Global Journal

of Computer Science and Technology: E

Network, Web & Security

Energy Consumption

Multi-Channel Scheduling

Highlights

Decision Support System

A Review on Internet of Things

Discovering Thoughts, Inventing Future

Volume 16 Issue 7 Version1.0

Global Journal of Computer Science and Technology: E
Network, Web & Security

Global Journal of Computer Science and Technology: E
Network, Web & Security

Volume 16 Issue 7 (Ver. 1.0)

Open Association of Research Society

Incorporation No.: 0423089
License No.: 42125/022010/1186
Registration No.: 430374
Import-Export Code: 1109007027
Employer Identification Number (EIN):
USA Tax ID: 98-0673427

Global Journals Inc.

*(A Delaware USA Incorporation with "Good Standing"; **Reg. Number: 0423089**)*

Sponsors: *Open Association of Research Society*
Open Scientific Standards

Publisher's Headquarters office

Global Journals® Headquarters
945th Concord Streets,
Framingham Massachusetts Pin: 01701,
United States of America
USA Toll Free: +001-888-839-7392
USA Toll Free Fax: +001-888-839-7392

Offset Typesetting

Global Journals Incorporated
2nd, Lansdowne, Lansdowne Rd., Croydon-Surrey,
Pin: CR9 2ER, United Kingdom

Packaging & Continental Dispatching

Global Journals
E-3130 Sudama Nagar, Near Gopur Square,
Indore, M.P., Pin: 452009, India

Find a correspondence nodal officer near you

To find nodal officer of your country, please email us at *local@globaljournals.org*

eContacts

Press Inquiries: *press@globaljournals.org*
Investor Inquiries: *investors@globaljournals.org*
Technical Support: *technology@globaljournals.org*
Media & Releases: *media@globaljournals.org*

Pricing (Including by Air Parcel Charges):

For Authors:
22 USD (B/W) & 50 USD (Color)
Yearly Subscription (Personal & Institutional):
200 USD (B/W) & 250 USD (Color)

Global Journals Constitutional Editorial Board

~Integrated~

Dr. Xiaohong He

Professor of International Business

University of Quinnipiac

BS, Jilin Institute of Technology; MA, MS, Ph.D,

(University of Texas-Dallas)

Web: quinnipiac.edu/x1606.xml

Dr. T. David A. Forbes

Associate Professor and Range Nutritionist

Ph.D Edinburgh University - Animal Nutrition

M.S. Aberdeen University - Animal Nutrition

B.A. University of Dublin- Zoology.

Web: essm.tamu.edu/people-info/faculty/forbes-david

Dr. Burcin Becerik-Gerber

University of Southern Californi

Ph.D in Civil Engineering

DDes from Harvard University

M.S. from University of California, Berkeley

M.S. from Istanbul Technical University

Web: i-lab.usc.edu

Dr. Bassey Benjamin Esu

B.Sc. Marketing; MBA Marketing; Ph.D Marketing

Lecturer, Department of Marketing, University of Calabar

Tourism Consultant, Cross River State Tourism Development Department

Co-rdinator , Sustainable Tourism Initiative, Calabar, Nigeria

Dr. Söhnke M. Bartram

Department of Accounting and Finance

Lancaster University Management School

Ph.D. (WHU Koblenz)

MBA/BBA (University of Saarbrücken)

Web: lancs.ac.uk/staff/bartras1/

Dr. Maciej Gucma

Asistant Professor,

Maritime University of Szczecin Szczecin, Poland

Ph.D. Eng. Master Mariner

Web: www.mendeley.com/profiles/maciej-gucma/

Dr. Söhnke M. Bartram

Ph.D, (IT) in Faculty of Engg. & Tech.

Professor & Head,

Dept. of ISE at NMAM Institute of Technology

Dr. Shun-Chung Lee

Department of Resources Engineering,

National Cheng Kung University, Taiwan

Dr. Balasubramani R

Department of Accounting and Finance

Lancaster University Management School

Ph.D. (WHU Koblenz)

MBA/BBA (University of Saarbrücken)

Web: lancs.ac.uk/staff/bartras1/

Dr. Fotini Labropulu

Mathematics - Luther College, University of Regina

Ph.D, M.Sc. in Mathematics

B.A. (Honours) in Mathematics, University of Windsor

Web: luthercollege.edu/Default.aspx

M. Meguellati

Department of Electronics,

University of Batna, Batna 05000, Algeria

Dr. Vesna Stanković Pejnović

Ph. D. Philospohy , Zagreb, Croatia

Rusveltova, Skopje, Macedonia

Contents of the Issue

i. Copyright Notice
ii. Editorial Board Members
iii. Chief Author and Dean
iv. Contents of the Issue

1. A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches. *1-9*
2. Automock: Automated Mock Backend Generation for Javascript based Applications. *11-18*
3. The Wireless Body Area Sensor Networks and Routing Strategies: Nomenclature and Review of Literature. *19-30*
4. Securing Cluster Head Selection in Wireless Sensor Networks. *31-40*
5. Multi-Channel Scheduling with Optimal Spectrum Channel Hole Filling (MCS-OSHF) for Cognitive Radio Wireless Networks. *41-47*
6. ECARDM: Energy Consumption Aware Route Discovery for Multicasting in Mobile Ad hoc Networks. *49-56*
7. Webgis based Decision Support System for Disseminating Nowcast based Alerts: Opengis Approach. *57-64*

v. Fellows
vi. Auxiliary Memberships
vii. Process of Submission of Research Paper
viii. Preferred Author Guidelines
ix. Index

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches

By Muhammad A. Iqbal, Oladiran G.Olaleye & Magdy A. Bayoumi
University of Louisiana at Lafayette

Abstract- The world is undergoing a dramatic rapid transformation from isolated systems to ubiquitous Internet-based-enabled 'things' capable of interacting each other and generating data that can be analyzed to extract valuable information. This highly interconnected global network structure known as Internet of Things will enrich everyone's life, increase business productivity, improve government efficiency, and the list just goes on. However, this new reality (IoT) built on the basis of Internet, contains new kind of challenges from a security and privacy perspective. Traditional security primitives cannot be directly applied to IoT technologies due to the different standards and communication stacks involved.

