

3.4.5

Department: Computer Science & Engineering
Research papers per teacher in the
Journals notified on UGC website

Supporting Documents



Having an EAGLE-eye on GENI

Shifali*, Monika Sachdeva** and Sunny Behal***

ABSTRACT

Experimentation with new network architecture and protocols is one of the idiopathic stimuli for piling future internet test bed such as GENI (Global Environment for Network Innovations) test bed. GENI proffer a virtual laboratory for networking and distributed system scrutiny and breeding. The motive of this test bed is to nurture the experimentation with succeeding protocols, services and network architecture instead to frame succeeding Internet. As a cause of reconnaissance of network, GENI foster innovations in network security, science, applications and services. In this paper, we have an eagle eye on GENI by scrutinizing its Resource Reservation Tool - Jack and Instrumentation and Measurement Tool-GENI Desktop. As part of the work, GENI has been used to synthetically generate different kinds of network traffic datasets like legitimate traffic, high rate DDoS attack and Flash Events(FE) traffic.

Keywords: Validation Techniques, GENI, GENI-Desktop, Workflow of GENI.

1. INTRODUCTION

In the Recent time, the collegial, public & self-sufficing facility tabbed to be Internet which is handy for hundreds of millions of people worldwide has spread its wings globally. However the intrinsic frangibility of Internet provides opportunities to attackers. Distributed Denial of Service (DDOS) impersonates slang threat to the availability of Internet. DDOS attacks encompass the stiff security problems in today's Internet. With meager or no advance warning, a DDOS attack can easily cripple the resources of its mark within a precise cycle of time. There are various network research validation techniques for analyzing these attacks like Mathematical Models, Simulation, Emulation and Real time experiment. By the whole of these, GENI is tremendously used in network related research based on real time experiments. In GENI, the experiment is not stipulate by system, but is licensed by the experimenter.

• MOTIVATION:

The idea for using GENI test bed is motivated from [1], since number of researcher has used the publicly available datasets for validating their proposed approaches. However most of these available datasets are obsolete. So there is need to generate realistic datasets. Based on this, we have synthetically generated our own datasets in GENI test bed.

• CONTRIBUTIONS:

The major contribution of this paper is:

- (1) Distinct research validation techniques are given along with the brief introduction of GENI test bed.

* Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India, Email: shifalichawla91@yahoo.in

** Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India, Email: monika.sal@rediffmail.com

*** Department of Computer and Science Engineering SBS State Technical Campus, Ferozepur, Punjab, India, Email: sunnybehal@rediffmail.com

34/12

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Energy Efficient Task Scheduling Mechanism in Cloud Computing

*Prabhpreet Kaur **Monika Sachdeva

Abstract : From last few years' Cloud computing has become more and more popular. This increase in popularity of cloud services results in higher resource demands on the provider ends. To fulfill the consumers requirements for cloud hardware, software, platform etc, large number of datacenters is constructed that utilize a huge bulk of datacenters energy and produces carbon dioxide emissions which are very harmful for the environment. Power conservation is one of the major concern in Cloud computing. In this research we are focusing on the concept of task scheduling mechanism in cloud computing. The main objective is to reduce total consumption of energy in datacenters. This research presents a new approach of Energy productive scheduling of tasks to reduce the wastage of power in datacenters so that resources can be properly used. The cloudlets submitted to the cloud provider are executed in an energy efficient DVFS approach.

Keywords : Cloud Computing, DVS, Green Computing, VM, Host.

1. INTRODUCTION

Cloud computing refers to the computing that is based on Internet and contributes a variety of resources, data and applications according to the requirement and demand of consumers. It reduces the burden of IT companies as there is no need to purchase hardware, software and thereby maximizing their profits. Resources of cloud are utilized globally, thus help in reducing the unnecessary wastage of resources and save the cost. Cloud services can be used from anyplace and from any device only through internet connection. Cloud services are metered services i.e. consumers are charged according to their usage [1].

Users attracted towards the cloud technology are increasing day by day and their demands for cloud resources are also increasing and to meet the increasing demands of cloud users; there is need to construct large number of datacenters. These datacenters produces huge bulk of heat. As a result, there is increase in the power consumption of IT companies. Nearly 38 GW power was consumed in the year 2012 by datacenters. This power consumption was near about 63% increased than in year 2011 [2]. Likely, for UK families this power would have been sufficient to meet their requirements of energy [3].

If the power consumption is more, bills will also be high. Today, power consumption of datacenters is serious problem as it not only decreases the profit of providers also causes harmful effect on the surroundings. Green Cloud computing is becoming popular to decrease the power consumption, increases the profits of providers and reduces the impact on environment [4]. The main goals of green cloud computing are development of computer systems and applications that have cost-effectiveness and reduced power consumption [5]. One way to achieve green computing is by using Dynamic voltage scaling i.e. DVS. DVS helps in reducing the power consumption of datacenters by reducing the voltage supply and frequency.

There are some following research works that have given many ways to solve the problem of power consumption of datacenters and carbon dioxide emissions. Wissam Chedid et.al in [6] explains two techniques for managing power, one is static that is applied at the time of design and second is dynamic that is applied at the run time and their main objective is to reduce the power consumed by systems. DVS is used in dynamic technique to save power at CPU level. Abhishek Patil and Sunny Behal in [7] attempts to secure data by using RSA algorithm from unauthorized access. Data security is provided by encrypting the given data based on Key combinations which can only be decrypted by authorized person by making use of his private key. Mohammad A. Haque et.al in [8] proposed a technique in which two processors are used i.e. primary and spare. Primary processor execute tasks

Research Scholar, Department of Computer Science Engineering, SBSSTC, Ferozepur sandhuprabh36@yahoo.com, Associate Professor, Department of Computer Science Engineering, SBSSTC, Ferozepur monika.sal@rediffmail.com

35/12

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Document details - A Grouping based Scheduling Algorithm on Load Balancing in Cloud Computing

1 of 1

[Export](#) [Download](#) [More...](#)

International Journal of Control Theory and Applications

Volume 9, Issue 22, 2016, Pages 293-299

Cited by 0 documents

Inform me when this document is cited in Scopus:

[Set citation alert >](#)[Set citation feed >](#)

A Grouping based Scheduling Algorithm on Load Balancing in Cloud Computing(Article)

Kaur, P., Sachdeva, M.

Department of Computer Science Engineering, SBSSTC, Ferozepur, India

Abstract

Cloud Computing is the web based processing where the data, application and infrastructure are provided to computers and other devices on demand over the network. A load balancing is process of distribution of the proper load among different resources load balancing aim to optimize resources, and avoid overload and under load of resources. We proposed a grouping based scheduling algorithm in which load is assign to virtual machine according to instruction size of given cloudlet to avoid the underutilization and improve the response time, data transfer cost and waiting time. © International Science Press.

SciVal Topic Prominence

Topic: Task Scheduling | Scientific Workflow | Execution Costs

Prominence percentile: 98.538

①

Author keywords

[Cloud computing](#) [Datacenter](#) [Datacenter broker](#) [Host](#) [Load balancing](#) [Virtual machine](#)

Related documents

Find more related documents in Scopus based on:

[Authors >](#) [Keywords >](#)

ISSN: 09745572

Source Type: Journal

Original language: English

Document Type: Article

Publisher: Serials Publications

© Copyright 2016 Elsevier B.V., All rights reserved.

About Scopus

[What is Scopus](#)[Content coverage](#)[Scopus blog](#)[Scopus API](#)[Privacy matters](#)

Language

[日本語に切り替える](#)[切换到简体中文](#)[切换到繁體中文](#)[Русский язык](#)

Customer Service

[Help](#)[Contact us](#)

ELSEVIER

[Terms and conditions >](#) [Privacy policy >](#)

Copyright © Elsevier B.V., All rights reserved. Scopus® is a registered trademark of Elsevier B.V.

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Nature Inspired Feature Selection Approach for Effective Intrusion Detection

Rajinder Kaur¹, Monika Sachdeva¹ and Gulshan Kumar²

¹Department of Computer Science Engineering, Shaheed Bhagat Singh State, Technical Campus, Ferozepur, India; khalsarajkaur@gmail.com, monasach1975@gmail.com

²Department of Computer Applications, Shaheed Bhagat Singh State, Technical Campus, Ferozepur, India; gulshanahuja@gmail.com

Abstract

Objectives: To reduce the dimensionality of network traffic dataset by selecting the relevant and irredundant features for accurate and quick intrusion detection. To achieve the target, we proposed a new feature selection approach based on the nature. **Methods/Statistical Analysis:** The proposed Modified Cuttlefish Algorithm (MCFA) approach plays a crucial role in intrusion detection by selecting appropriate subset of most relevant features from huge amount of dataset. Griewank fitness function is used to calculate the fitness of the modified cuttlefish algorithm. Naive bayes classifier is employed at the generated subset of features from benchmark KDD 99 dataset in WEKA data mining tool. Compare the results of proposed approach with the existing approaches of WEKA and Improved Cuttlefish Algorithm (ICFA) with different performance metrics. **Findings:** As per the outcomes are obtained by the WEKA Experimenter with the 9 feature selection approaches on KDD 99 10% training dataset, it has been observed that the Consistency Subset feature selection approach with Greedy stepwise search method gives higher accurate results than other approaches and from the literature survey has been found that the ICFA performs well, but still there is problem of low True positive (TP) rate and False negative (FN) rate. These problems are addressed by the proposed feature selection approach which outperforms best from others in accuracy rate (91.79%), True positive rate (0.947), false positive rate (0.025) and ROC area (0.9982) with the minimum amount of time at 19 relevant subset of features instead of 41 features. As the consequence, the proposed approach is novel from existing approaches to increase the intrusion detection rate and discard the redundant and irrelevant subset of features. **Application/Improvements:** MCFA has improved intrusion detection rate by increasing the TP rate and decreasing the FP rate, so MCFA can be used for the real time applications of intrusion detection system.

Keywords: Accuracy, Dimensionality, Feature Selection Approach, FP Rate, Intrusion Detection, Modified Cuttlefish Algorithm, TP Rate

1. Introduction

According to the popularity and fast growth of internet, the possibility of network attacks has been increased significantly in recent years. Therefore, to provide more secure information channels much attention has been needed. Distinguish the attack action from the normal network action, is not a simple process. This problem is overcome with the proposed concept of Intrusion Detection in 1980¹. Intrusion Detection System (IDS) provides a defense mechanism in computer networks against

the various attacks and criminal activities. Intrusions are a set of activities and actions that are made an attempt to compromise the security objectives like integrity, comprehensibility and availability of the information resources². The main role of IDS is to recognize the unusual access, attacks and activities to make sure the more protection in the network channels. When any potential attack is detected in network traffic, an alarm is triggered and taking an appropriate action against the attacks by IDS. During the building of IDS many challenges are needed to consider such as collection of data, data processing,

*Author for correspondence

37/121

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



Original research article

A survey on LEACH and other's routing protocols in wireless sensor network

Vishal Kumar Arora (Research Scholar)^a, Vishal Sharma^{b,*}, Monika Sachdeva^a^a Department of Computer Science & Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab 152004, India^b Department of Electronics & Communication Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab 152004, India

ARTICLE INFO

Article history:

Received 17 February 2016

Accepted 13 April 2016

Keywords:

Clustering

LEACH protocol

Network routing

Energy

Wireless sensor network

ABSTRACT

An extensive range of applications of Wireless Sensor Networks such as military, environment, surveillance, home, vehicle tracking/detection, traffic flow and medical make it hot-spot in the epoch of wireless networks. A WSN consisting of numerous sensor-nodes is equipped with inadequate energy, memory, and computation capability issues. Further, such networks are limited to reinstate the dead nodes caused by energy's depletion and to maximize the life-span of the system. To achieve this aim, several routing algorithms are proposed and investigated. In this work, an attempt is carried out to assess the diverse hierarchical routing protocols, developed from LEACH and is extended to other presented routing protocols like TEEN, APTEEN, and PEGASIS. Depending upon the observations and scrupulous consideration, a relative conclusion is drawn in the last.

© 2016 Elsevier GmbH. All rights reserved.

1. Introduction

Wireless Sensor Network (WSN) is a collection of large number of small size and moderately inexpensive computational nodes that forward the valuable information to a central point for appropriate processing. The environment can be an information technology framework, a biological system or a physical work. There are four parts of sensor network: (i) sensors (ii) network connecting different sensors (iii) centralized information gathering store (iv) resources performing computation which include data mining, data correlation etc. [1–3]. Sensors nodes make an ad hoc network that are useful to monitoring temperature, pressure, humidity, military surveillance, disaster management, forest fire-tracking and many more [4]. Routing in WSN is different from other wireless network due to sensor node have constraints of energy, processing activities, transmitting collected data from multiple nodes to a single sink, unique global address is not possible due to random deployment of nodes etc. Due to all of these reasons, different types of routing protocols were developed for such scenarios. All these routing protocols had considered all those inherited features of WSNs. Main aim of these protocols were to reduce power consumptions and increasing network life time. This can be achieved by implementing routing protocols that consume minimum energy, choose path between sensor nodes and base station in such manner that increase network life time. Basically, WSN routing protocols are classified into four main categories: Network structure, communication models, topology based and reliable routing schemes [5]. Network structure protocols, basically, rely upon the architecture

* Corresponding author.

E-mail addresses: vishal.fer@gmail.com (V.K. Arora (Research Scholar)), et.vishusharma@yahoo.com, 78vishusharma@gmail.com (V. Sharma), monika.sad@rediffmail.com (M. Sachdeva).<http://dx.doi.org/10.1016/j.ijleo.2016.04.041>

0030-4026/© 2016 Elsevier GmbH. All rights reserved.

