptographic operations.

Problem Definition: A specific multiplication presence in encryption algorithm is not capable to provide all the preferred performance for nodes in WSNs, so Public key cryptography is adopted. Public key cryptography is computationally expensive for WSNs if not accelerated by cryptographic hardware. Scalar Multiplication which is the key operation requires major time, power and chip area. Hence, the design of multiplier and its functional behavior becomes the basis of ECC design. Compared to microprocessor based platforms FPGA hardware implementations can be designed optimally with respect to time and area complexity for most applications. This work utilizes encoded and Vedic multipliers in underlying finite field arithmetic's to enhance the process of encryption thus increasing the network lifetime.

Contribution: The proposed work implements Elliptic Curve Crypto Processor on FPGA with Montgomery Multiplication using Vedic and Encoded Multipliers over GF (2^m) for Nodes in Wireless Sensor Networks for equal data and key size of 8 and 194 bits. Hardware implementation is performed for GF (2^8) on Spartan 3E with limitation of input and output pins.

Organization: Section II, discusses the related work to Public Key Cryptography, ECC security techniques and

A Light Weight Implementation of ECC Cryptosystem on FPGA for nodes in Wireless Sensor Networks

Leelavathi G[1], shaila K[1], Venugopal K R[2]

[1] Vivekananda Institute of Technology, Bengaluru, Karnataka, India

[2] University College of Engineering, Bengaluru, Karnataka, India

ABSTRACT

The ECC Cryptosystem is implemented on FPGA for sensor nodes that are used in Wireless Sensor Networks in which nodes are FPGA based. Scalar or Point multiplication, the most important operation of ECC is carried out with double and add algorithm which is implemented using Karatsuba Multiplier. The Karatsuba Multiplier designed for basic finite field multiplication operations at lower levels of design increased the overall performance of the cryptosystem in terms of area, speed, operating frequency and power consumption. The processor is optimized for scalar multiplications with Lopez Dahab and Mixed coordinate systems. This work concentrates on lightweight implementation of ECC that is suitable for Wireless Sensor Nodes. The previous implementations mainly concentrates only on Point multiplication where as in our work we have implemented complete ECC cryptosystem with 40% less device utilization on FPGA Artix-7xc7a100t-2csg324 and the speed achieved is 432MHz.

Keywords: Elliptic curve cryptography, FPGA, Karatsuba Multiplier, Point Multiplication, Wireless Sensor Networks

I. INTRODUCTION

The special needs of Wireless Sensor Networks (WSNs) such as security issues, communication protocols and hardware platforms, require an intense research activity. Different applications employed on the same WSNs environment will have diverse security requirements, inferring the necessity of using dissimilar security algorithms. Encryption is a sensible countermeasure to protect data, although it increases new processing load to the nodes. Conventional microcontrollers found sensor nodes do not provide adequate computation power to process public key cryptographic operations [1][2]. The practice and potentials of FPGAs in sensor node architectures and their applications are explored in [2].

Neal Koblitz and Victor Miller proposed Elliptic Curve Cryptography (ECC) in the year 1985. At present, ECC is the most efficient and preferred PKC system with shorter keys. The security is to concentrate the difficulty of solving Elliptic Curve Discrete Logarithmic Problem (ECDLP)[3]. ECC is attaining popularity since it provides similar security with significantly smaller key lengths. This feature makes it suitable for resource constrained devices like wireless sensor nodes.

255 |

Implementation of Public Key Crypto Processor with Probabilistic Encryption on FPGA for Nodes in Wireless Sensor Networks

G. Leelavathi   K. Shaila   K. R. Venugopal   All Authors

Alerts

Abstract

Document Sections

I. Introduction

II. Related Work

III. Model and Computational Details

IV. Results and Discussions

V. Conclusions

Authors

Figures

References

Citations

Abstract: Cryptographic algorithms are fundamental to the secure communications over Wireless Sensor Networks. This paper presents complete public key cryptosystem with mathematica... View more

▶ Metadata

Abstract:

Cryptographic algorithms are fundamental to the secure communications over Wireless Sensor Networks. This paper presents complete public key cryptosystem with mathematical model essential for designing a cryptographic algorithm that integrates probabilistic encryption. The encryption process is presented as a secured pseudo random number generator that supports key generation process. The main goal of our work is to design Public Key Crypto Processor with modification of Public Key Algorithms RSA and ECC for Wireless Sensor Node architecture considering speed, time and area as the design parameters. The Crypto Processor is simulated on different FPGA devices with key lengths 32 bits. The comparison of the performance is done with respect to area and speed. The proposed Public Key Crypto algorithm is modeled using Verilog and synthesized on Spartan 3 and 6, Virtex 7, Kintex 7 and Artix 7. Combinatorial path delay is not determined in any of the module implemented. The design satisfies the requirements of resource constrained Wireless Sensor Network's devices with 0.05% resourceless device utilization with speed of 906.6MHz.