Keywords: internet of things (IOT), security, privacy issues, wireless sensor networks, RFID, authentication, key management.

GJCST-E Classification: C.2.0 K.4.1

Strictly as per the compliance and regulations of:

A Review on Internet of Things (Iot): Security and Privacy Requirements and the Solution Approaches

Muhammad A. Iqbal [α], Oladiran G. Olaleye [σ] & Magdy A. Bayoumi [ρ]

Abstract- The world is undergoing a dramatic rapid transformation from isolated systems to ubiquitous Internet-based-enabled 'things' capable of interacting each other and generating data that can be analyzed to extract valuable information. This highly interconnected global network structure known as Internet of Things will enrich everyone's life, increase business productivity, improve government efficiency, and the list just goes on. However, this new reality (IoT) built on the basis of Internet, contains new kind of challenges from a security and privacy perspective. Traditional security primitives cannot be directly applied to IoT technologies due to the different standards and communication stacks involved. Along with scalability and heterogeneity issues, major part of IoT infrastructure consists of resource constrained devices such as RFIDs and wireless sensor nodes. Therefore, a flexible infrastructure is required capable to deal with security and privacy issues in such a dynamic environment. This paper presents an overview of IoT, security and privacy challenges and the existing security solutions and identifying some open issues for future research.

Keywords: internet of things (IOT), security, privacy issues, wireless sensor networks, RFID, authentication, key management.

I. Introduction

The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it". This was Mark Weiser's central statement in his seminal paper [Weis 91] in Scientific American in 1991. IoT concept has begun to shape our modern world including a common man's everyday life in the society, a world in which devices of every shape and size are manufactured with "smart" capabilities that allow them to communicate and interact not only with other devices but also with humans, exchange their data, make autonomous decisions and perform useful tasks based on preset conditions. IoT is becoming well-known concept across many horizontal and vertical markets with its numerous applications [1].Just to give an example how IoT would affect our daily life: You enter the supermarket and receive your fridge's text message: "You are out of milk." In the dairy section, sensors signal your grocery cart that you've taken a milk carton. As you walk towards the pharmacy, your fitness wristband vibrates as it takes your vitals and streams the results to your doctor to adjust your prescription. When you're finished shopping, you simply walk out the door. Your credit card is charged when you exit the supermarket's geofence. As you drive home, your car communicates with other cars on the roadway to prevent accidents.

The early years of Internet of Things (IoT) started with Machine to Machine (M2M) communication. M2M communication indicates two machines communicating with each other, usually without human involvement. The communication platform is not defined, and can be both wireless and wired communication. The term M2M stems from telephony systems. In these systems, different endpoints needed to exchange information between each other, such as the identity of the caller. This information was sent between the endpoints without a human being needed to initiate the transmission. The M2M term is still very much in use, especially in the industrial market, and is commonly regarded as a subset of IoT [5].

The term internet of things was devised by Kevin Ashton, cofounder and executive director of Auto-ID Center at MIT in 1999 and refers to uniquely identifiable objects and their virtual representations in an "internet-like" structure [25]. The Oxford Dictionary perhaps offers a concise definition that invokes the Internet as an element of the IoT:

Internet of things (noun): The interconnection via the Internet of computing devices embedded in everyday objects enabling them to send and receive data.

Nevertheless, in the past decade, this concept has been extended because of new IoT network applications such as e-healthcare and transport utilities [25]. The evolution of the IoT has its origin in the convergence of wireless technologies, advancements of micro electromechanical systems (MEMS) and digital electronics where has been as a result miniature devices with the ability to sense and compute and communicate wirelessly. In the era of IoT, the interaction or relationship between humans and machines is ever more considered as machines getting smarter and starting to handle more human tasks, and in this situation humans

Author α σ: The Center for Advanced Computer Studies, University of Louisiana at Lafayette, LA 70504 USA working in the area of security for Internet of Things, Wireless Sensor Networks and Cognitive Radio Networks. e-mail: mxi1678, ogo8842@cacs.louisiana.edu

Author ρ: Dr. Magdy Bayoumi is Professor at The Center for Advanced Computer Studies, University of Louisiana at Lafayette, LA 70504 USA. e-mail: mab@cacs.louisiana.edu

are required to trust the machine and feel safe. In this way, a thing might be a patient with a medical implant to facilitate real-time monitoring in a healthcare application or an accelerometer for movement attached to the cow in a farm environment [26].

These things or devices in IoT include familiar scannables and wearables and more complex systems like home appliances, vehicles, and smart roads and bridges. It is predicted that IoT will consist of 50 billion connected devices by 2020 and that the worldwide IoT market will be more than a $10 trillion industry. These projections depict the possibility of a smarter, efficient and safer world of inter-connected devices [27] while some observers show concerns that the IoT represents a darker world of surveillance, privacy and security violations, and consumer lock–in. Attention-grabbing headlines about the hacking of internet-connected automobiles, surveillance concerns arising from voice recognition features in "smart" TVs, and privacy fears stemming from the potential misuse of IoT data have captured public attention. This "promise vs. peril" debate along with an influx of information though popular media and marketing can make the IoT a complex topic to understand [22].

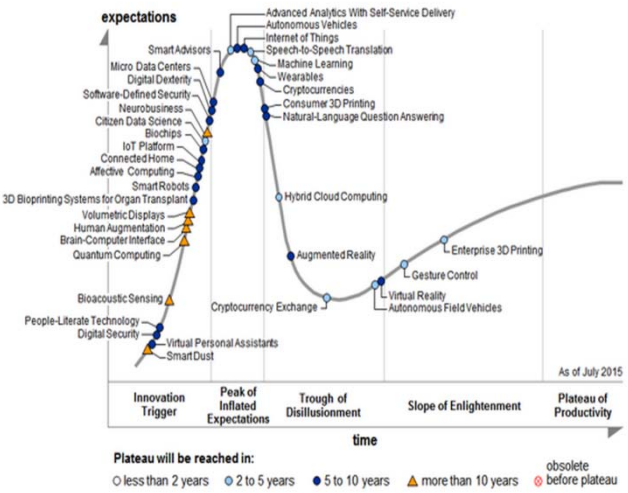

Figure 1: Hyper Cycle for Emerging Technologies, 2105[12]

Garter's Hype Cycle is a way to represent emergence, adoption, maturity and impact on applications of specific technologies. The latest Gartner Hype Cycle for Emerging Technologies places it at the peak. IoT has been identified as one of the emerging technologies as shown below in the Hype Cycle in Emerging Technologies Report for the year 2015[28].