38/121

y PL

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



Characterizing DDoS attacks and flash events: Review, research gaps and future directions

Sunny Behal^{a,*}, Krishan Kumar^b, Monika Sachdeva^a

^a I.K.G. Punjab Technical University, Kapurthala, Punjab, India

^b U.I.E.T., Panjab University, Chandigarh, India

ARTICLE INFO

Article history:

Received 8 May 2017

Received in revised form 4 July 2017

Accepted 25 July 2017

Available online 10 August 2017

Keywords:

DDoS

Detection

Flash events

Network security

Review

ABSTRACT

A Distributed Denial of Service (DDoS) attack is an austere menace to network security. Nowadays in a technological era, DDoS attacks pose a severe threat to widely used Internet-based services and applications. Disruption of these services even for a fraction of time lead to huge financial losses. A Flash event (FE) is similar to a DDoS attack wherein a large number of legitimate users starts accessing a particular service concurrently leading to the denial of service. Both of these events cause overloading of network resources such as bandwidth, CPU, Memory to legitimate users and result in limited accessibility. Nowadays most of the DDoS attacks use the logical semantics of HTTP protocol to launch a similar kind of attack traffic as that of legitimate traffic which makes the distinction between the two very challenging. Many researchers have tried to discriminate these two types of traffic, but none of them has been able to provide any effective solution yet. This paper systematically reviews 40 such prominent research papers from 2002 to till date for providing insight into the problem of discriminating DDoS and FEs. This article downies and deliberates the list of traffic feature rationales and detection metrics used by the fellow researchers at both macro and micro level. Such a pragmatic list of rationales would surely be helpful to provide more robust and efficient solutions. The paper also highlights open issues, research challenges and future directions in this area.

© 2017 Elsevier Inc. All rights reserved.

Contents

1. Introduction.....	101
2. Flash events.....	103
2.1. Classification of flash events.....	104
2.2. Examples of popular Flash events.....	106
3. Review of DDoS attacks and Flash events.....	106
3.1. Based on information entropy.....	107
3.2. Based on information divergence.....	108
3.3. Based on correlation coefficient.....	110
3.4. Other methods.....	111
4. Key rationales to discriminate DDoS attacks from FEs.....	111
5. Research gaps and future directions.....	111
5.1. Research gaps.....	112
5.2. Conclusion and future directions.....	113
References.....	113

1. Introduction

In the present computer era, though the Internet-based applications and web services are the driving force of social evolution,

yet its architectural vulnerabilities proffer plethora leisure to the attackers for conquering diversity of attacks on its services. A DDoS attack is one of such prominent attack that constitutes a lethal threat to the Internet domain that harnesses its computing and communication resources. DDoS attacks deny the services of a web server by sending a huge amount of useless traffic towards critical

* Corresponding author.
E-mail address: sunnybehalsbs@gmail.com (S. Behal).

39/121

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Load Balanced and Link Break Prediction Routing Protocol for Mobile Ad Hoc Networks

Mandeep Kaur Gulati¹, Monika Sachdeva², and Krishan Kumar³

¹Deptt. of Computer Science, KCW ASR, PTU Kapurthala, Punjab, India

²Deptt. of Computer Science and Engineering, IKG Punjab Technical University, Kapurthala, Punjab, India

³Deptt. of Information Technology, University Institute of Engineering and Technology, Panjab University, Chandigarh

Email: gulati_mandeep@rediffmail.com, {monasach1975, k.salujasbs}@gmail.com

Abstract—A Mobile Ad-hoc Network (MANET) is an infrastructure less and decentralized network which needs a robust routing protocol. With the development of the MANET applications, more importance is given to Quality of Service (QoS) routing strategy. However congestion and mobility of the nodes lead to frequent link failures and packet losses affecting the QoS performance of the protocol. We consider these issues and propose a Load balanced and Link Break Prediction Routing Protocol (LBALBP) for Mobile Ad hoc Networks. The protocol finds least loaded path based on path count metric. Link break prediction mechanism is also integrated in the route maintenance phase of the protocol. Based on the signal strength of the packets received from the neighbour, the node calculates the link break prediction time of the link and if the link is found to be broken soon, an alternate path is found before the link actually breaks. Simulation results show that the proposed protocol outperforms AODV in terms of packet delivery ratio, delay, throughput and no. of link breakages but at the cost of high routing overhead.

Index Terms—mobile ad hoc network, quality of service, stability, load balance, Load Balanced and Link Break Prediction Routing Protocol (LBALBP), cross layer weight based on demand routing protocol, stable energy efficient qos based congestion and delay aware routing protocol

I. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a collection of mobile nodes that form a dynamic infrastructure-less communication network wherever it is required. The nodes in the network not only act as hosts but also as routers that discover and maintain routes to other nodes in the network. Therefore, finding and maintaining routes in MANET is a complicated task. Researchers proposed several routing algorithms for mobile ad hoc networks like AODV [1], DSR [2], DSDV [3], WRP [4] etc. However these protocols concentrate mainly on establishing shortest path without any attempt to provide QoS requirements. But such a selected path may not always be the best path for real-time audio and video applications which are sensitive to the Quality of Service (QoS). These applications require the underlying network to provide certain guarantees that are manifested in the

support of several important QoS parameters such as throughput, delay, jitter, packet delivery ratio, link stability, node buffer space, packet loss ratio etc. [5]. However, achieving QoS guarantees in MANETs is a challenging task due to dynamic topology, limited bandwidth and power, variable capacity, error-prone and insecure wireless channels.

The key factor which makes it difficult to develop QoS routing in ad hoc networks is congestion caused due to limited resources such as bandwidth, buffer space, battery power and memory etc. In min-hop routing protocols, nodes on the shortest path will be more heavily loaded than others since they are frequently chosen as the routing path. With the unbalanced traffic distribution, the heavily loaded nodes can exhaust their power resulting in node failures. With more failure of nodes, the connectivity of the network is reduced leading to network partitions. Furthermore, congested nodes can lead to packet loss and buffer overflow, resulting in longer end-to-end delay, degradation in throughput, and loss of transport connections. Hence, it is important for a routing protocol to have some form of load balancing so that traffic is uniformly distributed among various nodes. Load balancing can minimize traffic congestion and end to end delay, maximize node lifetime and can balance network energy consumption. Thus load balancing is emerging as a key tool to better use MANET resources and improve MANET performance. Another major problem in MANETs is the link breakage occurring due to the dynamic network topology and arbitrary movement of the nodes. This leads to the network partitioning and degradation of performance. When the route breaks, the routing protocols try to recover the connection either by repairing the route locally around the breakage or globally by informing the source node which then starts a completely new route discovery process. This kind of action taken after the route is already broken leads to increase in packet loss and the route rediscoveries. This can be avoided if the route maintenance phase of the protocol includes the link breakage prediction mechanism that predicts the link failure before its real occurring.

In this paper, we have considered these issues and proposed a Load balanced and Link Break Prediction (LBALBP) Routing Protocol for Mobile Ad hoc

Manuscript received January 2, 2017; revised June 20, 2017.
doi:10.12720/jcm.12.6.353-363

40/121

Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Discriminating Flash Events from DDoS Attacks: A Comprehensive Review

Sunny Behal¹, Krishan Kumar², Monika Sachdeva¹

(Corresponding author: Sunny Behal)

I. K. Gujral Punjab Technical University¹

Kapurthala, Punjab 144603, India

(Email: sunnybehal@sbstc.ac.in)

Information Technology Department, University Institute of Engineering and Technology²

Chandigarh, India

(Received June 23, 2016; revised and accepted Sept. 3 & Nov. 15, 2016)

Abstract

Millions of people across the globe access Internet-based applications and web services in their day to day activities. Distributed Denial of Service (DDoS) attack is one of the prominent attacks that cripple down the computing and communication resources of a web server hosting these services and applications. The situation turns further crucial when DDoS attacks are launch during similar looking legitimate traffic called a flash event (FE). Both DDoS attacks and FEs causes a sudden surge in the network traffic leading to delay in the responses from the web server. It often leads to massive financial losses, and thus, require timely actions. This paper presents a comprehensive review that broadly discusses the DDoS and FE problem, and recapitulates the recently published strategies in this field. As part of the work, a pragmatic list of rationales to discriminate the two has been proposed. This list can help the researcher community for better understanding the problem and can provide more effective solutions to the ongoing problem of discriminating DDoS attacks from FEs.

Keywords: DDoS Attack; Discrimination; Flash Event.

1 Introduction

A DDoS attack deploys the collection of compromised hosts and results in unavailability of network resources for the intended users. Not directly or permanently damaging the data, but intentionally compromising the availability of the resources is the motive of these attacks [24]. However, the attackers keep on strengthening their proficiency for launching sophisticated DDoS attacks by compromising the freely available credulous hosts. Differentiating DDoS attacks from legitimate traffic is an immense chal-

lenge to the network security researchers since the attackers strike with more suave techniques to the victim every time. Almost all types of DDoS attacks are launched using botnets nowadays [13]. The prominent websites are the prime victims of such DDoS attacks. Recently Twitter, Spotify, and Amazon suffer interruptions in their services for almost two hours on Oct 21, 2016, because of DDoS attacks. Such interruptions in the services lead to huge financial losses. The revenue loss has amplified to \$209 million in the first quarter of 2016, compared to \$24 million for all of 2015 [8]. According to the recent Worldwide Infrastructure Security Report (WISR), the traffic volume of such attacks has amplified to around 600 Gbps in the year 2015 [14].

Apart from detecting of DDoS attacks, there is an another kind of network traffic which is gaining popularity among security researchers, and which causes a denial of service to legitimate users of a web service, is a Flash Event (FE). As per [4], an FE is similar to high-rate DDoS (HR-DDoS) attack wherein thousands of legitimate users try to access a particular computing resource such as a website simultaneously. This sudden surge in legitimate traffic is mainly due to some breaking news happening around the world like the publishing of Olympic schedule or new product launch by companies like Apple, Samsung, etc. It causes the untimely delivery of responses from web service and thus, require immediate action. As there are only a few parametric differences between DDoS attacks and FE traffic, it is very challenging to discriminate the two [6]. The typical network traffic profile of a DDoS attack and an FE is shown in Figure 1(a) and Figure 1(b) respectively.

In this paper, we have presented a comprehensive review of the recent solutions proposed by the fellow researchers to discriminate DDoS attacks from similar looking FEs. We have compared the existing work on a set of

4/12

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/324124027>

D-FAC: A novel ϕ -Divergence based distributed DDoS defense system

Article in *Journal of King Saud University* · March 2018
DOI: 10.1016/j.jksus.2018.03.025

CITATIONS
0

READS
65

3 authors:



Surin Behal
Shaheed Bhagat Singh State Technical Campus
54 PUBLICATIONS 163 CITATIONS

[SEE PROFILE](#)



Krishan Kumar Saluja
University Institute of Engineering & Technology, Panjab Universit...
110 PUBLICATIONS 636 CITATIONS

[SEE PROFILE](#)



Monika Sachdeva
Shaheed Bhagat Singh State Technical Campus
35 PUBLICATIONS 243 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



D-FAC Defense View project



DDoS Defense View project

All content following this page was uploaded by Surin Behal on 06 April 2018.
The user has requested enhancement of the downloaded file.

42/121

4 PS
HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



D-FACE: An anomaly based distributed approach for early detection of DDoS attacks and flash events

Sunny Behal^{a,*}, Krishan Kumar^b, Monika Sachdeva^c

^a I.K.G. Punjab Technical University, Kapurthala, Punjab, India

^b Department of IT, U.I.E.T., Panjab University, India

^c Department of CSE, I.K.G. Punjab Technical University, Kapurthala, Punjab, India

ARTICLE INFO

Keywords:
Network security
DDoS attacks
Flash events
Entropy
Information distance

ABSTRACT

In the present computer era, though the Internet-based applications are the driving force of social evolution, yet its architectural vulnerabilities proffer plethora of leisure to the attackers for conquering diversity of attacks on its services. Distributed Denial of Service (DDoS) is one of such prominent attack that constitutes a lethal threat to Internet domain that harnesses its computing and communication resources. Despite the presence of enormous defense solutions, ensuring the security and availability of data, resources, and services to end users remains an ongoing research challenge. In addition, the increase in network traffic rates of legitimate traffic and flow similarity of attack traffic with legitimate traffic has further made DDoS problem more crucial. The current research has deployed DDoS defense solutions primarily at the victim-end because of the inherent advantages of easy deployment and availability of complete attack information. However, the huge network traffic volume generated by DDoS attacks and lack of sufficient computational resources at the victim-end makes defense solution itself vulnerable to these attacks. This paper proposes an ISP level distributed, flexible, automated, and collaborative (D-FACE) defense system which not only distributes the computational and storage complexity to the nearest point of presence (PoPs) routers but also leads to an early detection of DDoS attacks and flash events (FEs). The results show that D-FACE defense system outperformed the existing Entropy-based systems on various defense system evaluation metrics.

1. Introduction

Over the past decade, advancements in information and communication technology have significantly transformed the way in which information is accessed and communicated, particularly via the Internet. Thousands of organizations such as payment gateways, domain name servers, search engines (e.g. Google, Yahoo), banks, educational institutes, commercial servers (e.g. Flipkart, eBay, Amazon), social websites (e.g. Twitter, Facebook), stock trades, weather forecasting, etc. have deployed web servers to provide Internet-based services and applications to the end users. The increasing usage of these interactive Internet applications has induced an exponential rise in risks and possibilities of misuse of Internet. Out of these, DDoS attacks pose a very critical threat to network security in general. Usually prominent websites are the victim of these DDoS attacks. Recently Twitter, Spotify, and Amazon suffer interruptions in their services for almost two hours on Oct 21, 2016 because of DDoS attacks (DDoS, 2016). Such interruptions in

the services lead to huge financial losses. As per SCMedia (2016), high-rate DDoS attacks (HR-DDoS) are predominant nowadays, having traffic volume more than 1 Tbps. So, it is crucial to detect such attacks in time to ensure the timely delivery of the widely used Internet-based services and applications. HR-DDoS attacks are often amalgamated with several low-rate DDoS (LR-DDoS) attacks which follow the same distributed nature as of HR-DDoS attacks but having low traffic rates (Shevtchik et al., 2005; Wang et al., 2012).