Published in: 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)

Cite This   ✕

Plain Text   BibTeX   RIS   EndNote

☐ Citation & Abstract

G. Leelavathi, K. Shaila and K. R. Venugopal, "Implementation of Public Key Crypto Processor with Probabilistic Encryption on FPGA for Nodes in Wireless Sensor Networks," 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 2018, pp. 1-6, doi: 10.1109/ICCCNT.2018.9493894.

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

Nageswara S.V. Rao · Richard R. Brooks
Chase Q. Wu *Editors*

Proceedings of International Symposium on Sensor Networks, Systems and Security

Advances in Computing and Networking with Applications

In honor of Dr. S.S. Iyengar's 70th Birthday

🍃 Springer

About this paper

Cite this paper

Download citation

.RIS⬇   .ENW⬇   .BIB⬇

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

38

← Previous   Page   1   of 2   Next →

Back to top ↑

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

39

TASB-AC: Term Annotated Sliding-Window-Based Boosting Associative Classifier for DNA Repair Gene Categorization

A. Vidya, Santosh Pattar, M. S. Roopa, K. R. Venugopal & L. M. Patnaik

Conference paper | First Online: 24 May 2018

400 Accesses

Cite this paper

Vidya, A., Pattar, S., Roopa, M.S., Venugopal, K.R., Patnaik, L.M. (2018). TASB-AC: Term Annotated Sliding-Window-Based Boosting Associative Classifier for DNA Repair Gene Categorization. In: Rao, N., Brooks, R., Wu, C. (eds) Proceedings of International Symposium on Sensor Networks, Systems and Security. ISSNSS 2017. Springer, Cham. https://doi.org/10.1007/978-3-319-75683-7_19

Download citation

RIS⬇ ENW⬇ .BIB⬇

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

27/12/2023

(42)

Modeling and formal verification of SMT rail interlocking system using PyNuSMV

Cite This

PDF

All Authors

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

41

Modeling and Formal Verification of SMT Rail Interlocking System Using PyNuSMV

Rakesh L

Department of Computer Science and Engineering
Jain Institute of Technology
Davangere – 577 003, Karnataka, India
dr.rakesh168@gmail.com

Lokanna Kadakolmath

Department of Computer Science and Engineering
Vivekananda Institute of Technology
Bengaluru – 560 074, Karnataka, India
lokanna.vk@gmail.com

Abstract— The success of urban smart mass transportation (SMT) system lie down in their ability to give frequent, fast, safe, and comfortable journeys in the urban conglomeration. In the railway signaling province, a railway interlocking is a computerized system that manages the railway signaling entities to permit a risk-free operation of the train traffic. Being a safety-critical system, the development of a railway interlocking systems follow several standards, such as CENELEC EN50126, EN50128, and IEC62279, which suggest the use of finite state machine inside the system modeling phase, and formal methods in verification, and validation phases. Often, they do verification and validation of railway interlocking tables physically and is thus fault-prone and expensive. So, within our research work, we used nuXmv as a modeling tool, and PyNuSMV as a verification tool, for verifying safety and liveness properties. As well, the reliability of the developed model has been validated by means of counterexamples and custom CTL model checking algorithm. We can also apply our developed model on real urban railway interlocking systems.

Keywords— Binary decision diagram, control table, finite state machines, formal specification, formal verification, magnetic levitation, model checking, railway interlocking, safety-critical systems, smart mass transportation.

I. INTRODUCTION

Railway transportation system is deliberated as a keystone in nation transport organization, especially in metropolitan areas. Each year, greater than 600 million commuters use railway transport and greater than 7 million loads of cargo transported by rail. This prominent railway transport role in nation's budget is the threat of repetitive rail disastrous collisions in the past few centuries. In one of these collisions, the reason was improper physical verification, and validation of operational specifications (called control tables, or interlocking tables), for railway interlockings, and missing of safety requirements document [2] [12].

