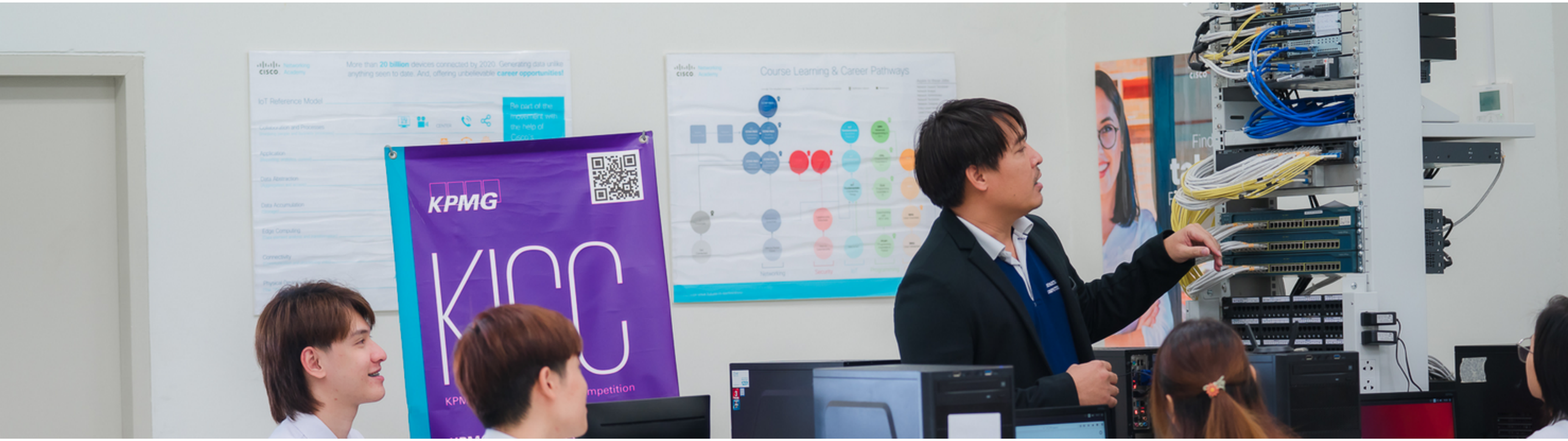


Applied Network Technology (ANT)

Collage of Computing, Khon Kaen University

123 Mitaparb Rd., Naimaung, Maung, Khon Kaen, Thailand

Applied Network Technology

COLLEGE OF COMPUTING
KHON KAEN UNIVERSITY

KKU
KHON KAEN UNIVERSITY

PEOPLE

PROF. DR. CHAKCHAI SO-IN
(HEAD OF ANT LAB)

ASST. PROF. BOONSUP WAIKHAM

ASST. PROF. DR. SATIT KRAVENKIT.

DR. PHET AIMTONGKHAM

DR. ARFAT AHMAD KHAN,

DR. YANIKA KONGSOROT
(RESEARCH SCHOLAR)
KHON KAEN UNIVERSITY

DR. PAKARAT MUSIKAWAN
(RESEARCH SCHOLAR)
KHON KAEN UNIVERSITY

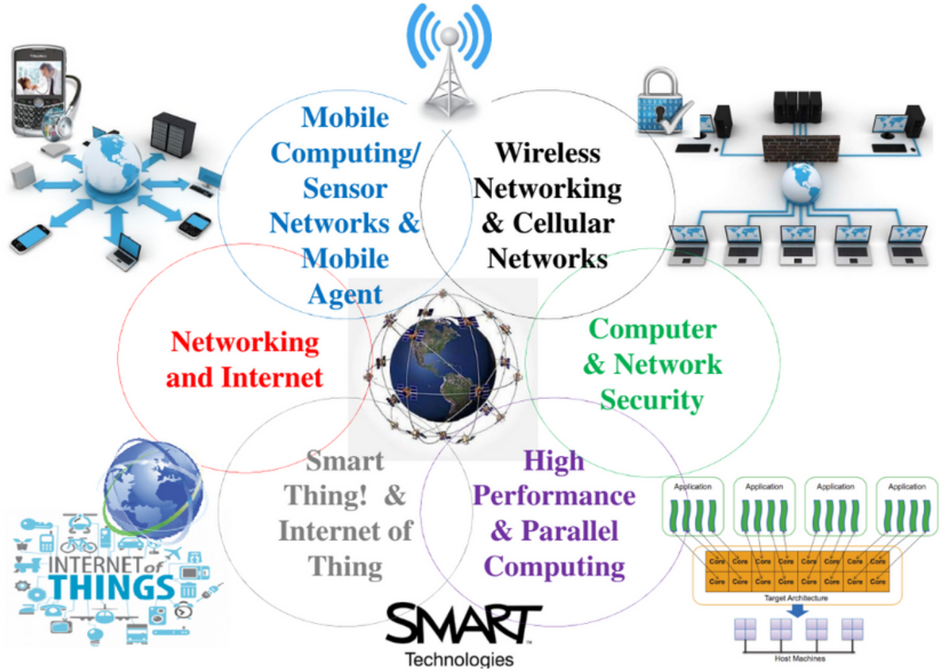
DR. VO NHAN VAN
(RESEARCH SCHOLAR)
DUY TAN UNIVERSITY

DR. SONGYUT PHOEMPHON
(RESEARCH SCHOLAR)
SURANAREE UNIVERSITY
OF TECHNOLOGY

DR. KANOKMON RUJIRAKUL
(RESEARCH SCHOLAR)
NAKHON RATCHASIMAR
RAJABHAT UNIVERSITY

OUR RESEARCH AREA

1. Computer Networks & Internet Technology
2. Wireless and Cellular Networks
3. Wireless Sensor Networks & Ad-Hoc Networks
4. Internet of Things & Cyber-Physical Systems
5. Mobile Computing & Distributed Systems
6. High-Performance Computing & Parallel Computing
7. Cloud & Edge Computing Technology
8. Cyber Security & Cryptography
9. Blockchain & Cryptocurrency Technology
10. Quantum Internet, Communications, and Security
11. Applied Artificial Intelligence & Intelligent Systems
12. Smart Technology (Smart *X*) Home, Farm, Health, Car, Industry, and City



PUBLICATION PROFILE

1. International Books/Chapters (ISBN) (6)
2. National Books/Chapters (ISBN) (16)
3. International Journal Manuscripts (91)
4. International Proceedings Manuscripts (44)
5. Lecture Notes (8)
6. Letter (1)
7. Technical Reports (2)
8. National Publications (19)
9. Petty Patent (5)

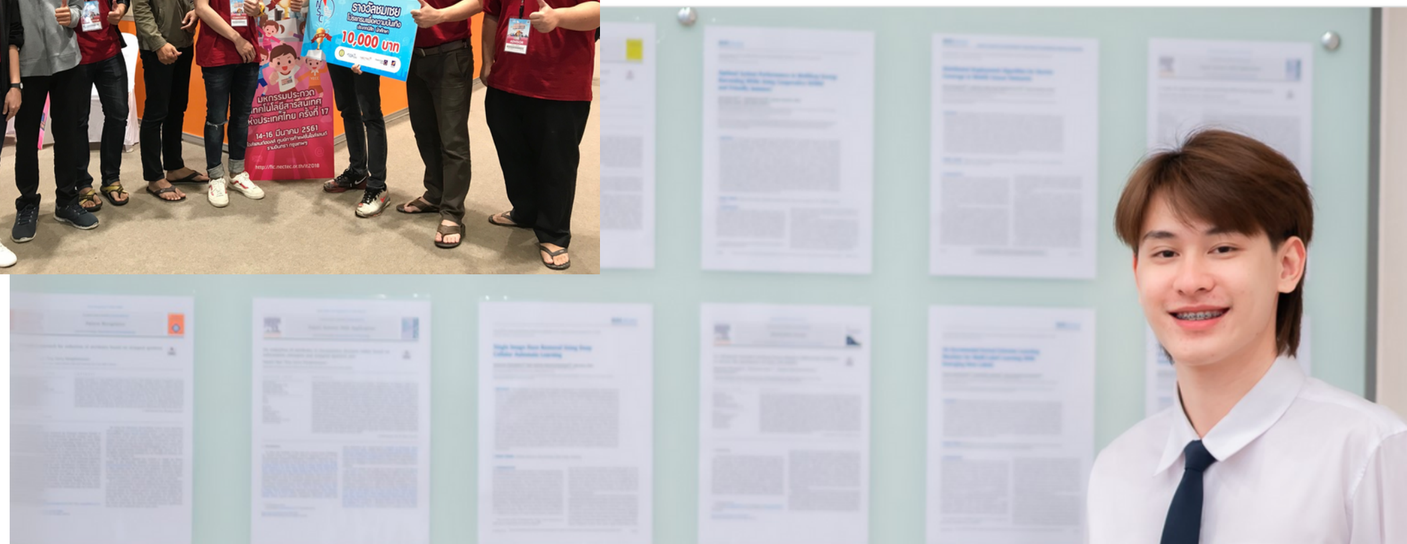
OUR WORKING: EXAMPLES

On-going Research

1. Routing (Network + IoT/ WSN)
2. IoT/ WSN Coverage/Deployment
3. IoT/ WSN Localization
4. IoT/ WSN Security
5. IoT/ WSN Congestion Control
6. IoT/ 5G/ UAV Security and optimization