There is another kind of network traffic called a flash event (FE) that also cause a denial of service to these extensively used Internet-based services. An FE is similar to a HR-DDoS attack wherein thousands of legitimate users try to access a particular computing resource such as a website simultaneously (Bhandari et al., 2016). This sudden surge in legitimate traffic is mainly due to some breaking news happening around the world like the publishing of Olympic schedule or new product launch by top notch companies like Apple, Samsung, etc. It causes untimely delivery of responses from a web service similar to the case

* Corresponding author.
E-mail address: sunnybehal.abc@gmail.com (S. Behal).

<https://doi.org/10.1016/j.jnca.2018.03.024>

Received 3 September 2017; Received in revised form 22 January 2018; Accepted 20 March 2018
Available online 23 March 2018

1084-8045/© 2018 Elsevier Ltd. All rights reserved.

43/121

Handwritten initials: Y, PR

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

A generalized detection system to detect distributed denial of service attacks and flash events for information theory metrics

Sunny BEHAL*, Krishan KUMAR, Monika SACHDEVA

Department of Computer Science and Engineering, Inder Kumar Gujral Punjab Technical University, Punjab, India

Received: 28.06.2017

Accepted/Published Online: 03.04.2018

Final Version: 27.07.2018

Abstract: Distributed denial of service (DDoS) attacks pose a severe threat to extensively used web-based services and applications. Many detection approaches have been proposed in the literature, but ensuring the security and availability of data, resources, and services to end users remains an ongoing research challenge. Nowadays, the traffic volume of legitimate users has also increased manifold. A flash event (FE) is a high-rate legitimate traffic situation wherein millions of legitimate users start accessing a particular network resource, such as a web server, simultaneously. The detection of DDoS attacks becomes more challenging when DDoS attacks are launched during behaviorally similar FEs. This research paper proposes a generalized detection system for metrics, based on information theory, capable of detecting different types of DDoS attacks and FEs. We used publically available MIT Lincoln, CAIDA, and FIFA datasets along with a synthetically generated DDoSTB dataset to validate the proposed detection algorithm in terms of various detection system evaluation metrics such as false positive rate, false negative rate, classification rate, and detection accuracy. Such a generalized detection system would be useful to researchers for validating and comparing various information theory metrics based solutions.

Key words: DDoS attacks, network security, information theory, flash event, entropy, divergence

1. Introduction

Distributed denial of service (DDoS) attacks are not a new problem for network security professionals. They have existed for many years now. Legitimate users are deprived of using web-based services and applications due to such attacks. Even a few minutes of service downtime can lead to not only loss in revenue, but also intangibles such as loss of customer faith, unfavorable media coverage, and legal actions. Usually, prominent websites are the prime victims of such attacks. Recently, DDoS attacks caused interruptions in the services of Twitter, Spotify, and Amazon for almost two hours. Such interruptions in the services lead to huge financial losses. According to a recent report (<https://www.ddosattacks.net/twitter-amazon-other-top-websites-shut-in-cyber-attack/>), revenue losses due to DDoS attacks reached \$209 million in the first quarter of 2017, compared to \$24 million for all of 2015. Based on the network traffic rate, DDoS attacks can be categorized into (a) high-rate DDoS (HR-DDoS) attacks, when the traffic rate is very different from legitimate traffic, and (b) low-rate DDoS (LR-DDoS) attacks, when the traffic rate is similar or less than legitimate traffic. However, it is comparatively easy to detect HR-DDoS attacks, as their traffic profile significantly deviates from the legitimate traffic profile.

A flash event (FE), wherein millions of legitimate users try to access a particular computing resource

*Correspondence: sunnybehal.sbs@gmail.com

44/121

PR

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs^{*}

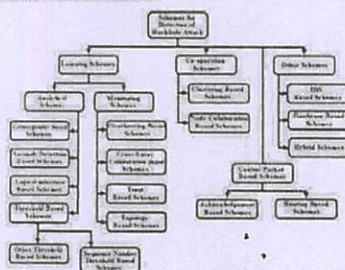
Nitin Khanna^{a,*}, Monika Sachdeva^b

^aDepartment of Computer Science, Kanya Maha Vidyalaya, Jaipur, India

^bDepartment of Computer Science & Engineering, IKGPTU, Kapurthala, India

GRAPHICAL ABSTRACT

In this paper, we present a comprehensive taxonomy on different categories of the mitigation and detection mechanism along with summarization and comparison of some published work related to these categories. They are in total sixteen different categories of mitigation mechanism and we have reviewed and summarized ninety one research works related to the presented categories on various parameters. Research gaps for future research are formulated. The logical taxonomy of blackhole attack and its variants is presented.



ARTICLE INFO

Article history:

Received 30 June 2018

Received in revised form 7 February 2019

Accepted 14 March 2019

Available online xxxx

Keywords:

MANET

Blackhole attack

Grayhole attack

Co-operative attack

Detection types

Trust based scheme

ABSTRACT

Mobile Ad hoc Network due to its intrinsic properties of mobility, infrastructure-less working and vulnerability of underlined standard routing protocols is exposed to various packet drop attacks such as blackhole attack, grayhole attack and co-operative blackhole attack. These attacking nodes participate actively in the route establishment process and when a path is established between two end nodes through these nodes, these nodes drop the data packets according to a pattern related to the type of attack. So, security of the network communication is a very critical issue and must be handled with greater efficiency and effectiveness. A lot of research has been carried out to detect and mitigate the effects of blackhole attack and its variants in MANET. In this paper, Different variants of blackhole attack are discussed along with shortcomings of present literature. We present a comprehensive taxonomy of the mitigation and detection mechanism along with summarization and comparison of some published work related to those categories. There are in total sixteen different categories of mitigation mechanism and we have reviewed and summarized ninety one research works related to the presented categories on various parameters like overhead, base protocol, modification in base routing protocol, detection type, nature, features and limitations.

© 2019 Elsevier Inc. All rights reserved.

Contents

1. Introduction.....	25
----------------------	----

^{*} No author associated with this paper has disclosed any potential or pertinent conflicts which may be perceived to have impending conflict with this work. For full disclosure statements refer to <https://doi.org/10.1016/j.cosrev.2019.03.001>.

^{*} Corresponding author.

E-mail addresses: nitinkhanna306@gmail.com (N. Khanna), monasach1975@gmail.com (M. Sachdeva).

<https://doi.org/10.1016/j.cosrev.2019.03.001>

1574-0137/© 2019 Elsevier Inc. All rights reserved.

45/12

2/

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

A Comprehensive Review of Mitigation Techniques for Blackhole Attack in AODV Routing Protocol in MANETs

Nitin Khanna¹ and Monika Sachdeva²

¹Department of Computer Science, Lyallpur Khalsa College, Jalandhar, India

²Department of Computer Science & Engineering, IKGPTU, Kapurthala India

¹nitinkhanna300@gmail.com, ²monasach1975@gmail.com

Abstract

Mobile Ad-hoc Network is a self-configuring network that has no infrastructure and communication happens in multi-hop fashion. This dynamic nature of MANET and lack of infrastructure makes it prone to many types of routing and security attacks. Ad-hoc On-demand Distance Vector is the most commonly preferred routing protocol in which route is formulated only when it is needed in a reactive manner. AODV is prone to a kind of packet drop attack called blackhole attack. In this paper, we have reviewed many existing solutions that are useful in mitigation of blackhole attack. These mechanisms are categorized as detection and prevention methodologies in the review. We have provided a detail on these mechanisms involving the concept of mechanism, simulation and result in brief and critically review them for their drawbacks and advantages along with their simulation and result highlights. A comparison is drawn and finally, the future research areas are identified on which the research should focus.

Keywords: Mobile Ad-hoc Networks, Blackhole Attack, Grayhole Attack, Ad-hoc On-demand Distance Vector Routing Protocol, Trust Algorithm

1. Introduction

Mobile Ad-hoc Network is a kind of self configuring network [1] which consists of many movable devices that communicates with each other to serve some purpose. These movable nodes communicate with each other in multi-hop [2] manner without any external or internal infrastructure. All the communication is done through wireless links that are formed by conforming to one of any routing protocol that all the mobile devices have implemented. MANET found its application in military operations, disaster management, and personal area network (PAN) [3] and many other applications where a fixed infrastructure cannot be established. The feature of infrastructure-less framework, multi-hop communication and dynamicity gives an added benefit of use of this network in scenarios where normal network cannot be established. The route establishment is done in MANET either reactively, pro-actively or through combination of both. For re-active path establishment, re-active route discovery protocols such as DSR [4], AODV [5], OLSR [6] etc are used in which routes are established only when these are needed for data transfer. On the other hand, in pro-active route establishment routes between all the nodes are maintained all the time whether these are needed or not. DSDV [7] is the prime example of pro-active routing protocol. While in the combination of these two types hybrid protocols are proposed such as Zone routing protocol (ZRP) [8] in which for local communication routes are maintained pro-actively while for distant communication routes are established in re-active manner. Each of these types of routing protocol comes with their advantages and drawbacks and is used according to the requirements that are desired from the network to be fulfilled.

Received (December 30, 2017), Review Result (February 5, 2018), Accepted (February 11, 2017)

46/121

27

PS

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Critical Review of Techniques for Detection and Mitigation of Co-operative Blackhole Attack in MANET

Nitin Khanna^{1,*} and Monika Sachdeva²

¹Department of Computer Science, Lyallpur Khalsa College, Jalandhar, India

²Department of Computer Science & Engineering, IKGPTU, Kapurthala India

¹nitinkhanna300@gmail.com, ²monasach1975@gmail.com

Abstract

Mobile Ad-hoc NETWORK can be stated as a self configuring network that is infrastructure-less and communication happens in multi-hop manner. This dynamic nature of MANET and lack of infrastructure makes it vulnerable to many types of attacks; both routing and security. Out of all these attacks a variation of packet drop attack known as co-operative Blackhole attack proves to be a bottleneck in MANET. In this paper, we have reviewed many existing solutions that are useful in mitigation and detection of co-operative Blackhole attack. Co-operative Blackhole involves two or more malicious nodes working together to perform packet drop. We have provided a detail on these mechanisms involving the methodology and algorithms followed in the mechanisms, simulation and their conclusive result in brief and their critical review for drawbacks and advantages. A comparison is drawn and finally, the areas are identified in the field of mitigation of co-operative Blackhole attack on which the future research should be focussed.

Keywords: Mobile Ad-hoc Networks, Co-operative Blackhole Attack, Blackhole Attack, Dynamic Source Routing, Routing Overheads

1. Introduction

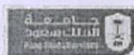
Mobile Ad-hoc Network is a self configuring network [1] which is composed of many mobile nodes that communicates with each other to for communication purpose. These movable nodes communicate with each other in multi-hop [2] fashion without any kind of infrastructure. All the communication is done via wireless links that are formed using any of routing protocol that all the mobile devices have implemented. MANET found its application in military operations, personal area network (PAN) [3], disaster management and many other applications where a fixed infrastructure is not possible to be established. The feature of infrastructure-less framework, multi-hop communication and dynamic nature gives an additional benefit of deployment of this network in cases where normal network cannot be established. The route establishment is done in MANET either reactively, pro-actively or through combination of both types. In pro-active route establishment routes between all the nodes are maintained all the time whether these are needed or not. DSDV [4] is the prime example of pro-active routing protocol. On the other hand, for re-active path establishment, re-active route discovery protocols such as AODV [5], DSR [6], OLSR [7], etc are used in which routes are established only when these are required for data transfer. While in the combination of these two types are known as hybrid are proposed such as Zone routing protocol (ZRP) [8] in which for local communication routes are maintained pro-actively and for distant communication routes are established in re-active manner. Each of these types of routing protocol comes with their advantages and disadvantages and is used depending upon the requirements that are desired from the network and needed to be fulfilled.

Received (December 25, 2017), Review Result (January 10, 2018), Accepted (January 11, 2018)

47/121

7

PS



On QoS evaluation for ZigBee incorporated Wireless Sensor Network (IEEE 802.15.4) using mobile sensor nodes

Vishal Kumar Arora^{a,*}, Vishal Sharma^b, Monika Sachdeva^c

^aResearch Scholar, IKG Punjab Technical University, Kapurthala, Punjab, India

^bDepartment of Electronics and Communication Engineering, SBS State Technical Campus, Punjab, India

^cDepartment of Computer Science and Engineering, IKG PTU Campus, Punjab, India

ARTICLE INFO

Article history:

Received 11 April 2018

Revised 19 September 2018

Accepted 22 October 2018

Available online xxxx

Keywords:

ZigBee

Node-mobility

Network-size

Node-density

QoS

ABSTRACT

The design of an efficient and scalable Wireless Sensor Network (WSN) to accommodate the fluctuations in topology, node-mobility, node-density, and network-size is an exigent task. A meticulous investigation is necessitated to implement the sensor nodes in an appropriate topology at optimum node-mobility in ZigBee incorporated WSN networks to offer optimum Quality of Services (QoS). Subsequently, an attempt to compute the comprehensive recital of a non-beacon mode based 802.15.4/ZigBee integrated WSN network is demonstrated. An analytical model is designed using parameters such as back-off number, retransmission limit, and back-off exponent considering the impact of node-mobility which has not reported earlier. Further, the investigation is carried out experimentally by evaluating the different QoS metrics, for instance, throughput, network load, bit error rate (BER), received power, signal to noise ratio (SNR) and end-to-end delay for diverse node-density and network-size of a mobile Wireless Sensor Network. Based on the measurements obtained, the authors recommend implementing the mobile sensor nodes in a cluster-tree fashion to afford the best possible QoS services.