II. Security for Internet of Things

If one thing can prevent the Internet of things from transforming the way we live and work, it will be a breakdown in security. While security considerations are not new in the context of information technology, the attributes of many IoT implementations present new and unique security challenges. Addressing these challenges and ensuring security in IoT products and services must be a fundamental priority. Users need to trust that IoT devices and related data services are secure from vulnerabilities, especially as this technology become more pervasive and integrated into our daily lives. Important challenge is the integration of security mechanisms and the user acceptance. User must feel that they control any information that is related to them rather than they feel they are being controlled by the system. This integration generates new requirements, not been previously considered.

The interconnected nature of IoT devices means that every poorly secured device that is connected online potentially affects the security and resilience of the Internet globally. This challenge is amplified by other considerations like the mass-scale deployment of homogenous IoT devices, the ability of some devices to automatically connect to other devices, and the likelihood of fielding these devices in unsecure environments. As a matter of principle, developers and users of IoT devices and systems have a collective obligation to ensure they do not expose users and the IoT infrastructure itself to potential harm. Accordingly, a collaborative approach to security will be needed to develop effective and appropriate solutions to IoT security challenges that are well suited to the scale and complexity of the issues [22].

Full potential of the IoT depends on strategies that respect individual privacy choices across a broad spectrum of expectations. The data streams and user specificity afforded by IoT devices can unlock incredible and unique value to IoT users, but concerns about privacy and potential harms might hold back full

adoption of the Internet of Things. This means that privacy rights and respect for user privacy expectations are integral to ensuring user trust and confidence in the Internet, connected devices, and related services. Indeed, the Internet of Things is redefining the debate about privacy issues, as many implementations can dramatically change the ways personal data is collected, analyzed, used, and protected. For example, IoT amplifies concerns about the potential for increased surveillance and tracking, difficulty in being able to opt out of certain data collection, and the strength of aggregating IoT data streams to paint detailed digital portraits of users. While these are important challenges, they are not insurmountable. In order to realize the opportunities, strategies will need to be developed to respect individual privacy choices across a broad spectrum of expectations, while still fostering innovation in new technology and services [22].

The remainder of this paper is organized as follows: Section II further gives an overview of the IoT features, layers; we first identify properties that make the IoT unique in terms of the security and privacy challenges. In the next section, we describe the security primitives and solutions approaches that take into account to secure the network communication and protect user's data. Finally, Section IV concludes the paper and gives insights regarding current research gaps and possible future directions.

a) IoT Features And Security Requirements

In this section, we identify the features that constitute the uniqueness of the IoT in terms of the security and privacy challenges and the layers of IoT. We will see how security issues are different in IoT as compared to traditional internet networks. Moreover, we will establish a number of security and privacy requirements, based on the described properties, and will discuss them in detail.

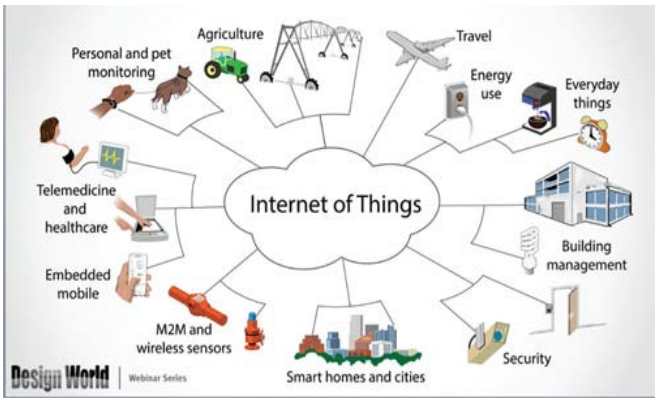

Figure 2: Internet of Things Applications

In contrast to traditional IT systems such as enterprise applications, cloud computing, and big data, a combination of a number of properties makes the IoT unique in terms of the challenges that need to be coped with. We identify these properties by analyzing related IoT research [29]–[30]. A major barrier to realizing the full promise of IoT is that around 85% of existing things were not designed to connect to Internet and cannot share data with the cloud according to IMS research. Addressing this issue, gateways from mobile, home, and industrial act as intermediaries between legacy things and the cloud, providing the needed connectivity, security and manageability described by Intel.

The identified distinguishing properties are four, namely: the uncontrolled environment, the heteroge- neity, the need for scalability, as well as the constrained resources utilized in the IoT

Uncontrolled Environment: Many things will be part of a highly uncontrolled environment; things travel to untrustworthy surroundings, possibly without supervision. Sub properties of the uncontrolled environment

Mobility: Stable network connectivity and constant presence cannot be expected in such an environment. Physical Accessibility: In the IoT, sensors can be publicly accessible, e.g., traffic control cameras, and environmental sensors.

Trust: A priori trusted relationships are unlikely for the large amount of devices interacting with each other and users [22]. Thus, automated mechanisms to measure and manage trust of things, services, and users are crucial for the IoT.

Heterogeneity: IoT is expected to be a highly heterogeneous ecosystem as it will have to integrate a multitude of things from various manufacturers. Therefore, version compatibility, and interoperability have to be considered.

Scalability: The vast amount of interconnected things in the IoT demands highly scalable protocols. This also has an influence on security mechanisms. For instance, centralized approaches, e.g., hierarchical Public Key Infrastructures (PKIs), as well as some distributed approaches, e.g., pairwise symmetric key exchange schemes, cannot scale with the IoT.