Project

1. Network/Security Projects
2. IoT/AI Projects



EXAMPLE: RESEARCH (I)

1. Routing (Network + IoT/ WSN)

Expert Systems With Applications 198 (2022) 116767

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

An enhanced fuzzy-based clustering protocol with an improved shuffled leaping algorithm for WSNs

Yanika Kongsorot [a], Pakarat Musikawan [a], Paisarn Muneesawang [b], Chakchai So-In [a,*]

[a] Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, 40002, Thailand
[b] Department of Electrical and Computer Engineering, Faculty of Engineering, Naresuan University, Phisanulok 65000, Thailand

ARTICLE INFO

Keywords:
Wireless sensor networks
Energy consumption
Network lifetime
Shuffled frog leaping algorithm (SFLA)
Clustering protocol
Fuzzy inference system (FIS)

ABSTRACT

Wireless sensor networks (WSNs), an important technology for the Internet of communications among small sensor nodes in a large-scale network. Due to the l small node, a clustering-based approach is used to conserve energy among the n lifetime. The tasks of a clustering-based protocol are related mainly to the sel cluster head nodes (CHs) and next-hop nodes (NHs) based on many influencing decision criterion, which can be addressed using a fuzzy inference system (FIS). Although FISs can provide satisfying decisions for selecting CHs and NHs for clustering protocols, FIS components such as fuzzy input variables, fuzzy rules, and fuzzy membership functions continue to be defined manually in most methods. Thus, these parameters must be tuned appropriately for specific applications. Therefore, in this paper, an enhanced fuzzy-based clustering protocol and an improved shuffled frog leaping algorithm (ISFLA) are proposed. In the proposed protocol, named EFC-ISFLA, a fuzzy-based clustering protocol optimized by the ISFLA is developed to maintain the network lifetime. The appropriate CHs are selected based on the energy threshold and optimized FIS with respect to the distance between adjacent CHs defined by the overlay boundary, resulting in reduced energy consumption and a longer network lifetime. Additionally, cluster formation and NH selection are performed based on the optimized FISs. A new encoding scheme is also designed to tune the network parameters and the FIS components simultaneously through the ISFLA. In the ISFLA, opposition-based operators and a surrogate model are adopted to address the limitations of the traditional SFLA. The experimental results show that the proposed technique provides better results in terms of maximizing the network lifetime, network stability, and total number of data packets delivered to the base station (BS).

IEEE INFOCOM 2023 - IEEE Conference on Computer Communications | 979-8-3503-3414-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/INFOCOM53939.2023.10228948

Designing Optimal Compact Oblivious Routing for Datacenter Networks in Polynomial Time

Kanatip Chitavisutthivong[†], Chakchai So-In[‡], Sucha Supittayapornpong[†]
[†]Vidyasirimedhi Institute of Science and Technology, Thailand
[‡]Khon Kaen University, Thailand

***Abstract*—Recent datacenter network topologies are shifting towards heterogeneous and structured topologies for high throughput, low cost, and simple manageability. However, they rely on sub-optimal routing approaches that fail to achieve their designed capacity. This paper proposes a process for designing optimal oblivious routing that is programmed compactly on programmable switches. The process consists of three contributions in tandem. We first transform a robust optimization problem for designing oblivious routing into a linear program, which is solvable in polynomial time but cannot scale for datacenter topologies. We then prove that the repeated structures in a datacenter topology lead to a structured optimal solution. We use this insight to formulate a scalable linear program, so an optimal oblivious routing solution is obtained in polynomial time for large-scale topologies. For real-world deployment, the optimal solution is converted into forwarding rules for programmable switches with stringent memory. With this constraint, we utilize the repeated structures in the optimal solution to group the forwarding rules, resulting in compact forwarding rules with a much smaller memory requirement. Extensive evaluations show our process i) obtains optimal solutions faster and more scalable than a state-of-the-art technique and ii) reduces the memory requirement by no less than 90% for most considered topologies.**

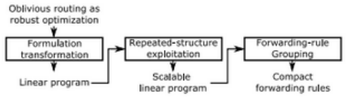


Fig. 1. The design process of optimal compact oblivious routing.

I. Introduction

The design of network topologies for data centers is currently shifting towards heterogeneous, structured topologies for high capacity, low cost, and low manageability [1], [2]. This attempts to replace the folded-Clos family, including FatTree [3], Google's Jupiter [4], Facebook's Fabric [5], and Microsoft's VL2 [6]. Alternative topologies have been proposed, such as Xpander [7], FatClique [2], DRing [8], SlimFly [9], and other server-centric networks, where servers have routing capability, such as BCube [10] and DCell [11]. However, some of them [2], [7], [8], [11] rely on sub-optimal routing approaches, while the others [9], [10] use dynamic routing that requires specialized hardware. This leads to an active research problem of how to design oblivious routing that achieves designed capacity without specialized hardware for these and future topologies [12].

The oblivious routing approach is widely used in production networks because of its robustness and simplicity. The routes from every source to every destination are designed to be robust to traffic variation, so neither re-configuration nor dynamic routing is required when traffic changes. For example, the folded-Clos family often employs the Equal-Cost Multi Paths (ECMP) routing approach [13] that splits traffic equally across all equal-cost paths, whose cost is independent of traffic. Another oblivious routing approach is Valiant Load Balancing (VLB) [14], [15], in which a traffic from a source is split equally to a set of intermediate switches, each then routes the received traffic to a destination. While, the ECMP and VLB approaches are optimal respectively for the folded-Clos and clique networks, they are sub-optimal for the alternative topologies due to topological differences.

Generally, designing an optimal oblivious routing solution for an arbitrary network topology is equivalent to solving a robust optimization problem [12], [15]–[17]. The work in [16] views this problem as a game and derived a linear program for intra-domain networks, albeit small-scale networks in comparison to datacenter networks. The recent work in [12] exploits the repeated network structures to reduce the complexity of a robust optimization problem, so an optimal oblivious routing solution is obtained for larger network sizes. In short, the first work can obtain the optimal routing solution in polynomial time (in the size of input instance, which is extremely large for large-scale networks), while the second work can scale to larger networks but could take non-polynomial time due to the complexity of robust optimization. This beg an open question: *Could we design optimal oblivious routing in polynomial time that also scales for large datacenter networks to achieve the best of both worlds?*

The memory constraint is another important issue for the real-world deployment of the oblivious routing. After an optimal routing solution is obtained, it is converted to forwarding rules that determine how traffic is split at each switch in a network. These rules are stored on switches with limited memory capacity, which becomes an issue for large-scale datacenter networks with thousands of destinations. The previous work in [18] trade-off split accuracy with memory

This work was supported by Office of the Permanent Secretary, Ministry of Higher Education, Science, Research and Innovation (OPS MHESI), Thailand Science Research and Innovation (TSRI), Vidyasirimedhi Institute of Science and Technology (VISTEC) under Grant No. RGNS 65-216.

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received June 22, 2021, accepted June 27, 2021, date of publication July 5, 2021, date of current version July 13, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3094541

Fuzzy Logic-Based Path Planning for Data Gathering Mobile Sinks in WSNs

CHATCHAI PUNRIBOON[1], CHAKCHAI SO-IN[1], (Senior Member, IEEE), PHET AIMTONGKHAM[1], AND NUTTHANON LEELATHAKUL[2]
[1]Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[2]Faculty of Informatics, Burapha University, Chonburi 20131, Thailand

Corresponding author: Nutthanon Leelathakul (nutthanon@buu.ac.th)

This work was supported in part by the Thailand Science Research and Innovation (TSRI), in part by the National Research Council of Thailand (NRCT) through the International Research Network Program under Grant IRN61W0006, and in part by Khon Kaen University, Thailand.