© 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

1. Introduction

The Wireless Sensor Network (WSN) nodes are capable of sensing data from the environment, removing redundancy from sense data and transmitting to the base station through wireless media. Usually, it is hard to establish a connection among wireless nodes due to either low battery status or other wireless failures Kobo et al. (2017). More and Raisinghani (2017). Hasan et al. (2017) presented real-time multi-path routing protocols for Wireless Multimedia Sensor Networks (WMSNs) and discussed the design issues affecting the development of strategic multi-path routing protocols that support multimedia data in WMSN. The WSN network can be categorized into two categories namely: Category-1 WSN and Category-2 WSN. Category-1 WSN network (C1WSN) incorporates nodes which are connected to each other using mesh

topology via dynamic routing. This type of network is used in a large system having massive data flow such as highway monitoring, military applications, habitat monitoring, and environmental surveillance. However, the Category-2 WSN (C2WSN) type network uses static routing and is based on either point to point or point to a multi-point system to connect the different sensing nodes inside the network. Mainly, such network is used for short-range systems such as a home control, industrial automation and medical system, etc. Prior to this, there are a number of wireless systems such as Wi-Fi, Infrared, and Bluetooth, which offers high data rates. Wi-Fi (IEEE 802.11b), being too complex and requires more bandwidth, hence, cannot be implemented in sensor networks Tahir et al. (2017). On the same side, Infrared necessitate line of sight that is almost not viable, thus, cannot be used for such networks. Alternatively, Bluetooth (IEEE 802.15.1) was considered a possible solution but supports a small number of devices in one PICONET, lack self-healing technology and moreover, it is also expensive (regarding power consumption). Consequently, Bluetooth technology is found inflexible to put into practice for sensor network Tahir et al. (2017).

In 2003, a new technology 802.15.4 along with ZigBee was found and becomes standard for a C2WSN network. IEEE 802.15.4 operates in 2.4 GHz band and currently, it can support data transmission from 4.8 kbps to 800 kbps in the range of

* Corresponding author.

E-mail address: vishal.fcr@gmail.com (V.K. Arora).

Peer review under responsibility of King Saud University.



Production and hosting by Elsevier

<https://doi.org/10.1016/j.jksuci.2018.10.013>

1319-1578/© 2018 The Authors. Production and hosting by Elsevier B.V. on behalf of King Saud University.

This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Please cite this article in press as: Arora, V.K., et al. On QoS evaluation for ZigBee incorporated Wireless Sensor Network (IEEE 802.15.4) using mobile sensor nodes. Journal of King Saud University – Computer and Information Sciences (2018), <https://doi.org/10.1016/j.jksuci.2018.10.013>

48/121

2

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



A multiple pheromone ant colony optimization scheme for energy-efficient wireless sensor networks

Vishal Kumar Arora¹ · Vishal Sharma² · Monika Sachdeva³

© Springer-Verlag GmbH Germany, part of Springer Nature 2019

Abstract

Ant colony optimization (ACO) is a well-applied technique to solve the real-time problem of discovering the energy-efficient routes to transmit the sensing information to the base station (BS). Traditionally, ACO incorporated wireless sensor networks used only one pheromone, i.e., minimum distance between the sensor nodes to discover the optimum route to the BS. The authors illustrated a multiple pheromone-based ACO technique known as multiple pheromone ant colony optimization (MPACO), for instance, distance between sensing nodes, their residual energy and number of neighbor nodes to ascertain an efficient route. MPACO enables the sensing nodes to transmit the sensing data to BS over optimal routes with economical energy consumption to achieve a prolonged network life span. The comprehensive evaluation reveals that MPACO proffers 20% more network lifetime than the current existing ACO technique, i.e., improved ACO. Moreover, MPACO shows a significant improvement of 300% in network life span than another existing fuzzy-based strategy, i.e., multi-objective fuzzy clustering algorithm.

Keywords Energy-aware routing · Wireless sensor networks · Swarm intelligence · Ant colony optimization

1 Introduction

Wireless sensor networks (WSNs) are being designed for a number of monitoring applications, for instance, to detect the water level in the dams, observing air quality to detect dangerous gases, to control pollutant in water and many other consumers/industrial areas (Qiu et al. 2017; Duan et al. 2017). Generally, WSN comprises of spatially dedicated sensor nodes for monitoring, aggregating and forwarding the collected data to a central location, i.e., BS. The sensor nodes are randomly deployed, left unattended and are expected to perform efficiently. Each sensor node consumes a certain amount of energy to sense, process and to transmit the processed data to the BS. These sensor nodes are battery operated

and difficult to replace or recharge. Moreover, each sensor node has a range of detection and estimates its distance from the source node by accessing the intensity of the received signal. This received signal is attenuated with an increase in distance between the destination node and the source node.

In couple of decades, a number of issues including energy consumption, clock synchronization techniques, secure data aggregation and efficient routing techniques have been analyzed and investigated by the researchers for improving the performance of such networks (Dehkordi and Schmaltz 2012; Labraoui et al. 2013). However, an energy-efficient routing technique is a challenging issue till date. Generally, energy-efficient routing reduces the power consumption by distributing load uniformly among the sensor nodes and is classified in two categories: flat and hierarchical routing protocols (Al-Karaki and Kamal 2004). In flat-based routing, each sensor node has its unique global address and at the same level. Alternatively, flat-based routing is further categorized as proactive, reactive and hybrid routing strategies (Pantazis et al. 2013). In proactive, each sensor node maintains its own routing table to evaluate a route to the destination. So, each sensor node transmits its own data to the destination node through the pre-defined route, for instance, the Wireless Routing Protocol (WRP), and Topology Dissemination

Communicated by V. Loia.

✉ Vishal Kumar Arora
vishal.fzr@gmail.com

¹ IKG PTU, Kapurthala, Punjab, India

² Department of Electronics and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India

³ Computer Science and Engineering Department, IKG PTU, Kapurthala, Punjab, India

Published online: 21 March 2019

Springer

49/121

X

PR

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



RESEARCH ARTICLE

WILEY

A distributed, multi-hop, adaptive, tree-based energy-balanced routing approach

Vishal Kumar Arora¹ | Vishal Sharma² | Monika Sachdeva³

¹Research Scholar, CSE, IKG Punjab Technical University, India

²Department of Electronics and Communication Engineering, SBS State Technical Campus, Ferozepur, India

³Department of Computer Science and Engineering, IKG PTU, Kapurthala, India

Correspondence

Vishal Kumar Arora, Research Scholar,
IKG Punjab Technical University,
Kapurthala, Punjab, India.
Email: vishal.arora@sbsstc.ac.in

Summary

To accomplish the primary objective of data sensing and collection of wireless sensor networks (WSN), the design of an energy efficient routing algorithm is very important. However, the energy constrained sensing nodes along with the intrinsic properties of the (WSN) environment makes the routing a challenging task. To overcome this routing dilemma, an improved distributed, multi-hop, adaptive, tree-based energy-balanced (DMATEB) routing scheme is proposed in this paper. In this scheme, a relay node is selected in view of minimum distance and high energy from a current sensing node. Further, the parent node is chosen among the selected relay nodes on the basis of high residual energy and less power consumption with due consideration of its associated child nodes. As each sensing node itself selects its parent among the available alternatives, the proposed scheme offers a distributive and adaptive approach. Moreover, the proposed system does not overload any selected parent of a particular branch as it starts acting as a child whenever its energy lowers among the other available relay nodes. This leads to uniform energy utilization of nodes that offers a better energy balance mechanism and improves the network lifespan by 20% to 30% as compared with its predecessors.

KEYWORDS

energy efficient routing, tree-based structure, wireless sensor network

1 | INTRODUCTION

Wireless sensor network (WSN) is a collection of small-size, low-priced sensing nodes deployed over a particular area in ad hoc fashion that measures environmental conditions and communicates such information to a base station (BS).^{1,2} The self-organization and fault-tolerance nature of such networks make them flexible for military, health, industrial, surveillance, and traffic systems. All sensor nodes sense and process the data from its neighbor node and is followed by its transmission to the other node or to the BS.³ WSN network has a requirement of rigorous design strategy as they have to operate in a resource constraint environment. To achieve this goal resourcefully, the energy efficient routing protocols had been developed that define different routes between the sensor nodes and BS.^{4,5} Moreover, the energy-constrained sensor nodes along with the intrinsic properties of the WSN environment makes the routing a challenging issue.⁶ The scheme presented by Heinzelman exclusively allows sensor nodes to directly communicate with their respective cluster heads (CHs) even if the distance between them is very large.⁷ These CHs transmit the gathered information directly to the BS in a single-hop manner. This method is straightforward, but because of the consumption of large energy, it makes this method inappropriate for long distance communication. Moreover, in some scenarios like CHs are positioned far away

50/121

7

PH

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



ACO optimized self-organized tree-based energy balance algorithm for wireless sensor network

AOSTEB

Vishal Kumar Arora¹ · Vishal Sharma² · Monika Sachdeva³

Received: 27 August 2018 / Accepted: 3 January 2019
© Springer-Verlag GmbH Germany, part of Springer Nature 2019

Abstract

Energy-efficient routing algorithms must handle power-limitation issue of the sensor nodes intelligently to prolong the network life of wireless networks. Accordingly, it is indispensable to collect and exchange the sensor data in an optimized way to reduce energy consumption. Subsequently, an ACO Optimized Self-Organized Tree-Based (AOSTEB) Energy Balance Algorithm for Wireless Sensor Network has been proposed that discovers an efficient route during intra-cluster communication. AOSTEB scheme operates in three phases: cluster-formation, multi-path creation, and data transmission. During cluster-formation, the desired number of sensor nodes are alleviated to the role of cluster-heads (CHs), and the remaining neighboring sensor nodes join the nearest CHs to form a cluster. Further, the multiple paths between the CH and member nodes are discovered using Ant Colony Optimization algorithm. A dynamic energy efficient optimized route is selected within a specific cluster on account of shortest distance and less energy-consumption to initiate the data exchange process within the cluster. The extensive simulation observations ascertain the efficiency of the proposed algorithm by demonstrating the prolonged network lifetime, enhanced stability period, and reduced energy consumption in contrast to the earlier reported works in wireless sensor networks.

Keywords Wireless sensor network · Energy efficient routing · Ant colony optimization

1 Introduction

Wireless sensor networks (WSNs) are extremely versatile in nature to support a large number of applications depending upon the deployment of sensors nodes. Despite the differences in the purposes of application scenarios, the main chore of the nodes is to sense the data and transmit to the base station (BS) (Fei et al. 2016; Yetgin et al. 2017). Energy-efficient routing protocols are used to achieve this chore efficiently. The design of routing algorithms must contemplate the energy limitation of the sensor nodes along

with the required resources of the intended application scenarios. Moreover, the traditional routing protocols cannot be used for WSNs due to high routing cost which further augments with the increase in network size and dynamic conditions. So, an efficient routing algorithm is required which consider the network adaptiveness, and power limitation of sensor nodes. To cater these needs of the sensor network, many classifications have been proposed in the past (Pantazis et al. 2017). One such classification is known as flat network architecture in which all sensor nodes performed the same role inside the network and are reflected at the same level. The main advantage of this architecture is less overhead to discover the multiple paths between the communicating nodes. In the second classification called hierarchical protocols, for instance, Low Energy Adaptive Clustering Hierarchy (LEACH), Power Efficient Gathering Sensor Information System (PEGASIS), Tree-Based Clustering (TBC), and General Self-organized Tree Based (GSTEB), the sensor nodes are organized into clusters. These routing

✉ Vishal Kumar Arora
vishal.fzr@gmail.com

¹ IKG PTU, Kapurthala, Punjab, India

² Department of Electronics and Engineering, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, India

³ Computer Science and Engineering Department, IKG PTU, Kapurthala, Punjab, India

5/1/21

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



Study of trust-based mechanism and its component model in MANET: Current research state, issues, and future recommendation

Nitin Khanna¹ | Monika Sachdeva²

¹Department of Computer Science, Kanya Maha Vidyalaya, Jalandhar, India

²Department of Computer Science & Engineering, IKGPTU, Kapurthala, India

Correspondence

Nitin Khanna, Department of Computer Science, Kanya Maha Vidyalaya, Jalandhar, India.
Email: nitinkhanna300@gmail.com

Summary

Security against routing attacks in MANET is most critical issue and traditional concepts of cryptography, authentication, or Watchdog are not that significant in mitigation of these attacks. In recent years, trust-based approach provides a reputation system that compose of different components to provide security against routing attacks. In this paper, we provide an in-depth analysis of various components that are used in trust-based mechanism and techniques deployed in effective and efficient execution of task by the components. Trust-based mechanisms generally have five components: monitoring and information gathering, trust calculation and evaluation unit, trust recommendation unit, decision-making and dissemination of detection unit. All or some of these units cooperate together to provide a reliable communication environment with the aim to prevent routing attacks from participating in route formation process and detect attacking nodes simultaneously. Different routing attacks and measures in trust-based mechanism along with some published work are discussed to understand the implementation of this type of mechanism. Various related issues are explored, discussed, and recommendations are pointed out for future research work in this field.