Infrastructures (PKIs), as well as some distributed approaches, e.g., pairwise symmetric key exchange schemes, cannot scale with the IoT.

Constrained Resources: Things in the IoT will have constraints that need to be considered for security mechanisms. This includes energy limitations, e.g., battery powered devices, as well as low computation power, e.g., micro sensors. Thus, heavy computational cryptographic algorithms cannot be applied to all things. IoT and traditional network security issues are different in many ways. IoT is composed of RFID nodes and WSN nodes, whose resources are limited, while the Internet is composed of PC, severs, smart phones whose resources are rich. In the Internet, we use combinations of complex algorithms and lightweight algorithms to maximize security with less considerations of resource usage such as computation power. While in IoT, most of the cases, we can only use lightweight algorithms to find the balance between security and power consumptions. Connection between IoT nodes are always through slower, less secure wireless media, which results in easy data leakage, easily node compromising and all other insecure issues. Whereas in Internet, most communications are through faster, more secure wire or wireless communications. Even with the Mobile Internet, wireless connections are built on top of complex secure protocols which are almost impossible to implement for resource limited IoT nodes.

Although there are various devices in the Internet, but with the abstraction of operating system, their data formats are almost the same with Window Family and Unix-like operating systems. However, in IoT, what we have is just bare wireless node. There is no operating system, just a simple embedded program for the chip. With the diversity of nodes perception goal, there comes different chip hardware which result in heterogeneous data contents and data formats. There are all kinds of IoT applications in application layer, used in our everyday life; they gather our private information every second automatically to make our life easier. These applications can even control our everyday life environment. It would be of great potential security problems if we lose control of IoT system. While in the Internet, if we do not provide our information ourselves, there is no way for attackers to get our information. And with the help of operating system and plenty of security software, the environment is more secure.

So in one word, IoT system lives in a more dangerous environment with limited resources and less network guards. So we need to implement lightweight solutions to deal with this more dangerous environment.

b) Internet of Things Layers

In order to analyze the security issues of IoT in more detail, IoT layers are divided into perception layer, transportation layer and application layer. Perception layer can further be divided into perception nodes and perception network, divide transportation layer into access network, core network, and LAN, and the application layer into application support layer and IoT applications.

Each layer has a corresponding technical support, these technologies at all levels play irreplaceable roles, but these techniques are more or less related to the existence of the range problems that can cause insecurity, privacy and other security issues of data. IoT must ensure the security of all layers. In addition, IoT security should also include the security of whole system crossing the perception layer, transportation layer and application layer.

- Perception layer includes RFID security, WSNs security, RSN security and any others.
- Transportation layer includes access network security, core network security and local network security. There are 3G access network security, Ad-Hoc network security, WiFi security and so on for these sub layers. Different network transmission has different technology.
- Application layer includes application support layer and specific IoT applications. The security in support layer includes middleware technology security, cloud computing platform security and so on. IoT applications in different industries have different requirements.

Perception layer is mainly about information collection, object perception and object control. Perception Network that communicates with transportation network. Perception node is used for data acquisition and data control, perception network sends collected data to the gateway or sends control instruction to the controller. Perception layer technologies include RFID, WSNs, RSN, GPS, etc.

c) LOT Security and Privacy Requirements

Security and privacy are crucial enabling technologies and thus among the biggest challenges for the IoT [31]. Therefore, it is compelling for the IoT architectures to consider and resolve these challenges upfront. Otherwise, applications as well as whole ecosystems building on top of such architectures may repeat the security fallacies of the past decades. For that, a precise understanding of security requirements in the context of the IoT is indispensable.

Prior technology trends, e.g., cloud computing and big data, are likely to share security requirements with the IoT. However, the uniqueness of the IoT introduces new challenges to security requirements, different from previous technology trends. Big data solutions for instance are designed to scale and deal with heterogeneity of data sources. Nevertheless, big data solutions are not required to deal with an uncontrolled environment and constrained resources; big data analytics run in isolated silos with time or resources to spare. Likewise, cloud computing by

design is supposed to scale and overcome challenges of constrained resources. However, cloud computing hardly deals with mobility of devices and physical accessibility of sensors. Related IoT security surveys are incomplete with respect to requirements. To provide a comprehensive overview, we summarize these security requirements from the domain of the IoT and split them into five groups: Network Security, Identity Management, Privacy, Trust, and Resilience. It is obvious that with regard to network security the constrained resources should have the strongest connection, mainly due to the restrictions that they apply to traditional security mechanisms, e.g., cryptography. Moreover, identity management is influenced by the heterogeneity of the IoT. Privacy is mostly connected with scalability and the constrained resources as restrictions are posed to the technology candidates that can be utilized. Furthermore, the uncontrolled environment and the heterogeneity of the IoT have a serious impact on trust. Lastly, resilience is directly connected to the need of the IoT for scalability [23].

Network Security: Network security requirements are divided into confidentiality, authenticity, integrity, and availability [34]. Factors like heterogeneity and constrained resources must be considered while applying these to IoT architectures. Interconnecting the devices require to have better confidentiality so technologies such as IPSec [35] and Transport Layer Security (TLS) [33] are employed to meet this requirement. There's another dedicated secure network stacks of IoT available in case overhead exceeds the resource constraints of things [32]. Authenticity confirms that the connection established is with an authenticated entity and authenticity also includes integrity of data but can be required separately to detect and recover failures so mechanisms such as TCP and TLS suffice this requirement.

Privacy: Privacy is considered to be one of main challenges in IoT [24] due to the involvement of humans and increasingly ubiquitous data collection. Privacy of data includes confidential data transmission in a way that it shouldn't expose undesired properties, e.g. identity of a person. This requirement is considered as big challenge as almost every other sensing device collect personal information and large amount of such data becomes Personally Identifiable Information (PII) when combined together; enough to identify a person [38].