ABSTRACT Mobile sinks (MSs) are capable of collecting data along specified paths in wireless sensor networks (WSNs). They are deployed as a popular alternative for data loggers, to which all nodes have to send sensory data. If MSs' paths (or cycles) are not well determined, it might take a relatively long time for the MSs to make a round trip. Recent research works have proposed methods to determine rendezvous points (RPs) that the MSs must pass by to collect data, with the aim of reducing the data-collection time. Determination of the number of RPs is important, and it is challenging to make ensure that there are sufficient RPs widely located throughout a sensor network, forming a circle along which the MSs can spend limited time traveling. This research presents a method for designing paths and pinpointing RPs for MSs to collect data, as well as determining the next hop to relay data for each sensor node. Instead of reducing the MSs' travel time, the focus of this research is to preserve the energy of all sensor nodes in WSNs. Our method determines the maximum number of RPs such that the MSs can run through each RP's communication range (within a time constraint) without depleting their own energy. The method comprises three main steps. First, we calculate the number of RPs and design the MS path. Second, the exact data-collection points are determined. The last step is to specify the path along which sensory data are relayed to the MS. In our experiments, we simulate two WSNs of different sizes. The results show that our method outperforms the others by 70%-80% in terms of the sensor node uptime, power consumption, MS traveling time and the number of RPs.

Journal of Ambient Intelligence and Humanized Computing (2021
https://doi.org/10.1007/s12652-020-02090-z

ORIGINAL RESEARCH

An energy-efficient fuzzy-based scheme for unequal multihop clustering in wireless sensor networks

Songyut Phoemphon[1] · Chakchai So-In[1] · Phet Aimtongkham[1] · Tri Gia Nguyen[1,2]

Received: 11 December 2019 / Accepted: 5 May 2020 / Published online: 16 May 2020

Abstract
Currently, wireless sensor networks (WSNs) are providing practical solutions for various applications, including smart agriculture and healthcare, and have provided essential support by wirelessly connecting the numerous nodes or sensors that function in sensing systems needed for transmission to backends via multiple hops for data analysis. One key limitation of these sensors is the self-contained energy provided by the embedded battery due to their (tiny) size, (in) accessibility, and (low) cost constraints. Therefore, a key challenge is to efficiently control the energy consumption of the sensors, or in other words, to prolong the overall network lifetime of a large-scale sensor farm. Studies have worked toward optimizing energy in communication, and one promising approach focuses on clustering. In this approach, a cluster of sensors is formed, and its representatives, namely, a cluster head (CH) and cluster members (CMs), with the latter transmitting the sensing data within a short range to the CH. The CH then aggregates the data and forwards it to the base station (BS) using a multihop method. However, maintaining equal clustering regardless of key parameters such as distance and density potentially results in a shortened network lifetime. Thus, this study investigates the application of fuzzy logic (FL) to determine various parameters and membership functions and thereby obtain appropriate clustering criteria. We propose an FL-based clustering architecture consisting of four stages: competition radius (CR) determination, CH election, CM joining, and determination of selection criteria for the next CH (relaying). A performance analysis was conducted against state-of-the-art distributed clustering protocols, i.e., the multiobjective optimization fuzzy clustering algorithm (MOFCA), energy-efficient unequal clustering (EEUC), distributed unequal clustering using FL (DUCF), and the energy-aware unequal clustering fuzzy (EAUCF) scheme. The proposed method displayed promising performance in terms of network lifetime and energy usage.

EXAMPLE: RESEARCH (II)

2. IoT/ WSN Coverage/Deployment

Expert Systems With Applications 189 (2022) 116035

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

An enhanced obstacle-aware deployment scheme with an opposition-based competitive swarm optimizer for mobile WSNs

Pakarat Musikawan [a], Yanika Kongsorot [a], Paisarn Muneesawang [b], Chakchai So-In [a,*]

[a] Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen, 40002, Thailand
[b] Department of Electrical and Computer Engineering, Faculty of Engineering, Naresuan University, Phisanulok 65000, Thailand

ARTICLE INFO

Keywords:
Deployment optimization
Mobile wireless sensor networks
Competitive swarm optimizer
Metaheuristic algorithm
Voronoi diagram
Virtual force algorithm
Node deployment
Coverage area

ABSTRACT

The network coverage problem for an area with a randomly deployed wireless sensor network (WSN) in the presence of obstacles can be alleviated through mobile sensor nodes. However, the requirement for the dissipated energy in mobility and sensing has increased. Therefore, energy efficient coverage is a significant issue and has been near-optimally solved by heuristic techniques. Focusing on this issue, this paper introduces an improved competitive swarm optimizer to maximize the coverage area and minimize the network energy simultaneously. The proposed method incorporates the virtual force algorithm (VFA) and the Voronoi diagram (VD) to improve the network performance during the optimization process. The VFA is combined with a boundary mechanism to control the locations of sensors, while the VD is utilized to extract the network information for the decoding process. The superior performance of the model is verified by intensive evaluations against state-of-the-art techniques in terms of the coverage ratio and network energy consumption.

Peer-to-Peer Netw. Appl. (2017) 10:519–536
DOI 10.1007/s12083-016-0524-6

A novel energy-efficient clustering protocol with area coverage awareness for wireless sensor networks

Tri Gia Nguyen [1,2] · Chakchai So-In [1] · Nhu Gia Nguyen [3] · Songyut Phoemphon [1]

Received: 3 May 2016 / Accepted: 4 October 2016 / Published online: 18 October 2016

Received February 12, 2018, accepted March 13, 2018, date of publication April 2, 2018, date of current version May 2, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2822263

Distributed Deployment Algorithm for Barrier Coverage in Mobile Sensor Networks

TRI GIA NGUYEN [1,2], (Member, IEEE), AND CHAKCHAI SO-IN [2], (Senior Member, IEEE)
[1] Faculty of Information Technology, Duy Tan University, Da Nang 550000, Vietnam
[2] Applied Network Technology Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
Corresponding author: Chakchai So-In (chakso@kku.ac.th)

This work was supported by the Research Affairs and Graduate School, Khon Kaen University, Thailand, through the Post-Doctoral Training Program under Grant 59257.

ABSTRACT The deployment of sensor nodes (SNs) to form a network with coverage ability is one of the most important challenges of wireless sensor networks. In this paper, we study an efficient distributed deployment algorithm for barrier coverage improvement with mobile sensors, in which the SNs can be relocated after the initial deployment. To achieve the maximum number of barriers, we propose a distributed algorithm to construct k-barrier coverage by relocation of the SNs. Different from existing approaches, we propose a novel clustering technique based on the network area to reduce the information exchange messages. Then, based on the SNs clusters, we propose a heuristic method to assign the SNs evenly into each cluster with regard to the required number of SNs of each cluster and decide the moving SNs by computing the optimal relocation, considering moving distance minimization. The main goal of this approach is to relocate the SNs to form the maximum number of barriers with a minimum relocation cost, in terms of sensor energy consumption of communication and movement. The simulation results demonstrate the effectiveness of our algorithm when compared with other competing approaches.

Peer-to-Peer Networking and Applications (2019) 12:541–552
https://doi.org/10.1007/s12083-018-0675-8

An efficient coverage hole-healing algorithm for area-coverage improvements in mobile sensor networks

Chakchai So-In [1] · Tri Gia Nguyen [2] · Nhu Gia Nguyen [3]

Received: 1 October 2017 / Accepted: 7 August 2018 / Published online: 31 August 2018

Abstract
Maximizing network coverage is among the key factors in designing efficient sensor-deployment algorithms for wireless sensor networks (WSNs). In this study, we consider a WSN in which mobile sensor nodes (SNs) are randomly deployed over a two-dimensional region with the existence of coverage holes due to the absence of any SNs. To improve the network coverage, we thus propose a novel distributed deployment algorithm – coverage hole-healing algorithm (CHHA) – to maximize the area coverage by healing the coverage holes such that the total SN moving distance is minimized. Once the network is formed after an initial random placement of the SNs, CHHA is applied to detect coverage holes, including hole-boundary SNs, based on computational geometry, i.e., Delaunay triangulation. The distributed deployment feature of CHHA applies a concept to virtual forces that is used to decide the movement of mobile SNs to heal the coverage holes. The simulation results show that our proposed algorithm is capable of exact detection of coverage holes in addition to area-coverage improvement by healing the holes. The results also demonstrate the effectiveness of CHHA compared with other competitive approaches, namely, VFA, VEDGE, and HEAL, in terms of total moving distance.

…in evaluating the monitor-…ces in wireless sensor net-…of self-contained sensors is …rgy-efficient use while still …ance. Although techniques …e problem of area coverage, …t clustering methods, none … activation stage, which is …ptimizing energy usage. In …ver set to find the minimum …r the sensing ranges within …ensor activation. Our main …r of active sensors consid-…r set and to keep alive the … coverage task as long as …search proposes an area …ol (ACACP) with energy … respect to the activation sensor, network clustering, and multi-hop communication to improve overall network lifetime while preserving coverage. Throughout the intensive simulation, given a diversity of deployments with scalability concern, the results demonstrate the effectiveness of ACACP when compared with other competitive approaches such as ECDC and DECAR, including state-of-the-art clustering protocols such as LEACH, in terms of coverage ratio and overall network lifetime.