As railway systems evolved from the mid-19th century, the signaling systems started developing the initial primitive systems. The two main goals of railway signaling were:

1) Provision of safety from collisions, and derailments.

2) Give as greatest line capacity as possible, for running many trains on the same line within the safety constraints.

So, a general architecture of signaling model includes the subsequent documents:

1) The railway yard, which describes the location of signals, and points in a segment of the railway system, and the approved routes between the signals.

2) Functional requirements for the signaling of the railway yard this is nowadays given in the mode of control table and depicts how the overall signaling principles are realized in this railway yard.

As a safety-critical system, the development of railway interlocking system must meet the fail-safe requirements. So, the use of formal methods in railway interlocking system enhance the quality and boost the confidence level by automatically verifying the fail-safe requirements.

K. Winter and N. J. Robinson [14] have modeled the interlocking of large railway using ASM formal notation. They converted ASM model into NuSMV model and specified safety properties using CTL formulas.

R. Abo and L. Voisin [1] have checked large interlocking table using B language and the OVADO tool. But the use of B language is not appropriate to state the interlocking logical rules because these needs the system states to be retrieved globally by various logical rules, while abstract machines compress their state variables, which are reachable only through procedures.

N. A. Zafar [15] has modeled moving block railway interlocking system, using an un-directed topology that is dynamic topology in which direction of any track can be switched as needed, and formal specifications are described and validated using a VDM-SL toolbox. This work was one of the benchmarks for developing the abstract model.

Xi. Wang, S. Liu, and et al. [13] have modeled the communication-based train control (CBTC) interlocking system. In this method, they used a modern modeling method to build system model, state main safety properties, and perform formal verification using SCADE tool. But using SCADE we lose the state machines and any information on the underlying architecture of the model.

The National Institute of Engineering

(An Autonomous Institute under VTU, Belagavi)
Manandavadi Road, Mysuru- 570008

TEQP

Department of Electronics and Communication Engineering

National Conference 17ᵗʰ and 18ᵗʰ May 2018

Certificate

This is to certify that Prof./Dr./Mr./Mrs./Miss..... LOKANNA KADAKOLMATH

of .... V.K.I.T, Bengaluru

has presented a paper/participated in National Conference on Communication, Signal Processing, IoT,

Networking and Embedded Application (NCCOSINE-2018) on 17ᵗʰ and 18ᵗʰ May 2018, conducted by

Department of Electronics and Communication Engineering, National Institute of Engineering, Mysuru

Single Repair Pattern Tree Algorithm for Single Failure in Erasure-Coded Distributed Storage Systems.

Dr. Rohini Nagapadma
Prof. & Head ECE.

Dr. Nagaraju C
Coordinator

Dr. G Ravi
Principal

27/12/2023
Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

Single Repair Pattern Tree Algorithm for Single Failure in Erasure-Coded Distributed Storage Systems

Lokanna Kadakolmath, Pramod N, Lakshitha K, Harish A, Lokesh Kumar S

lokanna.vk@gmail.com,writesomething007@gmail.com,lakshithamk@gmail.com,
anupojharish@gmail.com,iamlokhi@gmail.com

Department of Computer Science and Engineering

Vivekananda Institute of Technology, Bangalore-74, Karnataka, India

Abstract - **In distributed systems we use erasure codes for data dependability. And we use of huge amount of data for repairing a single failure which would take more time on replacing a single node. To overcome researchers came out combining network coding for regenerating codes. Here they considered only about storage whereas the code construction was quite difficult. Hence this paper combines the network coding with network structure to generate a repair tree model to simplify the above repair problem. By decomposing the repair computing among the tree nodes will reduce the tension of computing. The performance and results of repair tree shows that it is three times faster in computing when compared to previous an double times the repair throughput even after having the data restrictions. And finally we present the extending idea of repair tree for repair multiple failures.**

Keywords --Distributed storage systems, Erasure codes, Repair tree, Decomposed repair computing, Single failure.

INTRODUCTION

Distributed storage system that manages large scale datasets and stores files as fixed-size blocks, which form the basic read/write units. It is usually specifically used to refer to either a distributed database where users store information on a number of nodes, or a computer network in which users store information on a number of peer network nodes.