A single person not being identifiable as the source of data or an action is anonymity, another challenge to face in IoT as mobile devices and wearable sensors may leak PII such as IP addresses and location unknowingly. There are some technologies already being employed such as anonymous credentials and onion routing, though may not scale well with IoT. Unlinkability protects from profiling in the IoT while pseudonyms may solve unlink ability. With pseudonymity, actions of a person are linked with a pseudonym, a random identifier, rather than an identity [23].

Intel Security also announced, its Enhanced Privacy Identity (EPID) technology will be promoted to other silicon vendors. EPID has anonymity properties, in addition to hardware-enforced integrity, and is included in ISO and TCG standards. The EPID technology provides an on-ramp for other devices to securely connect to the Intel IoT Platform [1].

Identity Management: A comprehensive attention should be given for identity management in IoT due to the number of devices and the complex relationship between devices, services, owners and users [38]. Methods for authentication, authorization including revocation, and accountability or non-repudiation are required. There may be multiple domain scenarios in IoT, authorization solutions, e.g., Kerberos [13], assume a single domain that encloses devices, owners, users, and services. Therefore, new authorization solutions that work with un-trusted devices, allow delegation of access across domains, and capable of quick revocation are needed. Accountability in trust management ensures that every action is clearly bound to an authenticated entity, is another challenge in IoT. It must be capable to deal with huge amounts of entities, delegation of access, actions that span organizational domains along with continuous derivation of data.

Resilience: Resilience and robustness against attacks and failures becomes another important challenge due to large scale of devices. IoT architectures must provide mechanisms to proficiently select things, transmission paths, and services according to their robustness (failure/attack avoidance). Also, fail-over and recovery mechanisms must be provided to maintain operations under failure or attacks, and to return to normal operations [2].

d) Cryptographic Primitives Goals and Attack Techniques

Cryptographic primitives are in general utilized to comply with the main security goals for exchanged messages and the system itself [3].

Main security requirements are

Confidentiality: message only disclosed to authorized entities

Integrity: Original message is not tempered
Authenticity: message is sent from a genuine entity
Availability: system keeps serving its purpose and stays uninterruptedly available for legitimate entities
It is also important to understand the attack techniques in order to rationalize security mechanisms in communication protocols. Some important attacks with respect to IoT are: *Eavesdropping:* process of

overhearing an ongoing communication, i.e. is as well preliminary for launching next attacks. In wireless communication, everyone has in general access to the medium so takes less effort to launch as compared to wired communication. Confidentiality is a typical counter-measurement against eavesdropping but if keying material is not exchanged in secure manner, eavesdropper could compromise the confidentiality. Secure key exchange algorithms such as Diffe-Hellman (DH) are used.

Impersonation: a malicious party pretends to be a legitimate entity for instance by replaying a generic message, in order to bypass the aforementioned security goals.

MITM Attack: Man-in-the-middle attack takes place when a malicious entity is on the network path of two genuine entities. Capable of delaying, modifying or dropping messages. Interesting within the context of PKC, malicious entity doesn't attempt to break the keys of involved parties but rather to become the falsely trusted MITM.

DoS Attack: targets the availability of a system that offers services, is achieved by exhaustingly consuming resources at the victim so that the offered services become unavailable to legitimate entities. A common way to launch this attack is to trigger expensive operations at the victim that consume resources such as computational power, memory bandwidth or energy. This attack is critical for constrained devices where existing resources are already scarce.

III. Internet of Things Security Solutions Approaches

Different approaches are being employed for secure End-to-End communication in WSNs and IoT, they can be classified into major research directions as follows

- Centralized Approaches
- Protocol-based Extensions and Optimizations
- Alternative Delegation Architectures
- Solutions that Require Special Purpose Hardware Modules

a) Centralized Approaches

Centralized security solution approaches are considered as efficient and suitable for the resource-constrained sensor networks but the common issue is the scalability of the key management; node must be pre-configured with shared keys of all entities before deployment. Some of the common centralized based approaches are SPINS (A centralized architecture for securing uni- and multicast communication in constrained networks, composed of two security protocols; SNEP and μTESLA) and the Polynomial-based scheme (Polynomial schemes aim at simplifying the key agreement process in distributed sensor networks, main idea is to assign every node n a polynomial share F(n; y) derived from a secret symmetric bi-variate polynomial F(x; y). This allows any possible pair of nodes with a polynomial share to be able to establish a common secret) [3].

b) Protocol-based Extensions and Optimizations

Approaches such as compression aim at optimizing the protocol without breaking the security properties. There are several compression schemes proposed such as the compression of IPV6 header, extension headers, and UDP (User Datagram Protocol) header now standard in 6LoWPAN. Some of these approaches are Abbreviated DTLS Handshake (allows for a shorter handshake that reuses the state information from the previous session, in order to resume the session). TLS Session Resumption without Server-Side State where server does not hold any state required to resume a session rather server's encrypted state is offloaded during the handshake towards the client and in caching, TLS Cached Information extension allows for omitting cached information, such as these large certificate chains from the handshake. Compression of header information is an approach to reduce the transmission overhead of packets in constrained environments, 6LoWPAN defines already header compression mechanism for IP packets.

c) Delegation-based Architectures

Delegate computationally intensive tasks, such as public-key-based operations involved in session establishments, to more powerful devices. Some important approaches are:

Server-based Certificate Validation Protocol (SCVP), it enables a client to delegate the complex task of certificate validation or certificate path construction to a trusted server. SCVP server should be trusted.

Another delegation approach: by Bonetto [4]. It delegates the public-key-based operations to a more powerful device, such as the Gateway (GW). They describe the procedure for IKE session establishment, where the GW intercepts session establishment and pretends to be the end-point. After calculation of the session key, this key is handed over the constrained device and both peers can directly protect their communication with the session key. But in the vision of IoT, not always a trusted GW is present e.g. in the home automation scenario, constrained devices of different manufacturers might be present in the constrained network.

Tiny 3-TLS [6]: It requires a strong trust level between the constrained resource device and the GW, offloads expensive public-key-based operations to the GW. The constrained resource device trusts the GW and the unconstrained device authenticates itself to the GW and hence, GW trusts the unconstrained device.

constrained resource device trusts the GW and the unconstrained device authenticates itself to the GW and hence, GW trusts the unconstrained device.