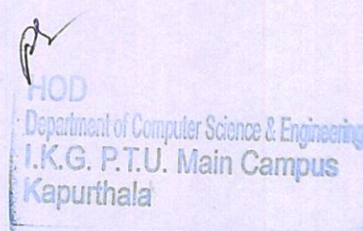
KEYWORDS

MANET, routing, security attacks, trust-based mechanism, trust mechanism components, trust model

1 | INTRODUCTION

MANET is a kind of ad-hoc network in which movable nodes are deployed for communication through wireless medium. Ad-hoc network implies formation of path on temporary basis due to the fact that with mobility, the path can be disrupted because of the movement of two nodes away from each other beyond their communication range. MANET is widely used in the field of military operations and disaster management where security and lack of infrastructure are the prime issues in the respective field. Infrastructure-less network¹ makes it handy to use in areas where installation of fixed structure network is not feasible. MANET can operate in that situation due to its mobility of nodes and communication with each other in multihop² manner in which nodes act as routers for delivery of data from source to destination. Source and destination are also the similar kind of nodes that can also work as multihops. This distributive, ad-hoc, and mobile nature of MANET makes it prone to many data security and routing attacks³ for mitigation of which it needs

52/121





OFFM-ANFIS analysis for flood prediction using mobile IoT, fog and cloud computing

Nitin Khanna¹ · Monika Sachdeva²

Received: 18 September 2019 / Revised: 18 September 2019 / Accepted: 19 December 2019
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract

Flood is one of the most destructive natural disaster that can affect hundreds of thousands people and infrastructure that can cost in the range billion of rupees. After so much research in this field, we still suffer from the disastrous effect of it due to lack of consideration of small scale flood affecting parameters affecting regional floods. In this research paper, an IoT based sensing network powered by mobile edge computing (MEC), fog computing and cloud computing is proposed for flood prediction and forecasting after analysis through modified multi-ANFIS architecture known as OFFM-ANFIS. The sensing layer includes various static and mobile sensors IoT nodes that pass the data to fog server via MEC. Both regional fog server and cloud is facilitated with the training, testing, analysis and decision making power that rates the chances of flood on an ordinal scale. The OFFM-ANFIS includes seven modified ANFIS models that make decision on flood forecasting on the basis of trained data and analysis of received senses data. The flow of raw and analyze data from OFFM-ANFIS is staged in a way that more influential parameters have strong impact in the final forecasting output. Evaluation of the proposed mechanism is done on the basis of data provided by Indian Meteorological Department and effectiveness is shown in the application of proposed mechanism in forecasting flood well before its occurrence.

Keywords IoT · OFFM-ANFIS · Flood prediction · Fog computing · Cloud computing · Computational verification

1 Introduction

With the rise of new era in computational world, Internet of Things (IoT) [1] has powered different sectors by delivering numerous services in various fields like agriculture, healthcare, smart city build up, transportation, disaster management, etc. [2–6] and emerged as the core part of pervasive and ubiquitous networking [7]. IoT is defined as a technology that interconnects different devices over some form of a network. It can be both wired or wireless. The devices involved in the IoT network can be sensors, different form of hardware, software, actuators, triggers, etc.

that can be used in variety of applications according to the need. With revolutionary development in this field it serves the living beings in variety of ways. The term IoT is presented as IoT, IoN [8] in some of the literature but meant same set of technology just giving it a much more application specific terminology. IoT devices help in sensing and gathering data from the surroundings which are then further used for analysis and decision making by that device or is sent to some centralized component in the network such as IoT cluster head, fog server or cloud computing server where the gathered data is analyzed, processed and appropriate activity is performed following data processing. Sometimes that activity is performed by IoT through their actuators in response to the command sent through that centralized servers. For large scale applications that involved bulk amount of data such as healthcare application or disaster management requires the use of cloud processing as IoT cannot process this huge amount of data on their own that too in decentralized manner. This is due to the fact that a lot of IoT sensors or devices are deployed for sensing data and performed

✉ Nitin Khanna
nitinkhanna300@gmail.com
Monika Sachdeva
monasach1975@gmail.com

¹ Department of Computer Science, Kanya Maha Vidyalaya, Jalandhar, India

² Department of Computer Science & Engineering, IKGPTU, Kapurthala, India

53/121

[Handwritten signature]

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

BEST: Battery, Efficiency and Stability Based Trust Mechanism Using Enhanced AODV for Mitigation of Blackhole Attack and Its Variants in MANETs.

Source: Adhoc & Sensor Wireless Networks . 2020, Vol. 46 Issue 3/4, p215-264. 50p.

Author(s): KHANNA, NITIN; SACHDEVA, MONIKA

Abstract:

This paper attempts to resolve the issue of mitigation of blackhole attack and its variants by presenting a battery, efficiency and stability based trust mechanism that performs both prevention and detection of packet drop attacks followed by isolation using the process of dissemination of information validated by the fair nodes. The proposed work operates in two modes to combat both single as well as co-operative form of attack. In standard mode, the promiscuous facility and trust update lead to detection of attack while in advance mode a set of trusted trace packets and procedures detect co-operative attacking nodes thus break the co-operation among malicious nodes. After detection of malicious nodes, dissemination process leads to isolation of the attacking node and validation is performed to avoid bad mouthing attack. The work is compared with several published mechanisms against parameters like PDR, normalized control load, accuracy in detection and residual energy.

Copyright of Adhoc & Sensor Wireless Networks is the property of Old City Publishing, Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use. This abstract may be abridged. No warranty is given about the accuracy of the copy. Users should refer to the original published version of the material for the full abstract.

For access to this entire article and additional high quality information, please check with your college/university library, local public library, or affiliated institution.



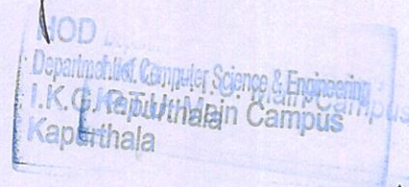
Important User Information: Remote access to EBSCO's databases is permitted to patrons of subscribing institutions accessing from remote locations for personal, non-commercial use. However, remote access to EBSCO's databases from non-subscribing institutions is not allowed if the purpose of the use is for commercial gain through cost reduction or avoidance for a non-subscribing institution.

[Privacy Policy](#) | [A/B Testing](#) | [Terms of Use](#) | [Copyright](#) | [Cookie Policy](#)

© 2021 EBSCO Industries, Inc. All rights reserved.

54/121

Handwritten signature and initials.



[View article](#)



Monika Sachdeva

[Edit](#) [Delete](#)

Detection of denial of service using a cascaded multi-classifier

Authors: Avneet Dhingra, Monika Sachdeva

Publication date: 2021

Journal: International Journal of Computational Science and Engineering

Volume: 24

Issue: 4

Pages: 405-416

Publisher: Inderscience Publishers (IEL)

Description The paper proposes a cascaded multi-classifier two-phase intrusion detection (TP-ID) approach that can be trained to monitor incoming traffic for any suspicious data. It addresses the issue of efficient detection of intrusion in traffic and further classifies the suspicious traffic as a DDoS attack or flash event. Features portraying the behaviour of normal, DDoS attack, and flash event are extracted from historical data obtained after merging CAIDA'07, SlowDoS2016, CIC-IDS-2017, and WorldCup 1998 benchmark datasets available online along with the commercial dataset for e-shopping assistant website. Information gain is applied to rank and select the most relevant features. TP-ID applies supervised learning algorithms in the two phases. Each phase tests the set of classifiers, the best of which is chosen for building a model. The performance of the system is evaluated using the detection rate, false-positive rate, mean ...

Scholar articles Detection of denial of service using a cascaded multi-classifier
A Dhingra, M Sachdeva - International Journal of Computational Science and ..., 2021
All 2 versions

[Help](#) [Privacy](#) [Terms](#)

55/121

9/

PL

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

VALIDATION OF RATIONALE CHARACTERIZING THE ANOMALIES
CAUSING DENIAL OF SERVICEA. DHINGRA¹ AND M. SACHDEVA

ABSTRACT. The DDoS attack is not just about surging traffic; it includes all the active appliances into its botnet, targeting a specific model of the device. Subsequently, the attacks have become stealthier and sophisticated. Flash event (FE), the legitimate counterpart of DDoS attack, overwhelms the server with requests from legitimate users trying to access information. Both traffic patterns compromise the availability of the target server. This paper highlights the characteristics of DDoS and FE, and evaluates the characteristics discerning DDoS and FE traffic using real-time benchmark datasets. The rationale for both events has been empirically investigated. The paper compares the relative variability of parameters discerning the anomalies by applying the coefficient of variation. The analysis shows that CV of time-interval between request, request sent by each user throughout the event, and request sent by each user in a given time-interval is higher for FE when compared to DDoS attack. From the statistical results obtained, it can be concluded that the FE traffic is more unplanned and non-specific. Thus, though two mentioned events exhibit the same behaviour, the variation in behaviour is observed in quantifying the rationale.

1. INTRODUCTION

Distributed Denial of service attack (DDoS) has become a severe threat to the availability and reliability of the victim server. The attack saturates or somehow blocks the victim server and its infrastructure with spoofed requests using

¹corresponding author

2010 Mathematics Subject Classification. 68M12, 94A17.

Key words and phrases. DDoS attacks, Flash Event, network anomaly, IP Address.

4103

58/121

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

A Comprehensive Study of Routing Layer Intrusions in ZigBee based Wireless Sensor Networks

Navjot Sidhu¹ and Monika Sachdeva²

¹Research Scholar, Department of RIC, IKG Punjab Technical University, Kapurthala

²Associate Professor, Department of Computer Science & Engineering, IKG Punjab Technical University, Kapurthala

¹navjotsidhu8@gmail.com, ²monasach1975@gmail.com

Abstract

The security of Wireless Sensor Network is a critical research topic these days. The major issue in such networks, is the vulnerability of routing protocols to network attacks. Most of the researchers have studied several possible attacks in these networks either considering different proposed routing algorithms or in general. However, actual sensor nodes work only on standardized protocol stack. Therefore, ZigBee Wireless Sensor Network is considered to present the impact and consequences of routing attacks in this paper. Additionally, the theoretical analysis of possible attacks in Ad-hoc on Demand Distance Vector routing protocol is presented in terms of attacker's actions and goals behind such intrusions in sensor networks. This study is advantageous for the research community to implement these attacks in test-bed or simulated environments. So that the impact of attacks can be captured correctly and the timely detection of these intrusions can be proposed for resource constrained wireless sensor networks.

Keywords: Intrusion, Network, Protocol, Routing, Security, Wireless Sensor Network, ZigBee

1. Introduction

Wireless Sensor Network (WSN) is an infrastructure-less network consists of small sized, inexpensive, low power and resource constrained sensor nodes. These sensors are deployed either randomly or manually to sense the environmental conditions. The prime functions of a sensor node include sensing of environmental data, processing of local data and sending the data to the base station [1]. Due to the various functionalities provided by these networks, these have been implemented in multiple real time applications. The Great Duck Island (GDI) System used for habitat monitoring [2], PODS a small ecological sensor network used to investigate the endangered species [3], Automated Local Evaluation in Real Time (ALERT) [4], an automated flood alarm system are few popular real time WSN projects that were being successfully implemented and installed to monitor different environmental scenarios initially.

With the advancements in the wireless technology, these networks have gained huge popularity in the global market in last decade. However, security of these unattended networks is still a very critical issue that need to be addressed to save the constrained network resources from being damaged by attackers. As discussed by [5] the major security issues of these networks can be categorized as cryptography, key management, attacks detection and prevention, secure routing, secure location and secure data aggregation. In order to do research in any of these mentioned areas, the research community must have a deep knowledge of the working and implementation of these networks in real time.



Face mask detection using YOLOv3 and faster R-CNN models: COVID-19 environment

Sunil Singh¹ · Umang Ahuja¹ · Munish Kumar² · Krishan Kumar¹ · Monika Sachdeva³

Received: 7 July 2020 / Revised: 23 January 2021 / Accepted: 10 February 2021 /
Published online: 1 March 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC part of Springer Nature 2021

Abstract

There are many solutions to prevent the spread of the COVID-19 virus and one of the most effective solutions is wearing a face mask. Almost everyone is wearing face masks at all times in public places during the coronavirus pandemic. This encourages us to explore face mask detection technology to monitor people wearing masks in public places. Most recent and advanced face mask detection approaches are designed using deep learning. In this article, two state-of-the-art object detection models, namely, YOLOv3 and faster R-CNN are used to achieve this task. The authors have trained both the models on a dataset that consists of images of people of two categories that are with and without face masks. This work proposes a technique that will draw bounding boxes (red or green) around the faces of people, based on whether a person is wearing a mask or not, and keeps the record of the ratio of people wearing face masks on the daily basis. The authors have also compared the performance of both the models i.e., their precision rate and inference time.

Keywords COVID-19 · YOLO v3 · Faster R-CNN · Face mask detection · Deep learning

✉ Munish Kumar
munishcse@gmail.com

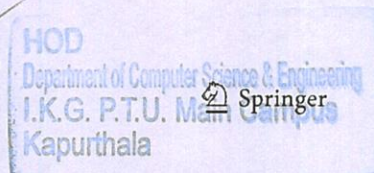
Sunil Singh
sunil32123singh@gmail.com

Umang Ahuja
umangahuja1203@gmail.com

Krishan Kumar
k.salujaiet@gmail.com

Monika Sachdeva
monasach1975@gmail.com

Extended author information available on the last page of the article



Efficient Resource Management Technique for Performance Improvement in Cloud Computing

Harvinder Singh*

Research scholar, IKGPTU Kapurthala, Punjab, India
harvinder9815653260@rediffmail.com

Dr. Anshu Bhasin

IKGPTU Kapurthala, India
Dr.anshubhasin@ptu.ac.in

Abstract

Cloud computing is growing technology which provide services to user's on affordable budget. Resource demand comes with different nature and create uncertainty situation for efficient resource matching and workload management on resources. Thus service providers' focus on suitable resource allocation technique for efficient resource matching based on resource availability and requirements. Such matching problems should be addressed using optimization approach. In this research paper we have presented an optimization approach using ant colony optimization (ACO) mechanism for efficient resource matching to minimize execution time. Our presented algorithm has been executed on cloud based simulation environment. The comparative analysis of results show that proposed algorithm performed better against existing algorithms and suitable for resource allocation in cloud to achieve quality of service (QoS) requirements and improve customer reliability.

Keywords: Cloud computing; performance; resource allocation; execution time; swarm intelligence.