Keywords Area coverage · Clustering · Coverage-awareness · Multi-hop communication · Sensor activation · Wireless sensor networks

1 Introduction

In recent years, wireless sensor networks (WSNs) have attracted considerable attention in research communities due to their widespread practical applications such as reconnoiter-

EXAMPLE: RESEARCH (III)

3. IoT/ WSN Localization

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

A hybrid localization model using node segmentation and impr particle swarm optimization with obstacle-awareness for wirel sensor networks

Songyut Phoemphon[a], Chakchai So-In[a,*], Nutthanon Leelathakul[b]

[a] Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40
[b] Faculty of Informatics, Burapha University, Chon Buri 20131, Thailand

ARTICLE INFO

Article history:
Received 4 July 2019
Revised 7 October 2019
Accepted 17 October 2019
Available online 30 October 2019

Keywords:
Localization
Node segmentation
Obstruction
Particle swarm optimization
Wireless Sensor Networks

ABSTRACT

Other than energy consumption, precision is of the utmost importance in node localization. Various wireless-sensor-network applications require the accurate information of sensor nodes' locations. For instance, an enemy intrusion detection system (e.g., geo-fencing) needs accurate sensor nodes' locations to detect where intruding enemies are located. As practical examples, forest fire, landslide, and water quality monitoring systems require the early identification of root causes' exact locations before they can widely spread. In general, range-based localization techniques often yield higher accuracies because the localization estimation can be directly derived from the distance between hops and can leverage received signal strength indicator (RSSI) values but require model approximation of various hops and distances as in range-free localization techniques. However, the important factor that affects the accuracies is sensor node positioning, especially when sensor nodes (SNs) are spread across areas filled with obstructions causing less localization accuracy. Due to the diffraction caused by obstructions, the approximate distances between pairs of anchor nodes and unknown nodes using RSSI can differ substantially from the actual values. This research, therefore, aims to improve sensor node localization in situations where SNs are in areas with obstructions. We propose a novel technique, node segmentation with improved particle swarm optimization (NS-IPSO) that divides SNs into segments to improve the accuracy of the estimated distances between pairs of anchor nodes and unknown nodes. First, we determine candidate sensor nodes that could potentially be used to segment anchor nodes in the area. Such sensor nodes (STs) are those on the shortest paths between anchor nodes that appear more often than the average appearances of all sensor nodes. Then, segment nodes (SMs, sensor nodes for segmenting the anchor nodes) are selected from all the other STs based on certain specified conditions. To further improve the localization precision, we

Fuzzy Weighted Centroid Localization With Virtual Node Approximation in Wireless Sensor Networks

Songyut Phoemphon, Chakchai So-In, *Senior Member, IEEE*, and Nutthanon Leelathakul

***Abstract*—Due to their low cost, various range-free localization techniques are widely applied to estimate device locations in wireless sensor networks (WSNs), especially where other communication signals, such as those from a global positioning system, are absent. Among range-free techniques, the centroid algorithm has gained popularity because of its simplicity and low computational cost, rendering it suitable for power-sensitive sensor nodes or nodes. WSN topologies are unpredictable because sensor nodes are often deployed at arbitrary locations, making it difficult for sufficient numbers of known (anchor) nodes to cover all unknown nodes. Consequently, both centroid algorithm and its enhanced versions [e.g., weighted centroid (WC) algorithms] yield relatively high localization inaccuracy. In this paper, to successfully form anchor-node triangles, we propose a low-cost technique to determine the number of virtual anchor nodes or virtual nodes together with their positions. Specifically, we develop and provide proof for accurate approximate unknown node sides. We also improve localization accuracy by adding virtual nodes that collaborate with physical anchor nodes to provide the necessary coverage of the unknown nodes. We address estimations of unknown node locations by applying a fuzzy-based centroid localization method to prioritize anchor nodes by assigning different fine-tuned weighted factors. The results show that the proposed algorithm outperforms state-of-the-art fuzzy-based localization techniques for WC algorithms.**

routing, self-organizing, and self-computing) to form a wireless sensor network (WSN). In addition to sending data, sensor nodes deliver commands to control various devices. There are many types of connecting devices, and networks may be large; therefore, data are normally relayed via wireless connections to mitigate the impact of inaccessible terrain. One feature of a WSN is its ad hoc protocol: a WSN depends only on itself, unlike a cellular or wireless local area network, which may require infrastructure [1].

In recent years, WSNs have evolved in many respects. They require much less energy due to micro electro mechanical system sensors. Advances in embedded system technologies have led to the development of WSNs that meet real industrial needs. For instance, they guarantee quality of service [2], facilitate data aggregation [3], and achieve real-time communication [4], and provide energy-aware computing and transmission [5].

To put WSNs to good use, it is necessary to know the locations of sensor nodes. Therefore, it is important to address localization problems. Sensor nodes are often small and are designed to save energy; equipping each of them with a global

Expert Systems With Applications 175 (2021) 114773

Contents lists available at ScienceDirect

Expert Systems With Applications

journal homepage: www.elsevier.com/locate/eswa

Improved distance estimation with node selection localization and particle swarm optimization for obstacle-aware wireless sensor networks

Songyut Phoemphon[a], Chakchai So-In[a,*,1], Nutthanon Leelathakul[b]

[a] Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[b] Faculty of Informatics, Burapha University, Chon Buri 20131, Thailand

ARTICLE INFO

Keywords:
Wireless sensor networks
Node localization
Obstacle awareness
Anchor node selection
Improved distance estimation
Bounding box
Particle swarm optimization

ABSTRACT

Sensor-node localization is among the greatest concerns in the field of wireless sensor networks. Range-based localization techniques generally outperform range-free techniques, particularly in terms of their accuracy. Range-based localization techniques depend on a popular distance estimation method, which requires conversion from a received signal strength indicator to distances. In a case where sensor nodes are in an area with obstacles, direct communication between certain pairs of nodes is impracticable; the data must be relayed over multihop (or detour) routes. One promising approach to improve the accuracy of sensor-node distance estimation is to segment (or cluster) sensor nodes to a restricted set of anchor nodes whose estimated distances to unknown nodes are not on a detour route. Some certain topologies can decrease the localization precision; e.g., when each group's node density is low, large empty spaces (or gaps) might affect the localization precision. If an unknown node is close to another group, using only anchor nodes within its own group could reduce the estimation precision. When anchor nodes within the same group lie along a straight line, the approximation of the unknown-node location could be misinterpreted. Thus, to enhance the localization precision, we make use of anchor nodes in other nearby groups to estimate the locations of unknown nodes. We also apply particle swarm optimization (PSO) with an improved fitness function to estimate the locations of unknown nodes. The localization performance is intensively evaluated in obstacle-prone scenarios. The simulation results show that the proposed scheme achieves higher accuracy than recent state-of-the-art PSO-based methods.

Journal of Network and Computer Applications

Available online 10 November 2023, 103783

In Press, Journal Pre-proof What's this?

An enhanced node segmentation and distance estimation scheme with a reduced search space boundary and improved PSO for obstacle-aware wireless sensor network localization

Songyut Phoemphon[a], Nutthanon Leelathakul[b], Chakchai So-In[c]

Show more

https://doi.org/10.1016/j.jnca.2023.103783

EXAMPLE: RESEARCH (IV)

4. IoT/ WSN Security

An Enhanced Deep Learning Neural Network for the Detection and Identification of Android Malware

Pakarat Musikawan, Yanika Kongsorot, Ilsun You, *Senior Member, IEEE*, and Chakchai So-In, *Senior Member, IEEE*

***Abstract*—Android-based mobile devices have attracted a large number of users because they are easy to use and possess a wide range of capabilities. Because of its popularity, Android has become one of the most important platforms for attackers to launch their nefarious schemes. Due to the rising sophistication of Android malware obfuscation and detection avoidance tactics, many traditional malware detection approaches have become impractical due to their limited representation capabilities. Inspired by the success of deep learning in representation learning, this article presents an effective improved deep neural network to safeguard Android devices from malicious apps called AMDI-Droid. The presented approach contains three enhancements: 1) from the ensemble classifier perspective, we propose a new architecture based on a deep neural network, where the predictive outputs obtained from all hidden layers are blended to produce a final prediction; 2) the first hidden layer learns an effective feature representation from the original data through multiple subnetworks; and 3) a loss function is formulated by combining the predictive loss of each base classifier connected to the corresponding hidden layer. The superior performance of the proposed model is verified via intensive evaluations against state-of-the-art techniques in terms of the accuracy, precision, recall, *F*1-score, and Matthews correlation coefficient (MCC) metrics.**

worldwide has grown, from 3.6 billion in 2016 to 6.3 bill in 2021, marking a 75% growth over a rather short 5-y period [48], [69]. Moreover, the report released by Stati illustrates that the number of smartphone users could rea 7.3 billion in 2025; this is more than half of the worl population [47].