Consequently, Tiny 3-TLS assumes that by means of transitive trust the constrained device could trust the unconstrained device. Tiny 3-TLS distinguishes between partially and fully trusted GWs.

Sizzle [7] implements a complete SSL-secured HTTP web server for constrained devices with support for ECC-based authentication. This approach, in contrast to previous delegation-based architectures, delegates only the task of adapting the underlying transport-layer protocol. This is achieved by terminating the incoming TCP connection at the GW and sending the payload via a UDP-based reliable protocol to the constrained device. Sizzle only allows for certificate-based authentication towards powerful clients and does not implement certificate handling for constrained devices.

Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks in the context of Internet of Things (IoT). Symmetric key cryptography such as AES provides fast and lightweight encryption and decryption on smart devices and their integrated hardware supports it as well. However, when number of devices connected becomes high, exchanging symmetric keys becomes a challenging task and an efficient scalable key establishment protocol is required. Asymmetric key cryptography is another method for key establishment at two ends, but it involves high computational overheads which are the main concerns for resource-constrained devices [9]. Sensors with low resources (energy, computation) are not meant to perform complex asymmetric cryptographic operations.

Key establishment protocols are used to provide shared secrets between two or more parties, typically for subsequent use as private keys for a variety of cryptographic objectives [12]. These objectives are in turn used as security primitives for enabling various security protocols such as source authentication, integrity protection or confidentiality [8]. To afford interoperable network security between endpoints from independent network domains, variants of traditional End-to-End IP security protocols have recently been proposed for resource-constrained devices and the networks formed by them [9].

- Protocol variants such as Datagram Transport Layer Security (DTLS) [14], HIP-DEX [15], and minimal IKEv2 [16] consider public-key cryptography in their protocol design. As public-key cryptography acquires significant computational processing and transmission overheads in resource-constrained network environments, research and standardization currently focuses to reduce the public-key related overheads during the protocol handshake.
- Another interesting approach has been suggested in [20] and [8]. In these papers, a proxy-based solution is proposed to delegate the heavy cryptographic operations from a resource-constrained device to less constrained nodes. A similar approach might be found in [11] for ambient-assisted living and also in [21] where communication is made from one resource-constrained node to another resource-constrained sensor node. These approaches have assumed the sensor nodes to be trustworthy and the mechanism in case if nodes are compromised, misbehave, authentication fails or nodes fail to deliver its assigned share. Still the risk involved is there for the secret shared key to be revealed by the attacker from the compromised nodes. Selection criteria are described for these assisting nodes to evaluate their abilities before they are assigned computational tasks to work as proxies.

Other approaches proposed including session resumption mechanisms [17] and caching of static handshake information such as certificates [18]. However, the considerable RAM and ROM requirements make the use of public-key cryptography unsuitable for a wide range of constrained devices [9]. One such implementation of two-way authentication scheme for the IoT based on DTLS protocol is described in [19]. This approach even generates considerable overheads to the network traffic due to the utilization of X.509 certificates and RSA public keys with DTLS handshake. Both these X.509 certificate and RSA public key with DTLS handshake involve heavy computations for the low performing and high resource-constrained sensor nodes.

d) Hardware-based Approaches

A class of security solutions relies on additional hardware security modules, such as TPMs. A Trusted Platform Module (TPM) is tamper-proof hardware that provides support for cryptographic computations especially public-key-based cryptographic primitives. TPMs can hold keys, such as RSA private keys, in a protected memory area. Furthermore, the cryptographic accelerator of TPMs is capable of

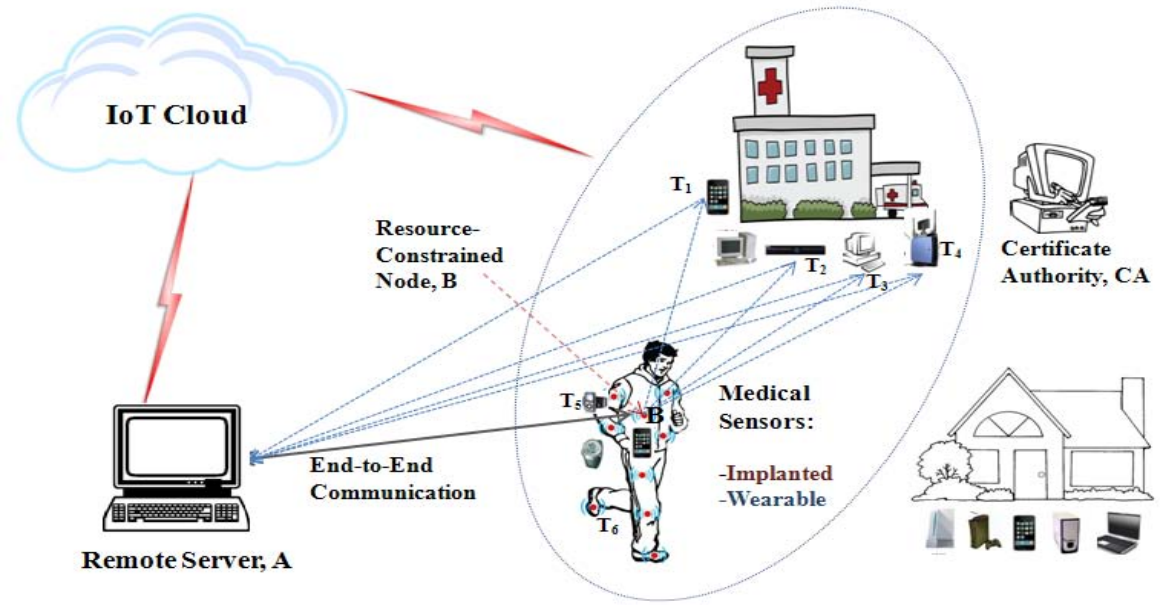

Figure 2: Network Model Scenario for Body Area Network in the context of Internet of Things (IoT)

computing the cryptographic computations with a higher performance. In contrast, ECC provides the same level of security with considerably smaller key sizes [3]. Therefore, ECC is preferred and recommend for constrained environments.