1. Introduction

Cloud computing is providing dynamic service on public domain in form of infrastructure as a service (IaaS), platform as a service (PaaS), software as a service (SaaS) based on quality of service (QoS) requirements. The cloud system motivates to organization to migrate from local commodity storage environment to on demand infrastructure which is based on pay-per-use model under service level agreement (SLA) rules. Thus, it avoids purchasing costly IT infrastructure and organizations use IT services on cost effective budget. As cloud is emerging platform to access information for different domains and energy consumption of resources impact on resource utilization and performance. Therefore, cloud service provider should manage efficient performance based on customer QoS expectations to improve user reliability and minimize execution time. So, cloud environment is becoming complex due to growing large scale applications. Performance can be improved based on QoS (execution time), if resources allocated as per demand from available resources. Resources allocation and management of resources direct impact on performance and consider as minimum execution time, which is difficult problem in clouds. As cloud users' demand for resource and expected results with limited time. Thus, service providers must ensure to provide effective cloud service as per application demand in the perspective of QoS with limited number of resources on minimum time. User demand have changed dynamically and difficult to maintain the load across the cloud resources as heterogeneity is there. We survey on existing research publications concerned to resource allocation problem which shown that presented techniques cannot be efficiently managed the cloud uncertainty problem where dynamic, heterogeneous and unpredictability exists. Therefore, an efficient resource allocation technique should be there based on QoS requirements to improve customer reliability and maximize profits. Resource allocation strategies impact on operational cost, utilization and energy consumption. To achieve effectively execution of task based on minimum execution time different resource management techniques used in cloud environment. Therefore, expected performance and QoS based results depends on resource management technique followed by resource matching procedure. "Cloud computing is a type of parallel and distributed system consisting of a dynamically

27

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Efficient Retrieval of HTML Documents using Hybrid PSO and Hybrid ACO in Web Document Clustering

¹MANJIT SINGH, ²ANSHU BHASIN, ³SURENDER

¹Ph.D Research Scholar, Department of Computer Applications, IK Gujral Punjab Technical University, Kapurthala, Punjab, India ²Assistant Professor, Department of Computer Science & Engineering, IK Gujral Punjab Technical University, Main Campus, Kapurthala, Punjab, India

³Assistant Professor, Department of Computer Science, Guru Tegh Bahadur College, Bhawanigarh, Sangrur, Punjab, India

Abstract—With the rapid development of web documents on WWW, the organization, analysis and presentation of these documents is becoming increasingly difficult. Web search is usually done with features which are just extracted from the web page text. The tag information in HTML documents has been found to be useful for getting better performance of the information retrieval system. However, in the recent times, the volume of data on the World Wide Web is rapidly increasing day by day. It becomes a significant challenge for finding the required information on the net. This leads to the need for the development of the new approach that may aid users in navigating, summarizing and organizing the required information. One of the techniques that could be useful to achieve this goal is web document clustering. However, existing partition clustering techniques suffer from local optima problems. Various efforts have been made for addressing such drawbacks. This includes the utilization of various meta-heuristic approaches as well. In this research work, we provide a document clustering technique which uses HTML tags and PSO (Particle Swarm Optimization) and Ant Colony Optimization (ACO) approaches. The hybrid PSO+ K-means and ACO+ K-means algorithm are used to cluster the web documents. In the proposed approaches, results are analyzed on WEBKB dataset.

Keywords: HTML, Information Retrieval, Ant Colony Optimization, Particle Swarm Optimization, Meta-Heuristic

I. INTRODUCTION

The Internet is now the best data repository, confronting the problem of overloading information. More and more people using the internet, nowadays, as the vital source of information. Due to the heterogeneous environment of the Web, information retrieval became a challenging practice for the average user. Search engines, generally, return several documents, only a few of returned documents are relevant and others are non-relevant. The search engine matches the query terms with the keywords that each webpage describes and provides results to users. These results are long lists of URLs that are very difficult to find. In addition, users those do not know the proper terminology without proper field knowledge could lead to the finding of more irrelevant pages. Currently, web search is usually carried out using features extracted from the text of the webpage only. The web documents present on the web are written using Hyper Text Markup Language mostly. These web pages are consist of a set of markup tags that describe the layout, the presentation, and the content of the web page. It has been found that by considering the terms within HTML tags of a web document, the performance of documents retrieval system can be improved. However, organizing the documents in a way which leads to better search without additional costs or complexity is an important challenge. This has led to new technologies to help users efficiently navigate, track and organize current web documents effectively. Clustering can play an essential role for organizing such a large amount of documents returned by search engines into significant clusters. The cluster is a collection of data items that are similar to each other in the same cluster and are dissimilar to data items in other clusters. Clustering can mainly be separated into hierarchical and partitions approaches. The major disadvantage of the hierarchical approach is that it is stagnant and cannot distinguish between overlapping groups. K-means have been established for the clustering of large data sets. But K-means, due to its choice of initialization, also faces many drawbacks. The optimization techniques were considered in order to overcome these problems and the data clustering was considered as an optimization problem. Optimization techniques has significantly enhanced the accuracy and efficiency of clustering. Meta-heuristics usually used are Particles Swarm Optimization, Ant Colony Optimization, and Genetic Algorithms.

*Corresponding Author: MANJIT SINGH, Email : singh53@gmail.com

Article History: Received: 04-04-2019, Revised: 25-05-2019, Accepted: 13-06-2019

1856

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Energy Conscious Packet Transmission in Wireless Networks Using Trust Based Mechanism: A Cognitive Approach

Anshu Bhasin^(✉), Sandeep Singh, and Anshul Kalia

IKG Punjab Technical University, Kapurthala, India
Dr.anshubhasin@ptu.ac.in, Sandeep_madda@yahoo.co.in,
Anshul17215@ptuuniversity.in

Abstract. The self-motivated nature of wireless ad-hoc networks deters the possibility of a centralized solution. Also, no specific node can act as a centralized point due to energy and processing constraints. Constraint of non-centralization demands efficient and effective transmission of data between nodes by sharing information whenever needed without any disruption. This co-operation is a prodigious challenge due to the presence of covetous and malicious nodes in the network. Hence, an asserted need of some lightweight trust based mechanism in differentiating among reliable and unreliable nodes arises. This mechanism enhances security and improve co-operation in nodes. Energy efficiency remains central to the above segregation. Many trust-based methods are proposed which use packet delivered ratio as the major parameter for direct trust calculation. This work presents investigation of other related parameters like routing overhead, energy level etc, which can increase the effectiveness of trust based mechanisms for early detection of malicious nodes along with packet delivered ratio. Furthermore, an ameliorated energy optimization model is proposed for wireless network.

Keywords: Wireless ad-hoc networks · Routing · Attacks · Energy · MANET

1 Introduction

Wireless systems are extensively in use for communication nowadays. Wireless systems have various characteristics like scalability, dynamic topology, low cost, easy setup, mobility, high user density, multi hop wireless transmission and convenience [1]. In ad hoc setup, nodes can move in or move out from the network at any time, causing the topology to change quickly and unpredictably. Each node in the ad hoc setup has to work as a transmitter and a receiver. All nodes are in authority to create, operate and maintain the ad hoc network. Wireless systems can be categorized into two types - the infrastructure based wireless networks and the infrastructure-less wireless networks (ad hoc networks).

MANET is an interconnected system of wireless networks that can be designed quickly and dynamically without requiring any additional external router or access point [2]. MANET is also sometimes referred as Self-Organizing Networks (SONs) [3].

© Springer Nature Switzerland AG 2020

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario*, AISC 1132, pp. 1–21, 2020.
https://doi.org/10.1007/978-3-030-40305-8_11

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Using Meta-heuristic Approaches in Web Document Clustering in Web Search

Manjit Singh¹, Anshu Bhasin², Surender³

¹Ph.D Research Scholar, Department of Computer Applications, IKG
Punjab Technical University, Kapurthala, Punjab, India
manjitsingh1994@gmail.com

²Assistant Professor, Department of Computer Science & Engineering, IKG
Punjab Technical University, Main Campus, Kapurthala, Punjab, India
dr.anshubhasin@pu.ac.in

³Assistant Professor, Department of Computer Science,
Guru Tegh Bhadur College, Bhawanigarh, Sangrur, Punjab, India
jantra.surender@gmail.com

Abstract: Internet is a gigantic information resource, which is rapidly growing day by day as more and more data are being added to the World Wide Web. With the rapid growth of web documents on the internet, it is becoming difficult to organize, analyze and present these documents efficiently. Clustering can act as a key player in organizing such a hefty amount of documents into groups. The performance of the IR system could be improved by document clustering. It has been found that HTML tags which have particular meanings could be used to enhance the performance of IR system. This paper provides a brief survey of the available literature on a web search in which HTML tags have been used in information retrieval and Meta-heuristics approaches used in web document clustering.

Keywords: Internet, gigantic, information, Web search, HTML, World Wide Web, retrieval, Meta-heuristics, clustering.

1. Introduction

With the rapid growth of web documents on WWW, it is becoming difficult to organize, analyze and present these documents efficiently. Web search engines can help the web user to browse and locate the documents in quick fashion. Normally web search engines return many documents to the web user, out of which some are relevant and some irrelevant documents to the topic, for the given query. Usually, web search is a currently being done using features that are extracted from the web page-text only. Hyper Text Markup Language is mostly used to write web documents. It has been observed that by considering the terms within HTML tags of a web document, the performance of

7

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Efficient Retrieval of HTML Documents using Hybrid PSO and Hybrid ACO in Web Document Clustering

¹MANJIT SINGH, ²ANSHU BHASIN, ³SURENDER

¹Ph.D Research Scholar, Department of Computer Applications, I.K. Gujral Punjab Technical University, Kapurthala, Punjab, India ²Assistant Professor, Department of Computer Science & Engineering, I.K. Gujral Punjab Technical University, Main Campus, Kapurthala, Punjab, India

³Assistant Professor, Department of Computer Science, Guru Tegh Bahadur College, Bhanisiggarh, Sangrur, Punjab, India

Abstract—With the rapid development of web documents on WWW, the organization, analysis and presentation of these documents is becoming increasingly difficult. Web search is usually done with features which are just extracted from the web page text. The tag information in HTML documents has been found to be useful for getting better performance of the information retrieval system. However, in the recent times, the volume of data on the World Wide Web is rapidly increasing day by day. It becomes a significant challenge for finding the required information on the net. This leads to the need for the development of the new approach that may aid users in navigating, summarizing and organizing the required information. One of the techniques that could be useful to achieve this goal is web document clustering. However, existing partition clustering techniques suffer from local optima problems. Various efforts have been made for addressing such drawbacks. This includes the utilization of various meta-heuristic approaches as well. In this research work, we provide a document clustering technique which uses HTML tags and PSO (Particle Swarm Optimization) and Ant Colony Optimization (ACO) approaches. The hybrid PSO+ K-means and ACO+ K-means algorithm are used to cluster the web documents. In the proposed approaches, results are analyzed on WEBKB dataset.

Keywords: HTML, Information Retrieval, Ant Colony Optimization, Particle Swarm Optimization, Meta-Heuristic

1. INTRODUCTION

The Internet is now the best data repository, confronting the problem of overloading information. More and more people using the internet, nowadays, as the vital source of information. Due to the heterogeneous environment of the Web, information retrieval became a challenging practice for the average user. Search engines, generally, return several documents, only a few of returned documents are relevant and others are non-relevant. The search engine matches the query terms with the keywords that each webpage describes and provides results to users. These results are long lists of URLs that are very difficult to find. In addition, users those do not know the proper terminology without proper field knowledge could lead to the finding of more irrelevant pages. Currently, web search is usually carried out using features extracted from the text of the webpage only. The web documents present on the web are written using Hyper Text Markup Language mostly. These web pages are consist of a set of markup tags that describe the layout, the presentation, and the content of the web page. It has been found that by considering the terms within HTML tags of a web document, the performance of documents retrieval system can be improved. However, organizing the documents in a way which leads to better search without additional costs or complexity is an important challenge. This has led to new technologies to help users efficiently navigate, track and organize current web documents effectively. Clustering can play an essential role for organizing such a large amount of documents returned by search engines into significant clusters. The cluster is a collection of data items that are similar to each other in the same cluster and are dissimilar to data items in other clusters. Clustering can mainly be separated into hierarchical and partitions approaches. The major disadvantage of the hierarchical approach is that it is stagnant and cannot distinguish between overlapping groups. K-means have been established for the clustering of large data sets. But K-means, due to its choice of initialization, also faces many drawbacks. The optimization techniques were considered in order to overcome these problems and the data clustering was considered as an optimization problem. Optimization techniques has significantly enhanced the accuracy and efficiency of clustering. Meta-heuristics usually used are Particles Swarm Optimization, Ant Colony Optimization, and Genetic Algorithms.

*Corresponding Author: MANJIT SINGH, Email : singh53@gmail.com
Article History: Received: 04-04-2019, Revised: 25-05-2019, Accepted: 13-06-2019

QoS Based Efficient Resource Allocation and Scheduling in Cloud Computing

Harvinder Chahal, Ekptu Kapurthala, Punjab, India

Anshu Bhasin, Ekptu Kapurthala, Punjab, India

Parag Ravikant Kaveri, Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, India

ABSTRACT

The Cloud environment is a large pool of virtually available resources that perform thousands of computational operations in real time for resource provisioning. Allocation and scheduling are two major pillars of said provisioning with quality of service (QoS). This involves complex modules such as: identification of task requirement, availability of resource, allocation decision, and scheduling operation. In the present scenario, it is intricate to manage cloud resources, as Service provider aims to provide resources to users on productive cost and time. In proposed research article, an optimized technique for efficient resource allocation and scheduling is presented. The proposed policy used heuristic based, ant colony optimization (ACO) for well-ordered allocation. The suggested algorithm implementation done using simulation, shows better results in terms of cost, time and utilization as compared to other algorithms.