In coding theory, an erasure code is a forward error correction (FEC) code under the assumption of bit erasures (rather than bit errors), which transforms a message of k symbols into a longer message (code word) with n symbols such that the original message can be recovered from a subset of the n symbols. Erasure codes are an efficient means of storing data across a network in comparison to data replication, as they tend to reduce the amount of

data stored in the network and offer increased resilience in the presence of node failures. The codes perform poorly though, when repair of a failed node is called for, as they typically require the entire file to be downloaded to repair a failed node[3]. A new class of erasure codes, termed as regenerating codes were recently introduced, that do much better in this respect.
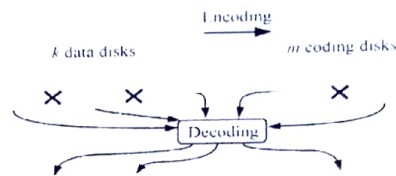

Fig.1 An erasure-coded storage system encodes k data disks onto m coding disks. When up to m disks fail, their contents are decoded by the erasure code[2]

A single point of failure (SPOF) is a part of a system that, if it fails, will stop the entire system from working. SPOFs are undesirable in any system with a goal of high availability or reliability, be it a business practice, software application, or other industrial system.
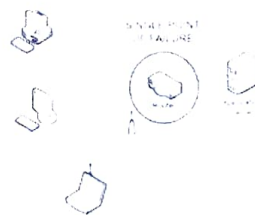

Fig 2 In this diagram the router is a single point of failure for the communication network between computers

Systems can be made robust by adding redundancy in all potential SPOFs. For instance, the owner of a

Dayananda Sagar Institutions

DAYANANDA SAGAR ACADEMY OF TECHNOLOGY & MANAGEMENT

Opp, Art of living, Udayapura, Kanakapura main road, Bangalore-560 082
(5 Branches Accredited by NBA- CSE, ISE ,ECE, EEE, MECH- validity:26-07-2018 to 30-06-2021)

NATIONAL CONFERENCE ON
CONVERGENCE OF SCIENCE, TECHNOLOGY AND MANAGEMENT
(NCCSTM-2019)

On Friday 10th May 2019

Certificate

This is to certify that Mr./Ms./Dr. **LOKANNA KADAKOLMATH** of

DEPT. OF CSE, VIVEKANANDA INSTITUTE OF TECHNOLOGY presented paper

Titled " **FORMAL VERIFICATION FOR URBAN RAILWAY INTERLOCKING SYSTEM** "

in the "National Conference on Convergence of Science, Technology and Management NCCSTM-2019"

held on 10th May 2019 at Dayananda Sagar Academy of Technology & Management, Bengaluru-82.

Dr..Sumithra Devi. K A,
Organizing Convener, Dean Academics.
Prof. & Head.
Dept of Information Science& Engineering

27/12/2023
Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

Dr. B.R Lakshmikantha
Organizing Chair & Principal

Formal Verification for Urban Railway Interlocking System

Lokanna Kadakolmath
Department of Computer Science and Engineering
Vivekananda Institute of Technology
Bengaluru – 560 074, Karnataka, India
lokanna.vk@gmail.com

Harshini V
Department of Computer Science and Engineering
Vivekananda Institute of Technology
Bengaluru – 560 074, Karnataka, India
harshini.v1998@gmail.com

Keerthana Reddy K
Department of Computer Science and Engineering
Vivekananda Institute of Technology
Bengaluru – 560 074, Karnataka, India
keerthanalahari108@gmail.com

Manasa M
Department of Computer Science and Engineering
Vivekananda Institute of Technology
Bengaluru – 560 074, Karnataka, India
manasamraj01@gmail.com

Abstract— Railways form a major part of the transportation nationally. It is mainly used as a means of transportation and to transport goods. To provide an efficient and a safe way of transportation, it's necessary to provide an efficient interlocking system. Manual methods of interlocking are fault prone due to which formal methods of verification and validation in computerized systems are used. General purpose programming languages show a lot of disadvantages for developing an urban railway interlocking system because of which the formal methods can be used to develop a better and a superior urban railway interlocking system. The success of urban smart transportation systems lie down in their ability. The railway signaling province that is railway interlocking is computerized system which ensures the entities for a risk free operation in the train traffic. It follows several standards which use the finite state machine in the system modelling phase, formal methods and validation process. To reduce the state space explosion problem we use CBMC as a bounded model checker and SAT solver for verifying safety ,properties and the reliability of the model have been validated with the help of counter examples.