Android devices are broadly employed because of their v satile operating system (OS), which can run on smartphon tablets, smartwatches, and Internet of Things (IoT) devices. Due to benefits, such as opensource functionality, scalabil- ity, and simplicity, the Android OS has surpassed all others as the most popular mobile platform [80]. The Android OS has retained its position as the leading mobile OS worldwide, with a market share of 72.26% in the first quarter of 2020, as reported by Statcounter [2], [68]. However, due to its open- ness, many Android applications in the Android market hide malicious software (malware), posing a significant threat to cyberspace security [80]. According to the 2019 Nokia annual threat intelligence report, Android devices were the devices

Multidirectional Trust-Based Security Mechanisms for Sinkhole Attack Detection in the RPL Routing Protocol for Internet of Things

Sopha Khoeurt[1], Chakchai So-In[2], Pakarat Musikawan[3] and Phet Aimtongkham[4*]

[1]Applied Network Technology (ANT), Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, Thailand. sopha.k@kkumail.com, Orcid: https://orcid.org/0009-0007-2809-2399

[2]Applied Network Technology (ANT), Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, Thailand. chakso@kku.ac.th, Orcid: https://orcid.org/0000-0003-1026-191X

[3]Advanced Intelligent Interdisciplinary Integration (AIII), Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, Thailand. pakamu@kku.ac.th, Orcid: https://orcid.org/0000-0001-5315-751X

[4*]Applied Network Technology (ANT), Department of Computer Science, College of Computing, Khon Kaen University, Khon Kaen, Thailand. phetim@kku.ac.th, Orcid: https://orcid.org/0000-0001-5289-1149

Received: May 15, 2023; Accepted: June 30, 2023; Published: September 30, 2023

Abstract

The Internet of Things (IoT) has gained popularity in recent years by connecting physical objects to the Internet, enabling innovative applications. To facilitate communication in low-power and lossy networks (LLNs), the IPv6-based routing protocol for LLNs (RPL) is widely used. However, RPL's lack of specified security models makes it vulnerable to security threats, particularly sinkhole attacks. Existing sinkhole attack detection techniques suffer from high detection delays and false positives. To overcome these limitations, in our research we propose a multidire detection approach for sinkhole attacks in the RPL routing protocol. Our model architecture that considers trust in parent, child, and neighbor directions, reducing We enhance detection efficiency and reduce false positives by combining fu (FLSs) and subjective logic (SL). Additionally, we introduce a new trust weigh from Shannon's entropy method and multiattribute utility theory. We adaptiv coefficient based on network conditions, replacing the constant coefficient value approach is compared to the most recent techniques, and we assess different indica positive rate, false-negative rate, packet delivery ratio, throughput, average consumption. Our results demonstrate superior performance in all these metrics effectiveness of our approach.

Keywords: Sinkhole Attack, RPL Attack, IoT, Fuzzy Logic System, Subjective

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applicatic volume: 14, number: 3 (September), pp. 48-76 DOI: *10.58346/JOWUA.2023.I3.005*

*Corresponding author: Applied Network Technology (ANT), Department of Compu Computing, Khon Kaen University, Khon Kaen, Thailand.

Future Generation Computer Systems 102 (2020) 198–209

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Averaged dependence estimators for DoS attack detection in IoT networks

Zubair A. Baig [a], Surasak Sanguanpong [b], Syed Naeem Firdous [c], Van Nhan Vo [d,e], Tri Gia Nguyen [e], Chakchai So-In [d,*]

[a] School of Information Technology, Deakin University, Geelong, Victoria, 3220, Australia
[b] Department of Computer Engineering, Faculty of Engineering, Kasetsart University, 10900, Thailand
[c] Edith Cowan University, Perth, 6000, Australia
[d] Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen, 40002, Thailand
[e] Faculty of Information Technology, Duy Tan University, Da Nang, 550000, Viet Nam

HIGHLIGHTS

- DoS attack detection for IoT platforms.
- AODE-based classification of network traffic.
- Machine learning and applications for network security in IoT on 5G networks.

ARTICLE INFO

Article history:
Received 15 January 2019
Received in revised form 3 July 2019
Accepted 6 August 2019
Available online 8 August 2019

Keywords:
Internet of Things
Communication system security
Machine learning algorithms

ABSTRACT

Wireless sensor networks (WSNs) have evolved to become an integral part of the contemporary Internet of Things (IoT) paradigm. The sensor node activities of both sensing phenomena in their immediate environments and reporting their findings to a centralized base station (BS) have remained a core platform to sustain heterogeneous service-centric applications. However, the adversarial threat to the sensors of the IoT paradigm remains significant. Denial of service (DoS) attacks, comprising a large volume of network packets, targeting a given sensor node(s) of the network, may cripple routine operations and cause catastrophic losses to emergency services. This paper presents an intelligent DoS detection framework comprising modules for data generation, feature ranking and generation, and training and testing. The proposed framework is experimentally tested under actual IoT attack scenarios, and the accuracy of the results is greater than that of traditional classification techniques.

An Intrusion Detection and Identification System for Internet of Things Networks using a Hybrid Ensemble Deep Learning Framework

Yanika Kongsorot, Pakarat Musikawan, Phet Aimtongkham, Ilsun You, *Senior Member, IEEE*, Abderrahim Benslimane, *Senior Member, IEEE*, and Chakchai So-In, *Senior Member, IEEE*,

Abstract—Owing to the exponential proliferation of internet services and the sophistication of intrusions, traditional intrusion detection algorithms are unable to handle complex invasions due to their limited representation capabilities and the unbalanced nature of Internet of Things (IoT)-related data in terms of both telemetry and network traffic. Drawing inspiration from deep learning achievements in feature extraction and representation learning, in this study, we propose an accurate hybrid ensemble deep learning framework (HEDLF) to protect against obfuscated cyber-attacks on IoT networks . To address complex features and alleviate the imbalance problem, the proposed HEDLF includes three key components: (1) a hierarchical feature representation technique based on deep learning, which aims to extract specific information by supervising the loss of gradient information; (2) a balanced rotated feature extractor that simultaneously encourages the individual accuracy and diversity of the ensemble classifier; and (3) a meta-classifier acting as an aggregation method, which leverages a semisparse group regularizer to analyze the base classifiers' outputs. Additionally, these improvements take class imbalance into account. The experimental results show that when compared against state-of-the-art techniques in terms of accuracy, precision, recall, and F1-score, the proposed HEDLF can achieve promising results on both telemetry and network traffic data.

EXAMPLE: RESEARCH (V)

5. IoT/ WSN Congestion Control

Wireless Networks (2021) 27:1287–1308
https://doi.org/10.1007/s11276-020-02513-x

Multistage fuzzy logic congestion-aware routing using d notification and the relative barring distance in wireless networks

Phet Aimtongkham[1] · Paramate Horkaew[2] · Chakchai So-In[1]

Accepted: 27 November 2020 / Published online: 2 January 2021

Abstract
Congestion management in a wireless sensor network (WSN) is a key determinant of the quality of service. Congestion in a network causes data loss, a reduced transmission rate, increased delays, and excess energy consumption. The latter has a direct impact on tiny sensor devices with limited resources and processing, buffering, and transmitting capabilities. In addition, a WSN relies on multiple packet relays between nodes, which inevitably results in network congestion near the base station, whose neighboring nodes incur crowded traffic from multisource deliveries. Thus, this paper proposes a novel routing method that minimizes congestion. The adaptive routing strategy consists of 3 main modules. First, an optimal notification level for queue control is specified by using multistage fuzzy logic (MFL). The resulting weights evaluated from congestion-related parameters are then passed onto the subsequent modules. The second module adjusts the congestion notification, which makes the module more flexible to improve its routing discovery efficiency and to reduce the chance of loss during the rerouting stage. Finally, we propose a routing adjustment and control mechanism by using a novel navigation technique based on linear and angular distances and MFL to create weights for path assessment. Simulation results demonstrate that the proposed method outperforms the state-of-the-art methods in terms of the packet loss ratio, average hop count, network lifetime, and energy consumption metrics.