KEYWORDS

Heuristics, Resource Availability, Resource Utilization, Swarm Intelligence

1. INTRODUCTION

Cloud computing service providers are providing commercial and reachable services to customers' as per requirements. It has been analyzed that organizations are migrating to cloud for variety of services which increases the difficulty in resource management that is challenging to achieve. Customer expectations are to get services on reasonable cost and in time. Thus, service providers must ensure to provide services based on customer needs, to meet quality of service (QoS). Proper allocation will lead to higher resource availability and increase the capability to meet customers' expectations. The appropriate workload distribution on resources is difficult due to user unpredictable demand. Therefore, resource distribution and workload management are research challenges in cloud computing that impact on utilization and performance. Research surveys indicate that cloud resource allocation and management is becoming complex day by day due to tremendous demand of cloud services (Mustafa et al., 2015). Therefore, to meet higher performance in cloud computing, an efficient resource allocation and scheduling technique should be developed. Optimizing resources in system will provide solutions to considering the resource with respect to demand and other aspects. In this

DOI: 10.4018/IJTHI.2019100102

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.



SECURE: Efficient resource scheduling by swarm in cloud computing

Harvinder Singh *

I.K. Gujral Punjab Technical University
Kapurthala 144601
Punjab
India

Anshu Bhasin *

I.K. Gujral Punjab Technical University
Main Campus
Kapurthala 144601
Punjab
India

Parag Kaveri *

Symbiosis Institute of Computer Studies and Research
(Symbiosis International Deemed University)
Pune 411016
Maharashtra
India

Abstract

Cloud computing is providing resources to customers based on application demand under service level agreement (SLA) rules. Service providers are concentrating on providing a requirement based resource to fulfill the quality of service (QoS) requirements. But, it has become a challenge to cope with service-oriented resources due to uncertainty and dynamic demand for cloud services. Task scheduling is an alternative to distributing resource by estimating the unpredictable workload. Therefore, an efficient resource scheduling technique needs to distribute appropriate virtual machines (VMs). Swarm intelligence, involving a metaheuristic approach, is suitable to handle such uncertainty problems meticulously. In this research paper, we present an efficient resource scheduling technique using ant colony optimization (ACO) algorithm, with an objective to minimize execution cost and time. The comparative analysis of results has been demonstrated that the proposed scheduling

*E-mail: rs.hachahal@ptu.ac.in (Corresponding Author)

*E-mail: dr.anshubhasin@ptu.ac.in

*E-mail: parag.kaveri@sicmr.ac.in

Cloud Resource Management: Comparative Analysis and Research Issues

Harvinder Singh¹, Anshu Bhasin¹, Parag Ravikant Kaveri², Vinay Chavan³

Abstract— Cloud resource management is momentous for efficient resource allocation and scheduling that requires for fulfilling customers' expectations. But, it is difficult to predict an appropriate matching in a heterogeneous and dynamic cloud environment that leads to performance degradation and SLA violation. Thus, resource management is a challenging task that may be compromised because of the inappropriate allocation of the required resource. This paper presents a systematic review and analytical comparisons of existing surveys, research work exists on SLA, resource allocation and resource scheduling in cloud computing. Further, discussion on open research issues, current status and future research directions in the field of cloud resource management.

Index Terms— Resource allocation, Resource scheduling, QoS, SLA, Heterogeneity, Scalability, VM management, Resource utilization, Energy consumption, Security, Monitoring

1 INTRODUCTION

Cloud computing providing virtual resources to customers under the pay-per-usage model managed by service providers. It includes infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). Service providers' priorities are to fulfill customers' expectations for competitive costs. Resource management needs the optimal usage of virtual resources to respond on a large scale. It is challenging to allocate a suitable resource on heterogeneous and dynamic task requirements that impacts performance and SLA. The quality of service (QoS) can be fulfilled by considering availability, scalability, utilization, cost, time, energy consumption and so forth. Cloud has the capacity to provide service according to the behavioral of applications. Organizations such as banking, health care system, educational platform, and e-commerce are using cloud services for storing and retrieving data [Pietri et al. 2016]. It has eliminated the need for purchasing physical resources [Jain et al. 2019]. Cloud service has become an integral part of our daily lives that fulfill information technology (IT) needs by cost-effectiveness and usability [Buyya et al. 2009]. To realize this, there is a challenge to ensure that guarantees QoS requirements and SLA by managing resource heterogeneity, dynamism, complexity, and uncertainty. It can distrust consumer and provider relations where pricing policies are according to QoS parameters [Mustafa et al. 2015].

Cloud computing features can efficiently manage varied application requirements need to be explored. Existing resource management techniques are unable to such a customizing environment to achieve important QoS parameters and avoid SLA violations. This survey has been conducted to provide a hands-on-information in the field of cloud resource management. In a cloud environment unpredictability and uncertainty, the problem causes inappropriate matching. It needs to consider the following:

- **SLA rules:** Consumers' are paying and expecting cloud service at a reasonable cost and time. But, it is challenging to provide expected performance and SLA violation.
- **Availability:** Resource availability plays an important role to process users' instant demand. But, dynamic reallocation leads to network congestion and energy consumption.
- **Dynamic environment:** The cloud environment is dynamic and unpredictable. It is difficult to manage dynamism and uncertainty.
- **Heterogeneity:** Cloud computing comprising heterogeneous resources. It can fulfill varied application demands. But, traditional techniques are unable to manage heterogeneity.
- **Geographical distance:** Cloud data centers are located in different geographical regions that require the proper distribution of isolated resources for higher utilization. But, existing resource management techniques are unable to manage diversified network resources.

Moreover, existing techniques need an extension to customize emerging platforms, such as edge computing, containers and hybrid cloud component [Gupta et al. 2017]. The main issue in this context to enhance availability, utilization, and elasticity that helps to avoid SLA violation [Zhan et al. 2015; Singh et al. 2015]. Therefore, a standardized technique should have existed for efficient cloud resource management.

1.1 Significance of Cloud Resource Management (CRM)

The motive of cloud resource management (CRM) is to provide applications based services by efficiently managing runtime resources. The traditional cloud would be replaced by hybrid components. There is a need for managing

- Harvinder Singh is currently pursuing Ph.D in computer application in IKGujrat Punjab Technical University Kapurthala, India E-mail: rs.techshub@ptu.ac.in
- Dr. Anshu Bhasin is currently Faculty in computer science and Engg at IKGujrat Punjab Technical University Kapurthala, India E-mail: dr.anshubhasin@ptu.ac.in
- Dr. Parag Ravikant Kaveri is currently Faculty in computer studies at Symbiosis Institute of Computer Studies and Research (SICSR), Symbiosis International (Deemed University), Pune, India E-mail: parag.kaveri@sicrs.ac.in
- Dr. Vinay Chavan is currently Faculty in computer science at Seth Kesarnil Purnani College, Kaushtee, Nagpur, India E-mail: dr.vinaychavan@yahoo.com

NO ACCESS

NITCO: an intelligent agent technique for optimising of resource utilisation in cloud

Harvinder Singh, Anshu Bhasin and Parag Ravikant Kaveri

Published Online: March 30, 2021 pp 69-75



ABOUT

Abstract

Efficient task scheduling is significant to meet the quality of service (QoS) requirements in cloud computing. Cloud is a large pool of virtual access resources to perform thousands of computational and storage operations. Task scheduling is an NP-hard problem, unsuitable matching leads to performance degradation and violation of service level agreement (SLA). The growing complexity of cloud services needs an extension of existing scheduling algorithms. In this paper, the scheduling problem has been explored based on growing application trends. Cloud dynamic resource provisioning can satisfy users' requirements if execution of tasks performed: identifying of task requirements; workflow of application scheduling using a sufficient amount of resources. In this research work, we present an intelligent agent technique for optimising resource utilisation named NITCO. NITCO considers the above mentioned challenge, identification of task requirements and configuration of resource. The performance of proposed NITCO has been evaluated on simulated cloud environment and comparison of results show that NITCO performed better in terms of execution cost, execution time, VM utilisation and SLA violation while it delivers quality of service.

Keywords

cloud computing, scheduling, utilisation, energy-consumption, service level agreement, SLA

[Previous Article](#)

HOD
Department of Computer Science & Engineering
J.K.G. P.T.U. Main Campus
Kapurthala

View article

E-I-I
Date

Capitulation of mitigation techniques of packet drop attacks in MANET to foreground nuances and ascertain trends

Author: Samdeep Singh, Anshu Srivastava, Anshu Kalia

Publication date: 2021/01/10

Journal: International Journal of Communication Systems

Volume: 34

Issue: 10

Pages: 14322

Description: MANET is a kind of wireless ad hoc network, in which mobile nodes operate in dynamic, distributed, and cooperative environment. Open nature of MANET makes it vulnerable to various kinds of attacks. Of these, the most severe are the packet drop attacks such as Blackhole attack, Cooperative Blackhole, and Grayhole attacks. The malicious nodes drop the packets as these packets are routed through them in accordance with the insider strategy of the particular packet drop attack, which adversely affects the network performance. A substantial amount of research papers focus on dealing with packet drop attacks in the last few years, but security is still an impending issue. In this paper, we have presented the systematic review of the literature of last 6 years on all varieties of packet drop attacks. We have classified these techniques into four categories: namely, mathematical based, monitoring based, network

Scholar articles: Capitulation of mitigation techniques of packet drop attacks in MANET to foreground nuances and ascertain trends
S Singh, A Srivastava, A Kalia - International Journal of Communication Systems, 2021
Related articles

ps

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

ANALYSIS AND DESIGN OF PROTOCOL FOR ENHANCED SELFISH ROUTING SCHEME

Raman Kumar

Department of Computer Science and Engineering
I K Gujral Punjab Technical University, Kapurthala, Punjab, India
er.ramankumar@aol.in

Abstract

The proposed routing mechanism in this paper has modified the conventional hello request and reply mechanism to include a new feature called power status. This feature keeps a node aware about the power status of neighboring nodes. Thus, the neighbor table of a node, in the proposed routing protocol, will have an additional entry in form of power status of the neighboring node. The knowledge about the power status of the neighbors helps a node in avoiding a node which is very low in power and may drop the packet in selfish manner to save the energy. A node in the ad hoc network can have five power statuses: very low, low, medium, high, very high with their ordinal values as 0, 1, 2, 3, 4 respectively.

Keywords: Average Power left per node, Average Throughput and Average no. of hop count for successful transmission

1. The Main Text

The Communication in an ad hoc network is a multihop communication wherein a source node communicates with a distant node using intermediate nodes to save the power. Thus, the major activity in an ad hoc network environment is to find a suitable route such that the delivery of the message is ensured beyond doubt. The route should be so chosen that all the nodes in the path are trustworthy, non-malicious, unselfish and the hop count is minimum.

The first receiver of the message to a distant node is some immediate neighbor of the source node. Therefore, it is necessary that every node in the ad hoc network must be aware of its immediate neighbors at every moment. To remain aware about its neighbor nodes, a node in the network keeps on broadcasting hello requests on the periodic basis and keeps on receiving the hello replies as well. Using these hello request and replies a node in the ad hoc network constructs and maintains a table of its neighbors known as neighbor table. Since the nodes in the ad hoc networks are mobile the neighbor table keeps on changing with time. Our proposal begins with the format for hello request packet as shown in Figure.1.

Packet Type	Source Address	Power Status
-------------	----------------	--------------

Figure 1 Hello Request Packet

The hello request packet has three fields, namely packet type, source address and power status. The packet type field denotes that it's a hello request packet, source address field is the identifier of the node in the network which generated the hello request and power status field indicates the current status of the power of the node issuing the hello request. There is no destination address in this packet as hello request is a broadcast mechanism.

Hello reply is multiple unicast mechanism wherein a node responds to the node from which it has received a hello request. The format of hello reply packet is shown in the Figure 2.

Packet Type	Source Address	Destination Address	Power Status
-------------	----------------	---------------------	--------------

Figure 2 Hello Reply Packet



PMME 2016

ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE AUDITING PROTOCOL FOR STORING DATA DYNAMICALLY IN CLOUD COMPUTING

Raman Kumar^a and Gurpreet Singh^b

^{a,b}Department of Computer Science and Engineering

^{a,b}D A V Institute of Engineering and Technology, Jalandhar, Punjab

^{a,b}er.ramankumar@aol.in

Abstract

The remote server (Cloud Service Provider (CSP)) store their data on cloud servers and users can access their data from cloud servers while implementing the concept of cloud computing. Because of some security constraints in data outsourcing, the latest concept of data hosting service also arises new security challenges, those challenges can be handled by third party auditing service to check the data integrity in the cloud server. There are few existing remote integrity checking methods those can serve for static stored data but not able to work dynamically. In this paper, we develop a three-tier security architecture for storing multimedia files which include role base access control, encryption, and signature verification. Therefore, an enhanced secure dynamic auditing protocol is proposed, which can store data correctly in the cloud. In the proposed scheme, both the combiner and the third party auditor (TPA) can verify the integrity of the information that they are receiving from each other. Therefore, the proposed an optimized secure dynamic auditing protocol is secure and efficient against various conspiracy attacks. © 2017 Elsevier Ltd. All rights reserved.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

Keywords: Cloud Computing, Communication overhead, Time cost of individual client, Packet delivery ratio, Energy level, Average delay, Packet delivery time and Throughput

1. Introduction

The cloud computing is a well nourishing paradigm. The NIST definition characterized on important aspects of cloud computing and broad comparisons of cloud computing services and deployment strategies. The service and formation models defined form a simple taxonomy not predetermined to constrain any particular method of implementation, service delivery, or business operation. The hybrid cloud management platform performs some

2214-7853© 2017 Elsevier Ltd. All rights reserved.