IV. Conclusion

This paper aims to provides the reader a basic overview about Internet of Things, the major security and privacy challenges because of its exponential growth and what kind of security primitives and solution approaches are being taken to make communication secure and to protect the user's data. Conventional security primitives cannot be applied due to the heterogeneous nature of sensors, low resources and the system architecture in IoT applications. To prevent unauthorized use of user's data, protect their privacy and to mitigate security and privacy threats, strong network security infrastructures are required. Peer authentication and End-to-End data protection are crucial requirements to prevent eavesdropping on sensitive data or malicious triggering of harmful actuating tasks. Any unauthorized use of data may restrict users to utilize IoT based applications. This review paper provides the security solution approaches been proposed recently identifying both the challenges related to security and privacy and the attack techniques used to compromise/fail the sensor nodes in Internet of Things as well. Current approaches are focused on pre-deployed, pre-shared keys on both ends whereas certificate-based authentication is generally considered infeasible for constrained resource sensors. New security paradigm are needed for End-to-End secure key establishment protocols that are lightweight for resource-constrained sensors and secure through strong encryption and authentication.

References Références Referencias

1. Somayya Madakam, R. Ramaswamy, Siddharth Tripathi "Internet of Things (IoT): A Literature Review"
2. Emmanouil Vasilomanolakis, Jorg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaie and Panayotis Kikiras "On the Security and Privacy of Internet of Things Architectures and Systems"
3. Hossein Shafagh (2013) "Leveraging Public-key-based Authentication for the Internet of Things" Master Thesis, RWTH Aachen University, Germany
4. R. Bonetto, N. Bui, V. Lakkundi, A. Olivereau, A. Serbanati, M. Rossi. "Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples". In IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'12), San Francisco, CA (June 2012), pp. 1–7. http://dx.doi. org /10.1109/WoWMoM.2012.6263790
5. Christian Dancke Tuen "Security in Internet of Things Systems" Master Thesis Norwegian University of Science and Technology.
6. Sepideh Fouladgar, Bastien Mainaud, Khaled Masmoudi, Hossam Afifi. "Tiny 3- TLS: a trust delegation protocol for wireless sensor networks". In Proceedings of the Third European conference on Security and Privacy in Ad-Hoc and Sensor Net works (ESAS'06), Hamburg, Germany (Nov 2006), pp. 32–42. http://dx. doi.org/10.1007/11964254_5
7. Vipul Gupta, Michael Wurm, Yu Zhu, Matthew Millard, Stephen Fung, Nils Gura, Hans Eberle, Sheueling Chang Shantz. (2005) "Sizzle: A standards-based end-to-end security architecture for the

embedded Internet. In Pervasive and Mobile Computing".
8. Y. B. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, (2014) "Lightweight collaborative key establishment scheme for the Internet of Things" Computer Networks, vol. 64, pp. 273 – 295.
9. R. Hummen, H. Shafagh, S. Raza, T. Voigt, and K. Wehrle, (2014) "Delegation based Authentication and Authorization for the IP-based Internet of Things," in IEEE SECON.
10. Ashton, K. "That 'Internet of Things' thing". Available online: http://www.rfidjournal.com/ (accessed on 22 June 2009).
11. Muhammad A Iqbal, Magdy Bayoumi (2016) "Secure End-to-End Key Establishment Protocol for Resource-Constrained Healthcare Sensors in the Context of IoT" The 14th Annual IEEE International Conference on High Performance Computing and Simulations (HPCS) 2016, Innsbruck Austria.
12. A. J. Menezes, S. A. Vanstone , P. C. Van Oorschot, "Handbook of Applied Cryptography", CRC Press, Inc., Boca Raton, FL, 1996.
13. Jennifer G. Steiner, B. Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An authentication service for open network systems. In Proceedings of the USENIX Winter Conference. Dallas, Texas, USA, January 1988, pages 191–202. USENIX Association, 1988
14. E. Rescorla and N. Modadugu, (2012) "Datagram Transport Layer Security Version 1.2," RFC 6347, IETF.
15. R. Moskowitz and R. Hummen, (2012) "HIP Diet EXchange (DEX)," draftmoskowitz-hip-dex-01 (WiP), IETF.
16. T. Kivinen, (2012) "Minimal IKEv2," draft-kivinen-ipsecme-ikev2-minimal-01 (WiP), IETF.
17. R. Hummen, H. Wirtz, J. H. Ziegeldorf, J. Hiller, and K. Wehrle, (2013) "Tailoring End-to-End IP Security Protocols to the Internet of Things," in Proc. of IEEE ICNP.
18. S. Santesson and H. Tschofenig, (2014) "Transport Layer Security (TLS) Cached Information Extension," draft-ietf-tls-cached-info-16 (WiP), IETF·
19. T. Kothmayr, C. Schmitt, W. Hu, M. Brünig, and G. Carle, (2013) "DTLS based security and two-way authentication for the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2710–2723.
20. Y. Saied and A. Olivereau, (2012) "D-HIP: A distributed key exchange scheme for HIP-based Internet of Things," in Proceeding of IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM) 2012, pp.1–7.
21. P. Porambage, A Braeken, A Gurtov, M Ylianttila and Susanna Spinsante "Secure end-to-end communication for constrained devices in IoT-enabled Ambient Assisted Living systems" in proceedings of 2nd World Forum on Internet of Things (WF-IoT), 2015.
22. "Internet of Things: An overview" by Internet Society https://www.internetsociety.org/sites/default/files/ISOC-IoT-Overview-20151014_0.pdf.
23. Emmanouil Vasilomanolakis, Jorg Daubert, Manisha Luthra, Vangelis Gazis, Alex Wiesmaier and Panayotis Kikiras "On the Security and Privacy of Internet of Things Architectures and Systems".
24. Joerg Daubert, Alexander Wiesmaier, and Panayotis Kikiras. 2015 A view on privacy & trust in iot. In IOT/CPS-Security Workshop, IEEE International Conference on Communications, ICC 2015, London, GB, June 08-12, 2015, page to appear. IEEE.
25. Sundmaeker, H.; Guillemin, P.; Friess, P.; Woelfflé, S. Vision and Challenges for Realising the Internet of Things; European Commission—Information Society and Media: Brussels, Belgium, 2010.
26. Bruce Ndibanje, Hoon-Jae Lee, and Sang-Gon Lee Security Analysis and Improvements of Authentication and Access Control in the Internet of Things.
27. Benjamin Kleine, Bethany Lobo, Amanada Levendowski March 2015 Internet of Things: The new frontier for data security and privacy (Part 1).
28. Gartner's Hype Cycle Special Report for 2015, Gartner Inc.,2015. http://www.gartner.com/technology/research/ hype-cycles/
29. Ahmad W Atamli and Andrew Martin. 2014 Threat-Based Security Analysis for the Internet of Things. In Secure Internet of Things (SIoT), pages 35–43. IEEE
30. Rolf H. Weber. Jan 2010, Internet of Things – New security and privacy challenges. Computer Law & Security Review, 26(1): 23–30.
31. Mohamed Abomhara and Geir M. Koien. 2014 Security and Privacy in the Internet of Things: Current Status and Open Issues. In Privacy and Security in Mobile Systems (PRISMS), pages 1–8. IEEE.
32. Riccardo Bonetto, Nicola Bui, Vishwas Lakkundi, Alexis Olivereau, Alexandru Serbanati, and Michele Rossi. 2012 Secure communication for smart IoT objects: Protocol stacks, use cases and practical examples. 2012 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012 - Digital Proceedings.
33. T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. RFC 5246 (Proposed Standard), August 2008. Updated by RFCs 5746, 5878, 6176.
34. Gunter Sch ¨ afer. ¨ Security in fixed and wireless networks - an introduction to securing data communications. Wiley, 2003.
35. S. Kent and R. Atkinson. Security Architecture for the Internet Protocol. RFC 2401 (Proposed Standard), November 1998. Obsoleted by RFC 4301, updated by RFC 3168.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Automock: Automated Mock Backend Generation for Javascript based Applications