Wireless Networks (2020) 26:3603–3627
https://doi.org/10.1007/s11276-020-02289-0

Fuzzy logic rate adjustment controls using a circuit breaker for persistent congestion in wireless sensor networks

Phet Aimtongkham[1] · Sovannarith Heng[1,2] · Paramate Horkaew[3] · Tri Gia Nguyen[1] · Chakchai So-In[1]

Published online: 4 March 2020

Abstract
Congestion control is necessary for enhancing the quality of service in wireless sensor networks (WS sensing technology, a substantial amount of data traversing a WSN can easily cause congestion, es resources. As a consequence, network throughput decreases due to significant packet loss and increa congestion not only adversely affects the data traffic and transmission success rate but also excessi which in turn reduces the sensor node and, hence, network lifespans. A typical congestion control st address congestion due to transient events. However, on many occasions, congestion was caused and, as a consequence, persisted for an extended period. This paper thus proposes a congestion co eliminate both types of congestion. The study adopted a fuzzy logic algorithm for resolving congest optimal path selection, traffic rate adjustment that incorporates a momentum indicator, and an optim circuit breaker to limit persistent congestion. With fuzzy logic, decisions can be made efficiently weights derived from fitness functions of congestion-relevant parameters. The simulation and experi herein demonstrate that the proposed strategy outperforms state-of-the-art strategies in terms of mission delay, queue utilization, and energy efficiency.

Received February 22, 2021, accepted March 19, 2021, date of publication April 12, 2021, date of current version April 23, 2021.
Digital Object Identifier 10.1109/ACCESS.2021.3072625

An Enhanced CoAP Scheme Using Fuzzy Logic With Adaptive Timeout for IoT Congestion Control

PHET AIMTONGKHAM[1], PARAMATE HORKAEW[2], AND CHAKCHAI SO-IN[1], (Senior Member, IEEE)
[1]Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen 40002, Thailand
[2]School of Computer Engineering, Institute of Engineering, Suranaree University of Technology, Nakhon Ratchasima 30000, Thailand
Corresponding author: Chakchai So-In (chakso@kku.ac.th)

This work was supported in part by a grant through the Post-Doctoral Training Program under the Thailand Science Research and Innovation (TSRI), and in part by the National Research Council of Thailand (NRCT) through the International Research Network Program under Grant IRN61W0006 and Khon Kaen University.

ABSTRACT Congestion management in the Internet of Things (IoT) is one of the most challenging tasks in improving the quality of service (QoS) of a network. This is largely because modern wireless networks can consist of an immense number of connections. Consequently, limited network resources can be consumed simultaneously. This eventually causes congestion that has adverse impacts on both throughput and transmission delay. This is particularly true in a network whose transmissions are regulated by the Constrained Application Protocol (CoAP), which has been widely adopted in the IoT network. CoAP has a mechanism that allows connection-oriented communication by means of acknowledgment messages (ACKs) and retransmission timeouts (RTOs). However, during congestion, a client node is unable to efficiently specify the RTO, resulting in unnecessary retransmission. This overhead in turn causes even more extensive congestion in the network. Therefore, this research proposes a novel scheme for optimally setting the initial RTO and adjusting the RTO backoff that considers current network utilization. The scheme consists of three main components: 1) a multidimensional congestion estimator that determines congestion conditions in various aspects, 2) precise initial RTO estimation by means of a relative strength indicator and trend adaptive-boundary backoff sented here reveal that the d, delay and percentage of

Research Article

Congestion Control and Prediction Schemes Using Fuzzy Logic System with Adaptive Membership Function in Wireless Sensor Networks

Phet Aimtongkham, [1] Tri Gia Nguyen, [2] and Chakchai So-In [1]

[1]*Applied Network Technology (ANT) Laboratory, Department of Computer Science, Faculty of Science, Khon Kaen University, Khon Kaen, Thailand*
[2]*Department of Information Technology, Duy Tan University, Vietnam*

Correspondence should be addressed to Chakchai So-In; so-in@ieee.org

Received 27 March 2018; Revised 21 June 2018; Accepted 4 July 2018; Published 1 August 2018

Academic Editor: Al-Sakib K. Pathan

Network congestion is a key challenge in resource-constrained networks, particularly those with limited bandwidth to accommodate high-volume data transmission, which causes unfavorable quality of service, including effects such as packet loss and low throughput. This challenge is crucial in wireless sensor networks (WSNs) with restrictions and constraints, including limited computing power, memory, and transmission due to self-contained batteries, which limit sensor node lifetime. Determining a path to avoid congested routes can prolong the network. Thus, we present a path determination architecture for WSNs that takes congestion into account. The architecture is divided into 3 stages, excluding the final criteria for path determination: (1) initial path construction in a top-down hierarchical structure, (2) path derivation with energy-aware assisted routing, and (3) congestion prediction using exponential smoothing. With several factors, such as hop count, remaining energy, buffer occupancy, and forwarding rate, we apply fuzzy logic systems to determine proper weights among those factors in addition to optimizing the weight over the membership functions using a bat algorithm. The simulation results indicate the superior performance of the proposed method in terms of high throughput, low packet loss, balancing the overall energy consumption, and prolonging the network lifetime compared to state-of-the-art protocols.

EXAMPLE: RESEARCH (VI)

6. IoT/ 5G/ UAV Security

IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING, VOL. 9, NO. 2, APRIL 2023

Outage Probability Minimization in Sec Cognitive Radio Systems With UAV A Machine Learning Approac

Van Nhan Vo, Le-Mai-Duyen Nguyen, Hung Tran, Viet-Hung Dang, Dusit Niyato, *Fellow, IEEE*, Dang Ngoc Cuong, Nguyen Cong Luong, and Chakchai So-In, *Senior Member, IEEE*

***Abstract*—This paper considers a multiple-input multiple-output (MIMO) non-orthogonal multiple access (NOMA) cognitive radio (CR) system with an unmanned aerial vehicle relay (UR). In this system, a secondary transmitter (ST) uses licensed spectrum from the primary network to transmit signals to its secondary receivers (SRs) based on NOMA. The UR is used as a relay to forward the signals from the ST to the SRs. As a result, the system can achieve significant improvements in spectral efficiency and network capacity. However, such a MIMO NOMA CR system faces issues of interference and security, i.e., eavesdropping attacks, due to the shared spectrum use and the UR. Therefore, we aim to minimize the outage probability of the secondary network, subject to constraints on the outage probabilities of the secondary and primary networks and the intercept probabilities at the eavesdroppers. We propose using a machine learning algorithm based on a constrained continuous genetic algorithm to solve the optimization problem.**

***Index Terms*—Cognitive radio, unmanned aerial vehicle, non-orthogonal multiple access, constrained continuous genetic algorithm, eavesdropping, machine learning.**

I. Introduction

COGNITIVE radio (CR) has recently been combined

Throughput Optimization for Noma Energy Harvesting Cognitive Radio With Multi-UAV-Assisted Relaying Under Security Constraints

Viet-Hung Dang, Le-Mai-Duyen Nguyen, Van Nhan Vo, Hung Tran, Tu Dac Ho, *Member, IEEE*, Chakchai So-In, *Senior Member, IEEE*, and Surasak Sanguanpong, *Member, IEEE*

***Abstract*—This paper investigates the throughput of a non-orthogonal multiple access (NOMA)-based cognitive radio (CR) system with multiple unmanned aerial vehicle (UAV)-assisted relays under system performance and security constraints. We propose a communication protocol that includes an energy harvesting (EH) phase and multiple communication phases. In the EH phase, the multiple UAV relays (URs) harvest energy from a power beacon. In the first communication phase, a secondary transmitter (ST) uses the collected energy to send confidential signals to the first UR using NOMA. Simultaneously, a ground base station communicates with a primary receiver (PR) under interference from the ST. In the subsequent communication phases, the next URs apply the decode-and-forward technique to transmit the signals. In the last communication phase, the Internet of Things destinations (IDs) receive their signals in the presence of an eavesdropper (EAV). Accordingly, the outage probability of the primary network, the throughput of the secondary network, and the leakage probability at the EAV are analyzed. On this basis, we propose a hybrid search method combining particle swarm optimization (PSO) and continuous genetic algorithm (CGA) to optimize the UR configurations and the NOMA power allocation to maximize the throughput of the secondary network under performance and security constraints.**

***Index Terms*—Cognitive radio (CR), non-orthogonal multiple access (NOMA), unmanned aerial vehicle (UAV), hybrid CGA-PSO, security constraints.**

I. Introduction

COGNITIVE radio (CR) is widely regarded as a potential solution for addressing the issue of spectrum scarcity, which has been exacerbated by the massive growth of wireless data traffic in fifth generation (5G) communication systems and beyond [1]. More specifically, Cognitive radio (CR) provides public access to underused spectral bands, allowing unlicensed (cognitive) users to exploit the licensed spectrum from an opportunistic standpoint and hence economically enhancing the overall spectral efficiency [2].