Selection and Peer-review under responsibility of International Conference on Processing of Materials, Minerals and Energy (July 29th – 30th) 2016, Ongole, Andhra Pradesh, India.

HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kanurthala



High-utility and diverse itemset mining

Amit Verma¹ · Siddharth Dawar² · Raman Kumar¹ · Shamkant Navathe³ · Vikram Goyal²

Accepted: 4 November 2020

© Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

High-utility Itemset Mining (HUIM) finds patterns from a transaction database with their utility no less than a user-defined threshold. The utility of an itemset is defined as the sum of the utilities of its items. The utility notion enables a data analyst to associate a profit score with each item and thereof to a pattern. We extend the notion of high-utility with diversity to define a new pattern type called High-utility and Diverse pattern (HUD). The notion of diversity of a pattern captures the extent of the different categories covered by the selected items in the pattern. An application of diverse-pattern lies in the recommendation task where a system can recommend to a customer a set of items from a new class based on her previously bought items. Our notion of diversity is easy to compute and also captures the basic essence of a previously proposed diversity notion. The existing algorithm to compute frequent-diverse patterns is 2-phase, i.e., in the first phase, frequent patterns are computed, out of which diverse patterns are filtered out in the second phase. We, in this paper, give an integrated algorithm that efficiently computes high-utility and diverse patterns in a single phase. Our experimental study shows that our proposed algorithm is very efficient as compared to a 2-phase algorithm that extracts high-utility itemsets in the first phase and filters out the diverse itemsets in the second phase.

Keywords Diverse patterns · Diversity measure · High-utility pattern mining

1 Introduction

Frequent pattern mining (FPM) and High-utility pattern mining (HUIM) are two widely studied techniques in the

area of data mining. The basic problem that these two techniques solve is as follows. Let D be a database of n transactions, and I be a set of all items. Each transaction consists of items from the set I , and each item in the transaction has associated with it a profit/utility score. A pattern $X \subseteq I$ (a high-utility or frequent pattern) having k items is referred to as k size pattern. For X to be a frequent pattern, the support of the pattern, $S(X)$, should be high in the database D . On the other hand, for X to be a high-utility pattern, its utility, $U(X)$ over the database, should be high, i.e., the utility of the pattern over the database is no less than the user-defined utility threshold. Wherein the utility of a pattern in each transaction is summed up to get the overall utility of the pattern.

The advantage of high-utility patterns is that it allows incorporating a notion of importance/relevancy with items. The notion of frequent-pattern considers the presence/absence of items and gives equal importance to each of them. This makes frequent pattern mining more restrictive and may not find patterns with high relevancy but having a low frequency. In particular, high-utility itemset mining (HUIM) can be used to identify sets of items that generates significant profit. The generalization to the utility can lead to new applications of itemset mining techniques firstly by

✉ Vikram Goyal
vikram@iiitd.ac.in

Amit Verma
verma0152@gmail.com

Siddharth Dawar
siddharthd@iiitd.ac.in

Raman Kumar
er.ramankumar@aol.in

Shamkant Navathe
sham@cc.gatech.edu

¹ Department of Computer Science and Engineering, IKGPTU, Kapurthala, Punjab, India

² Department of Computer Science, IIIT-Delhi, New Delhi, India

³ College Of Computing, Georgia Institute of Technology, Atlanta, Georgia, USA

Research Article

Edge-Based Convolutional Neural Network for Improving Breast Cancer Prediction Performance

Madhu  and Raman Kumar 

Department of Computer Science and Engineering, I K Gujral Punjab Technical University, Kapurthala, Punjab 144603, India

Correspondence should be addressed to Madhu; madhu.dahiya2588@gmail.com

Received 26 December 2020; Revised 23 February 2021; Accepted 19 June 2021; Published 13 July 2021

Academic Editor: Venkatesan Rajinikanth

Copyright © 2021 Madhu and Raman Kumar. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

There are many research studies in the field of breast cancer prediction, but it has been observed that the time taken for prediction needs to be reduced. The problem in the existing research is space consumption by graphical content. The proposed research is supposed to minimize the prediction time and space consumption. In this paper, research has focused on the study of existing breast cancer research and techniques and eliminating their limitation. It has been observed that when the number of datasets increases, every comparison makes a huge gap in size and comparison time. This research proposes a methodology for breast cancer prediction using an edge-based CNN (convolutional neural network) algorithm. The elimination of useless content from the graphical image before applying CNN has reduced the time consumption along with space consumption. The edge detection mechanism would retain only edges from the image sample in order to detect the pattern to predict breast cancer. The proposed work is supposed to implement the proposed methodology. A comparison of the proposed methodology and algorithm with the existing algorithm is made during simulation. The proposed work is found to be more efficient compared to the existing techniques used in breast cancer prediction. The utilization of proposed in the work area of medical science is supposed to enhance the capability in case of CNN at the time of decision-making. The proposed work is supposed to be more accurate compared to the existing works. It has been observed that the proposed work is fourteen to fifteen percent more accurate. It is taking 9/4 times less space and 1.0849004/0.178971 times less time compared to the general CNN model. Accuracy might vary as per size of the image and alteration performed in dataset of the image.

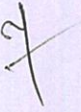
1. Introduction

There are several research studies on breast cancer detection [1]. Such research studies are beneficial to capture the symptoms of breast cancer in patients. Such type of research plays a significant role in predicting the probability of breast cancer [2]. The applications of CNN can be found in medical imaging since the 1990s.

“Transferability” is set in pretrained CNN. It is an important aspect of CNN [3]. According to earlier research, in the field of medical imaging, transfer learning has two parts. Initially, a pretrained system is used for the removal of qualities, and in a second group, remaining system has been applied as in the first one except that the logistic layer is used in place of a fully connected layer. Thus, in the present research, proposal of applying an edge detection mechanism

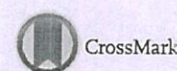
to enhance the efficiency in case of the previous convolutional neural network model has been illustrated. There have been limited works in the area of breast cancer [4] prediction model. This is because the nature of work is very complex. Research is considering CNN-dependent graphical processing to perform prediction of breast cancer [5].

Breast cancer has been considered a unique type of issue where cells of the breast get uncontrolled. Cancer stays nonaggressive until cells are not coming from the tubes [6]. Cancer may spread from the lymph glands. After that, it may spread to the other parts of the body. Mostly, it has been seen that breast cancer begins from ducts, which transfer the milk to the nipple. Such kind of cancer is referred to as ductal cancer. On the other hand, another kind of cancer [7] begins in the glands. Glands make the breast milk. It is lobular cancer. This type of disease also occurs in males. This disease


HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala



Improved shape matching and retrieval using robust histograms of spatially distributed points and angular radial transform



Pooja Sharma

Department of Computer Science and Applications, DAV University, Jalandhar, 144012, Punjab, India

ARTICLE INFO

Article history:

Received 9 June 2016

Received in revised form 26 April 2017

Accepted 30 April 2017

Keywords:

Histograms of spatially distributed points (HSDP)

Angular radial transform (ART)

Shape matching

Precision and recall

ABSTRACT

In this paper, the problem of shape based image retrieval is addressed by proposing a hybrid shape descriptor. The proposed descriptor conforms to human visual perception along with its low computational complexity. Since global features are related to the holistic characteristics of images, whereas local features describe the finer details within objects of images, in the proposed hybrid descriptor both global and local features of images are used to describe the entire aspects of image shape. For global features extraction, we use angular radial transform, which is also adopted by MPEG-7 as a region based shape descriptor. On the other hand, for local feature extraction, a novel local descriptor is proposed, which is referred to as histograms of spatially distributed points (HSDP). It is based on two components: radial distance and differential coefficient, which are used to build 2D histograms. Global and local features are combined using effective distance measures viz. Min-Max and Bray-Curtis. Their superiority is validated by experimental results. Apart from that, an extensive range of image databases is employed to assess the performance of the proposed hybrid descriptor. These databases represent several characteristics of shape such as partial occlusion, distortion, subject change, gray scale objects, rotated and noise affected objects, unstructured images, trademarks, blurred images, Corel images, etc. The results of wide range of experiments reveal that the fusion of ART and HSDP significantly improves the image retrieval accuracy and provides a robust and invariant solution for effective shape matching.

© 2017 Elsevier GmbH. All rights reserved.

1. Introduction

Effective image retrieval from large databases is a challenging task, which has not been completely solved yet. Relevance based image retrieval is applied to many applications such as medical imaging, trademark matching, digital library, computer aided design, military services, crime prevention, architectural and engineering design, geographical information, etc. Traditional image retrieval systems [1,2] were based on featuring the original data such as file name, note title, keywords, and indexing icon. However, textual annotations of images using keywords require intensive manual labor. When applied to large scale databases; these textual features become troublesome and time consuming. Besides; this method inadequately describes the image content; which does not meet the human visual perception exactly. In order to address these drawbacks; content based image retrieval (CBIR) systems have been proposed [3–9]. In CBIR; an image is generally represented by a set

E-mail addresses: sharma.pooja@live.com, pooja10013@davuniversity.org

Handwritten signature and stamp:
HOD
Department of Computer Science & Engineering
I.K.G. P.T.U. Main Campus
Kapurthala

Decision Tree based Classification and Dimensionality Reduction of Cervical Cancer

Diksha, Dinesh Gupta

Abstract: The data revolution in medicines and biology have increased our fundamental understandings of biological processes and determining the factors causing any disease, but it has also posed a challenge towards their analysis. After breast cancer, most of the deaths among women are due to cervical cancer. According to IARC, alone in 2012 a noticeable number of cases estimated 7095 of cervical cancer were reported. 16.5% of the deaths were due to the cervical cancer with the total deaths of 28,711 among women. To analyze the high dimensional data with high accuracy and in less amount of time, their dimensionality needs to be reduced to remove irrelevant features. The classification is performed using the recent iteration in Quinlan's C4.5 decision tree algorithm i.e. C5.0 algorithm and PCA as Dimensionality Reduction technique. Our proposed methodology has shown a significant improvement in the account of time taken by both algorithms. This shows that C5.0 algorithm is superior to C4.5 algorithm.

Keywords: Classification, Cervical Cancer, Decision Tree, Dimensionality Reduction.

I. INTRODUCTION

Cervical cancer is the preeminent causes of fatality among women of age 30 or above. Cervical cancer is a tumor of the cervix which is the lowermost part of uterus [1]. Human Papillomavirus (HPV) is the virus which is responsible for the cervical cancer [1]. When the body's cervical cells growth is malignant, the extra cells form a tumor. Mostly women have good immunity against HPV infection but if not, it can lead to cancer. Cervical cancer does not show any symptoms in the beginning. Regular check-ups are needed to diagnose it. But if the cancer has been diagnosed at early stages, it can be easily cured through various treatments. Size of the tumor is the key factor in deciding the type of treatment that is best fit for individual cases. Cervical cancer when left undiagnosed can lead to vaginal bleeding, pelvic pain, and unusual vaginal discharge. Various risk factors lead to cervical cancer. Some of them are smoking cigarettes, taking contraceptive pills for many years, weak immune system, having HIV. The chance of cervical cancer becomes higher with old age [2]. Cervical cancer can also unfold to more body parts in three ways through tissue, the liquid body substance system, and the blood. Several cancer deaths are caused once cancer moves from the first growth and spreads to alternative tissues and organs. This can be referred to as pathologic process cancer.

The 2010 WHO/ICO outline report states that girls aged 15 or above are prone to cervical cancer in Malaysia which has a population of 8.7 million of such girls. Annually, 631 out of 2126 girls suffering from cervical cancer die from the disease [3]. The American Cancer Society's estimates for cervical cancer in the U.S. for 2019 are [2] (1) Around 13,170 novel cases of cervical cancer will be analyzed, and (2) Around 4,250 women will expire from cervical cancer.

Many approaches have been proposed to detect the cervical cancer at early stages which are support vector machine (SVM), k-nearest neighbor, linear regression, and naive-bayes [1, 4]. Various dimensionality reduction techniques have been implemented in order to achieve low dimensional data space. The most common among the various used techniques is Principal Component Analysis (PCA). This algorithm is a useful statistical method which has its applications in various fields like speech recognition, image recognition [5, 6], text processing, and scientific data processing [7], and recommendation engines.

Rest of the paper is formulated as follows, Section II contains the introduction to dimensionality reduction, Section III contains some introduction to the classification, Section IV contains the related work, section V describes the proposed procedure with flow chart, Section VI interpret results, and Section VIII concludes research work with future directions

II. DIMENSIONALITY REDUCTION

The growth in data increases the sparsity in the data and unnecessarily increases storage space and processing time to analyze and classify the data. This is termed as Curse of Dimensionality. Value brought by way of extra size is plenty smaller in comparison to overhead it adds to the algorithm. To reduce the overhead of higher dimensionality, researchers often extract specific attributes (i.e. features) that are relevant in drawing the results by scaling down the dimensionality of the data.

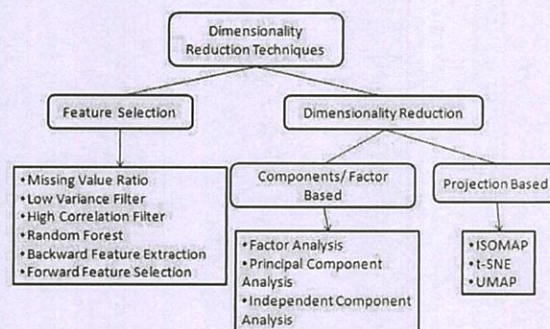


Figure 1: Dimensionality Reduction Techniques

Revised Manuscript Received on March 30, 2020.

* Correspondence Author

Diksha*, Department of Computer Science and Engineering, IKG Punjab Technical University, Jalandhar, India. Email: dikshaaggarwal100@gmail.com

Dinesh Gupta, Department of Computer Science and Engineering, IKG Punjab Technical University, Jalandhar, India. Email: dineshgupta@ptu.ac.in