Keywords— rail transit, deep learning, formal verification, formal specification, safety critical systems, smart mass transportation, interlocking system.

I. INTRODUCTION

One of the most important and keystone means of transportation is the railway system, transporting around 7 million people every year and 600 tons of goods. It is important to provide an efficient signaling and interlocking system for such a huge railway system. Some of the main goals of the interlocking system are:

1) Provide safety from any sort of collision and provide a critically safe environment for transportation

2) Provide the longest possible track clearance for running train so that frequent stops can be avoided.

To guarantee this safety, we use a formal method of functional requirement for the railway yard. One of the most important factors in the development of an urban railway interlocking systems that are critically safe is the formal and automated verification of code. Some of the major challenges that are seen in this method are that it is difficult to specify global constraints and it is a very big task to assume a previously taken global constraint and conduct verification on it. These disadvantages can be removed by using Event-B along with session types.

With increase RT (Rail Transit) safety becomes the most important factor. A small accident can be fatal leading to heavy losses and to prevent this there are existing systems that use fuzzy fault free technique and a shallow neural network. These systems have more error rate and it is difficult to get satisfactory results. To avoid this we use deep learning for the safety prediction of RT, the concept of deep belief network (DBN) is used and will produce satisfactory results

K. Winter and N. J. Robinson [14] have modeled the interlocking of large railway using ASM formal notation. They converted ASM model into NuSMV model and specified safety properties using CTL formulas.

R. Abo and L. Voisin [1] have checked large interlocking table using B language and the OVADO tool. But the use of B language is not appropriate to state the interlocking logical rules because these needs the system states to be retrieved globally by various logical rules, while abstract machines compress their state variables, which are reachable only through procedures

N. A. Zafar [13] has modeled moving block railway interlocking system, using an un-directed topology that is dynamic topology in which direction of any track can be switched as needed, and formal specifications are described and validated using a VDM-SL toolbox. This work was one of the benchmarks for developing the abstract model

Xi. Wang, S. Liu, and et al. [13] have modeled the communication-based train control (CBTC) interlocking system. In this method, they used a modern modeling method to build system model, state main safety properties, and perform formal verification using SCADE tool. But using SCADE we lose the state machines and any information on the underlying architecture of the model.

S. Busard, Q. Cappart, C. Limbree, & et al. [5] have modeled railway interlocking based on solid state interlocking (SSI). In this method, they used a modern modeling method to build system model, state main safety properties, and perform formal verification.

Xi malin and Loui vitton [1] have checked large interlocking table using B language and the OVADO tool. But the use of B language is not appropriate to state the interlocking

46

Panchajanya Vidya Peetha Welfare Trust ®

Dr. AMBEDKAR INSTITUTE OF TECHNOLOGY
(An Autonomous Institute, Affiliated to VTU, Belgaum)
BDA Outer Ring Road, Near Jnanabharathi Campus, Mallathahalli, Bangalore-560056.

National Conference on Recent Trends in Science, Engineering and Management

In Association with Institute of Engineering Technology,
Dr. Rammanohar Lohia, Awad University, Ayodhya - 224123, Uttar Pradesh, India

Sponsored by TEQIP - III

THE WORLD BANK
NPIU

Participation Certificate

This Certificate is awarded to Dr./Prof./Mr./Mrs./Ms. ......LOKANNA KADAKALMATH.....................

.................of........VKIT........................Presented/Contributed a paper entitled

Long Tail Web service recommendation using Deep Learning Framework...in the ....

.............of the Trends Recent Trend in Electrical Instrumentation Electronics & Communication

.... under TEQIP-III held on 7th & 8th June 2019 at Dr. AIT, Bangalore-56.

Jayaprakash M

Organizing Secretary

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

Principal

Long Tail Web Service Recommendation using Deep Learning Framework

Lokanna Kadakolmath[1], Anjitha R[2], Archana B S[3], Janhavi D Jadav[4], Kruthika S Sulghur[5]
Department of Computer Science and Engineering
Vivekananda Institute of Technology, Bengaluru- 560074, Karnataka India
{lokanna.vk, anjitha.r98, archanarajubs24, janhavidjadav, kruthikasulghur98}@gmail.com

Abstract—With the number of web services increasing on the internet today, developers are moving towards fusion of multiple services called as hybrids (mashups). Though these mashups find ready services it is difficult on the part of developers to choose which service is better. Recommendation of such services comes into picture. However, developers are more being engrossed towards the services that are non-popular (long tail services), although there is difficulty in understanding the recommendation of long tail web services. The two complications for the recommendation of long tail web services include antiquity of usage data, dissatisfying standard of description content. In this paper we initiate to build a deep learning framework that addresses these complications and performs a precise long tail recommendation. To overcome the problem of dissatisfying standard of description content, we use Stacked Denoising Auto Encoders (SDA) to perform feature extraction. To mark the infrequency of antiquity of usage data, we learn the patterns of developer's inclination instead of modeling individual services.