Furthermore, considering the requirements of 5G systems, especially spectral efficiency and massive-scale connectivity, non-orthogonal multiple access (NOMA) can be a complementary solution to the CR technique because it provides the

On Communication Performance in Energy Harvesting WSNs Under a Cooperative Jamming Attack

Van Nhan Vo, Hung Tran, Van-Lan Dao, Chakchai So-In, *Senior Member, IEEE*, Duc-Dung Tran, and Elisabeth Uhlemann, *Senior Member, IEEE*

***Abstract*—In this article, we consider the system performance of an energy harvesting (EH) wireless sensor network in terms of reliable communications when subjected to a cooperative jamming attack. A set of strategically located nodes acting as cluster heads (CHs) transfer energy to the wireless sensors within range, forming a cluster. The sensors use this energy to transmit data to the CHs, which, in turn, deliver the information to a base station (BS) using nonorthogonal multiple access. The BS processes the collected information and synchronizes the operation of all CHs. Furthermore, there exist two adversaries, namely, a jamming attacker and an eavesdropper, who cooperate to attack the considered system. To protect against this attack, the CHs should be controlled by suitable power allocation coefficients obtained from the security constraints of the CHs. Using these constraints, closed-form expressions are derived to find the power allocation coefficients that will enable reliable and secure communication. In addition, we propose an interference channel selection policy for the sensor-to-CHs links and CHs-to-BS links to improve the reliability of communication while enhancing energy utilization. Finally, an algorithm for finding the optimal EH time is also proposed.**

immediately report all events to a central monitoring or control unit [1]. WSNs have been proposed for various real-life applications, including natural environmental monitoring, fire detection, animal tracking, and health monitoring [2], [3].

Unfortunately, WSNs face crucial challenges due to the energy constraints imposed by the limited size and complexity of the sensors [4]. To address these challenges, several techniques for extending the sensor lifetime have been developed by the research community [5], [6]. For instance, Li *et al.* investigated a solution involving the configuration of a reasonable round time to prolong the lifetime of a cluster-based WSN [5]. Furthermore, Chincoli and Liotta proposed a transmission power control policy based on a reinforcement learning process to reduce energy consumption in WSNs [6].

However, the above works merely improve the sensors' energy consumption, and the sensor batteries still need to be periodically replaced or recharged to maintain operation [7].

Enhanced Intrusion Detection System for an EH IoT Architecture Using a Cooperative UAV Relay and Friendly UAV Jammer

Van Nhan Vo, Hung Tran, and Chakchai So-In, *Senior Member, IEEE*

***Abstract*—In this paper, the detection capabilities and system performance of an energy harvesting (EH) Internet of Things (IoT) architecture in the presence of an unmanned aerial vehicle (UAV) eavesdropper (UE) are investigated. The communication protocol is divided into two phases. In the first phase, a UAV relay (UR) cooperates with a friendly UAV jammer (UJ) to detect the UE, and the UR and UJ harvest energy from a power beacon (PB). In the second phase, a ground base station (GBS) sends a confidential signal to the UR using non-orthogonal multiple access (NOMA); the UR then uses its harvested energy to forward this confidential signal to IoT destinations (IDs) using the decode-and-forward (DF) technique. Simultaneously, the UJ uses its harvested energy to emit an artificial signal to combat the detected UE. A closed-form expression for the probability of detecting the UE (the detection probability, DP) is derived to analyze the detection performance. Furthermore, the intercept probability (IP) and throughput of the considered IoT architecture are determined. Accordingly, we identify the optimal altitudes for the UR and UJ to enhance the system and secrecy performance. Monte Carlo simulations are employed to verify our approach.**

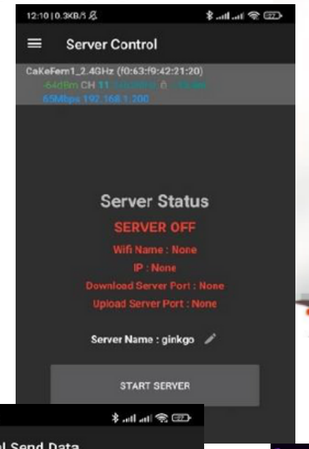
***Index Terms*—Detection probability (DP), energy harvesting (EH), friendly UAV jammer, Internet of Things (IoT), system performance, UAV detection.**

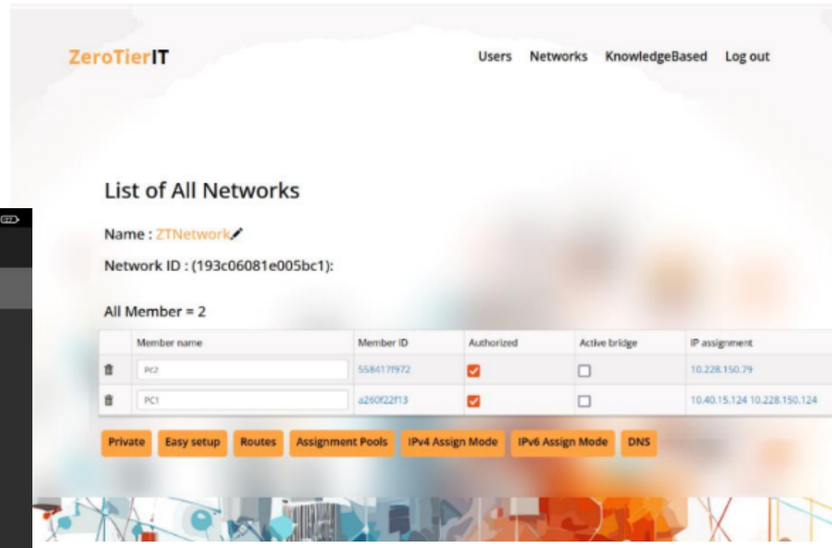
collecting and transmitting data for different purposes in various application scenarios (e.g., smart cities, smart factories, and smart agriculture) [1]–[3]. In parallel with the IoT revolution, unmanned aerial vehicles (UAVs) are considered promising solutions for numerous applications, such as aerial monitoring, photography, precision agriculture, traffic control, telecommunications, and especially search and rescue [4]. Low-altitude UAVs, in particular, have attracted a massive amount of research attention in the context of safe and secure communications due to their mobility, elevated positions, and relatively low cost, which make them an easy and inexpensive way to access a variety of areas for surveillance [5], [6].

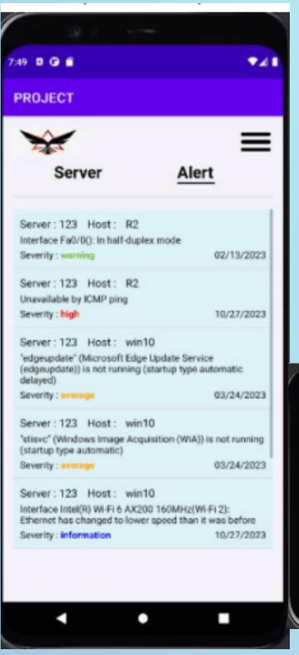
Accordingly, UAVs can contribute to overcoming the limitations of the terrestrial infrastructure of an IoT system. Specifically, the incorporation of UAVs into an IoT system can allow such a system to bypass obstacles that may block direct communication between a transmitter and a receiver (e.g., forests, mountains, or high buildings) [7]–[9]. For example, Motlagh *et al.* discussed the potential uses of UAVs

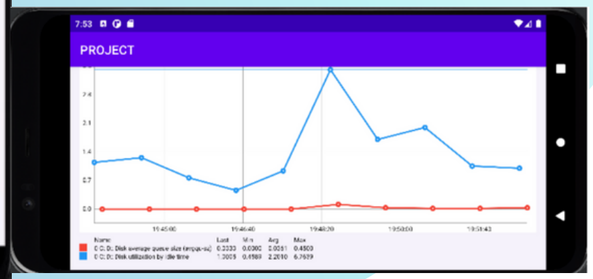
OUR PROJECT: EXAMPLES

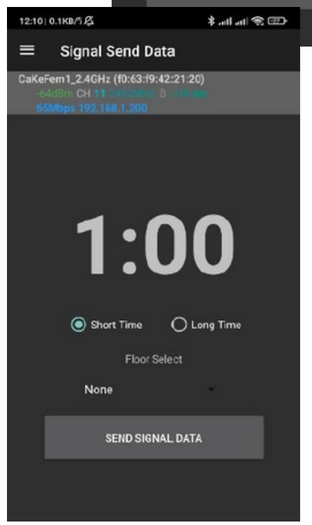
1. Network: Mobile Zabix: Network monitoring systems
2. Network: Wi-Fi signal and throughput analysis systems
3. Network: Internet authentication box with load balance and traffic logging systems
4. Security: Private VPNs