Index Terms—Long-tail, Mashup Query, Stacked Denoising Auto Encoder

I. INTRODUCTION

From the view of individual web developers, long-tail web service recommendations are also helpful which is demonstrated by giving social media as examples. For instance, whatsapp and telegram are useful in sharing around the globe. However, if developer wants to build a hybrid (mashups) to provide a platform where a user can share a picture, answer conference video and audio calls in an encrypted manner we can use "wickr" app which is a long tail. The figure 1 shows the histogram of long tail services.

In recent days, the long tail services are becoming interesting topics for developers. There are number of recommender systems such as collaborative based, content based and so on. But, they lack in accurate recommendations for long tail services. For recommending high performance and best accuracy web services, we come across two interesting challenges such as, unsatisfactory in developers' description content and lack of historical data usage.

The former challenge can be overcome by incorporating Stacked Denoising Autoencoder (SDA) [12]. SDA forms an important component to learn robust and effective representations. SDA will use screening noise, in order to affect the uncertainty of words provided by developers. For achieving better service representation and mashup queries, the deep denoising neural network plays an important role. The latter challenge explains that due to insufficient long tail usage records, we have considered linear combination of functionalities and various offline factors like update time, usage counts and other side information.
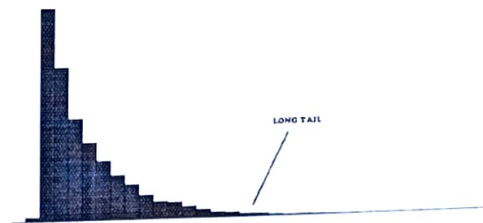

Figure 1: Histogram of long tail.

By making effective usage of above mentioned ideas, these challenges can be overridden and better accuracy with high performance recommendation system can be built.

A. Motivation
In the recent times with explosion of data available on the web, recommendation systems are playing vital role allowing the users to choose the most appropriate services according to their preference. With most developers considering services that have remained less familiar for their mashups, a need for a recommender system that very precisely suggests the most appropriate service comes into picture.

B. Contribution
Generally, user preferences, service features, ratings are used to generate recommendation lists that fails to consider the unfamiliar long tail services. So we have to develop a tool capable of extracting useful features from such services and recommend them to the developers based on the requirements they present in the form of mashup query. Here we intend to integrate the training done offline and the prediction of accurate long tail services.

C. Organization
The rest of this paper is organized as follows: Section II describes various aspects of deep learning used for

48

EAI/Springer Innovations in Communication and Computing

Anandakumar Haldorai
Arulmurugan Ramu
Sudha Mohanram
Chow Chee Onn *Editors*

EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing

BDCC 2018

∞EAI
RESEARCH MEETS INNOVATION

🦎 Springer

Cite this paper

Download citation

.RIS⭳ .ENW⭳ .BIB⭳

Principal
VIVEKANANDA INSTITUTE OF TECHNOLOGY
Bangalore - 560 074

49

Workshop on the Analysis of Big Data

EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing pp 329-338 | Cite as

Message and Image Encryption Embedding Data to GF(2m) Elliptic Curve Point for Nodes in Wireless Sensor Networks

G. Leelavathi, K. Shaila & K. R. Venugopal

Conference paper | First Online: 19 October 2019

Access via your institution   →

˅ Chapter   EUR 29.95
                            Price includes VAT (India)

- Available as PDF
- Read on any device
- Instant download

Cite this paper

Leelavathi, G., Shaila, K., Venugopal, K.R. (2020). Message and Image Encryption Embedding Data to GF(2m) Elliptic Curve Point for Nodes in Wireless Sensor Networks. In: Haldorai, A., Ramu, A., Mohanram, S., Onn, C. (eds) EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-19562-5_33

Download citation

RIS⬇   ENW⬇   BIB⬇

51