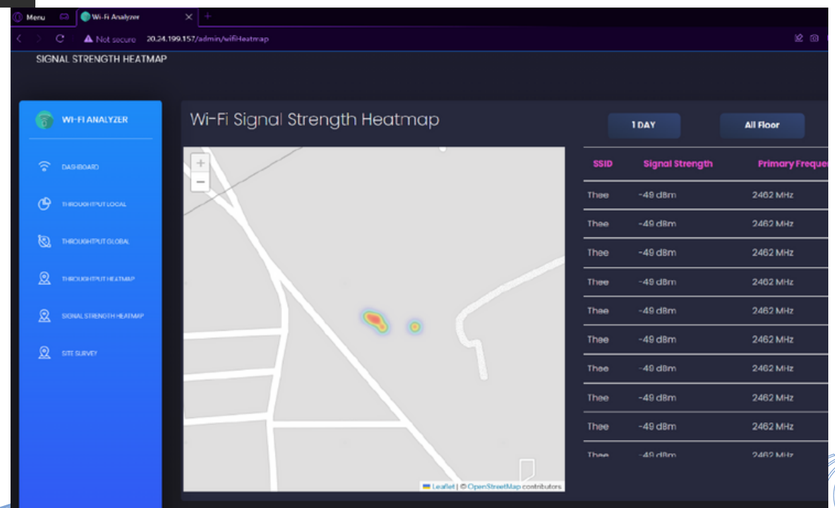








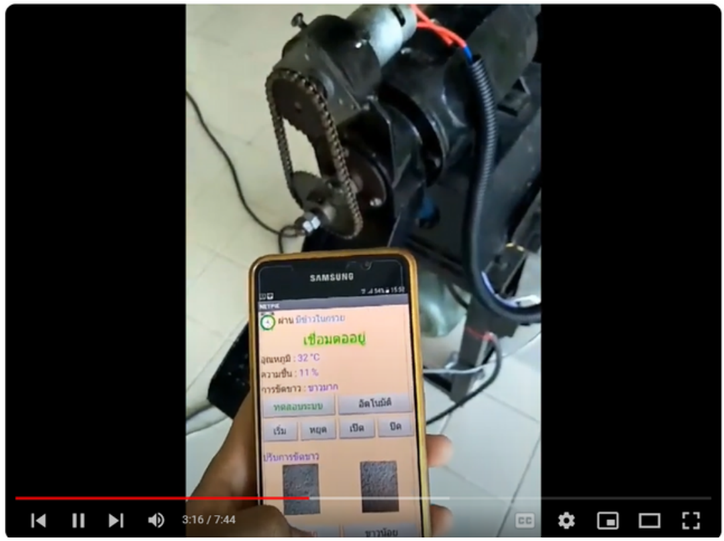


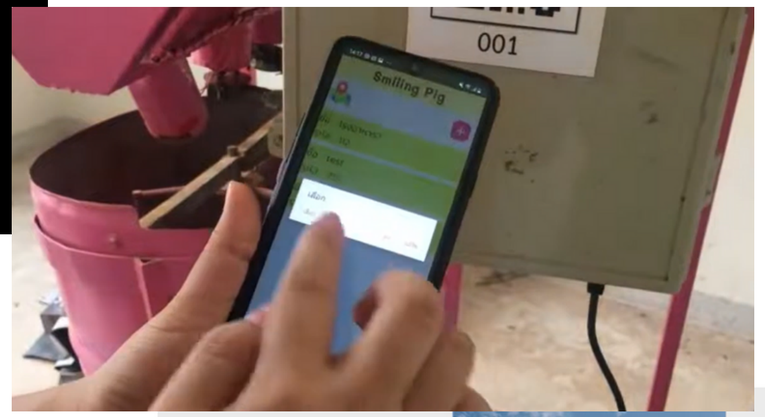


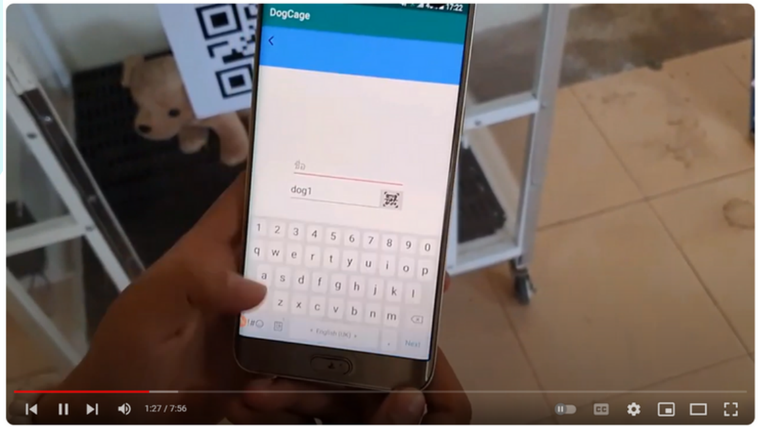
OUR PROJECT: EXAMPLES (CONT.)

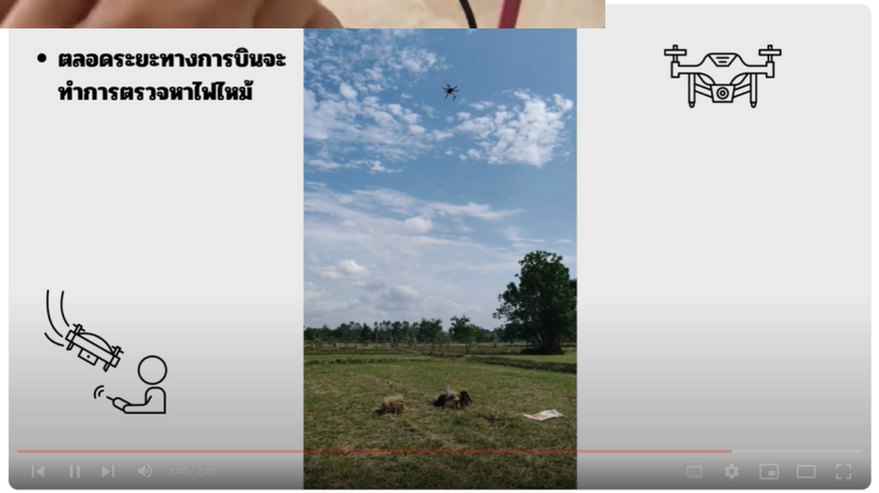
1. IoT = Rice Milling Machine
2. IoT = Moth Extractor
3. IoT = Food Mixer
4. IoT = Pet Cage for Vet Clinic
5. AI-IoT = Fire Detection using Drone

https://www.youtube.com/playlist?list=PLtfsF7Gq35lmkjz7mYApQcMWKRoGLCED3









OUR CURRENT INTEREST

Theme = AI in Network Computing

AI in Mobile/Wireless/Cellular Technology: Research and develop applications and improvements of AI efficiency in communication and computing. wireless and mobile networks; the Internet of Things; the automotive network; wireless sensor networks; unmanned communications; mobile and agent technologies; wireless local area networks; wireless personal area networks; wireless wide area networks; urban wireless networks including cellular such as 4G/5G; satellite and interplanetary wireless networks; ad hoc networks and peer-to-peer technologies; etc.

AI in Networking: Study and develop AI and computer networks to increase the efficiency of data transmission in the future; a network that supports the transmission of multimedia data such as data, images, audio, and video; high-speed communication; internet routing architecture; network management and surveillance; network data analysis and modeling, etc.

AI in Security: Research AI in support of high-speed network optimization to be reliable and reliable; Network data analysis for surveillance or prevention of various forms of attack (both intelligent detection and defense systems); a firewall; security on small devices; social networks; online transactions; network data conversion; different forms of encryption and attack analysis, etc.

AI in the Cloud: Research applying AI to parallel and high-performance computing: grid computing; versioning techniques; working with distributed systems; use of cloud services; parallel processing, etc.

Smart Technology: Adding intelligence to devices, computing, communications, or other technologies agriculture, agriculture, industry, automotive, medical, military, health care, various forms of service business, and so on

PARTNERSHIP/COLLABORATION

Open!

1. Visiting Profs.
2. Postdoc
3. Ph.D. candidate
4. Master candidate
5. Intern - any levels
6. Collaborative Work!

THANK YOU

HTTPS://SITES.GOOGLE.COM/VIEW/ANTLABKKU/HOME