By Neha Singhal & Harshit Jain

Abstract- Modern web development is an intensely collaborative process. Frontend Developers, Backend Developers and Quality Assurance Engineers are integral cogs of a development machine. Frontend developers constantly juggle developing new features, fixing bugs and writing good unit test cases. Achieving this is sometimes difficult as frontend developers are not able to utilize their time completely. They have to wait for the backend to be ready and wait for pages to load during iterations. This paper proposes an approach that enables frontend developers to quickly generate a mock backend that behaves exactly like their actual backend. This generated mock backend minimizes the dependency between frontend developers and backend developers, since both the teams can now utilize the entire sprint duration efficiently.

Keywords: javascript development; xml http request; javascript testing; web development; automated mock server.

GJCST-E Classification: D.1.1

Strictly as per the compliance and regulations of:

Automock: Automated Mock Backend Generation for Javascript based Applications

Neha Singhal [α] & Harshit Jain [σ]

Abstract- Modern web development is an intensely collaborative process. Frontend Developers, Backend Developers and Quality Assurance Engineers are integral cogs of a development machine. Frontend developers constantly juggle developing new features, fixing bugs and writing good unit test cases. Achieving this is sometimes difficult as frontend developers are not able to utilize their time completely. They have to wait for the backend to be ready and wait for pages to load during iterations.

This paper proposes an approach that enables frontend developers to quickly generate a mock backend that behaves exactly like their actual backend. This generated mock backend minimizes the dependency between frontend developers and backend developers, since both the teams can now utilize the entire sprint duration efficiently. The approach also aids the frontend developer to perform quicker iterations and modifications to his or her code.

Keywords: javascript development; xml http request; javascript testing; web development; automated mock server.

I. Introduction

The modern development process is increasingly moving towards an Agile Workflow. It is a process followed by teams both large and small. There has been a paradigm shift from long, slow development cycles to quick iterations. Agile processes have also been documented in multiple research papers [4; 5; 9].

The Agile approach is also followed for web application development (including development of Single Page Applications). A modern web application generally comprises two integral components—the frontend (or the UI) and the backend server. Both run in tandem and are heavily dependent on each other. The frontend depends on the backend for data and the backend relies on the frontend to display the content to the end user.

A typical development sprint is comprised of three major phases. First is the assignment of features to the frontend team and the corresponding backend team. Post the assignment phase, the sprint moves to the feature implementation stage. At this stage, Backend developers work on implementing the server features. The frontend developers have to generally wait for the backend to be ready. Once the backend is ready, the frontend developers implement the user interface. The backend developers are mostly idle during this time. One of the major challenges faced during development is that the non-production environments of integrated third-party services are unstable and not accessible at times, blocking developers from interacting with these services.

The final stage is the User interface (UI) unit testing stage. Post feature implementation, the developer has to write test cases for his or her module. There are some frequent issues usually faced at this point. Firstly, UI test cases for asynchronous network calls are messy and time consuming to write. Secondly, UI test cases that make network calls consume a lot of time in execution. Thirdly, UI test cases generally require consistent data based on real-world data. Finally, UI test cases must not add any test data to the database.

II. Proposed Model

Our approach resolves some of these issues faced by frontend developers. It has an intuitive interface and can easily be integrated into most JavaScript based applications with a single line of code.

The key features of our approach are:

- A fully-functional mock server
- Very lightweight; comprises just a single JavaScript file
- Flexibility to support as many API calls as required
- Automatic capture of any existing API calls and generation of mock data for them
- Integration into existing applications with a single line of code
- Support for polymorphic responses:
  - Alternate error responses for an API call
  - Multiple configuration based responses for the same API call
- No interaction with database

Author α σ: Adobe Systems Incorporated, Bengaluru, Karnataka, India.
e-mails: nsinghal@adobe.com, hajain@adobe.com

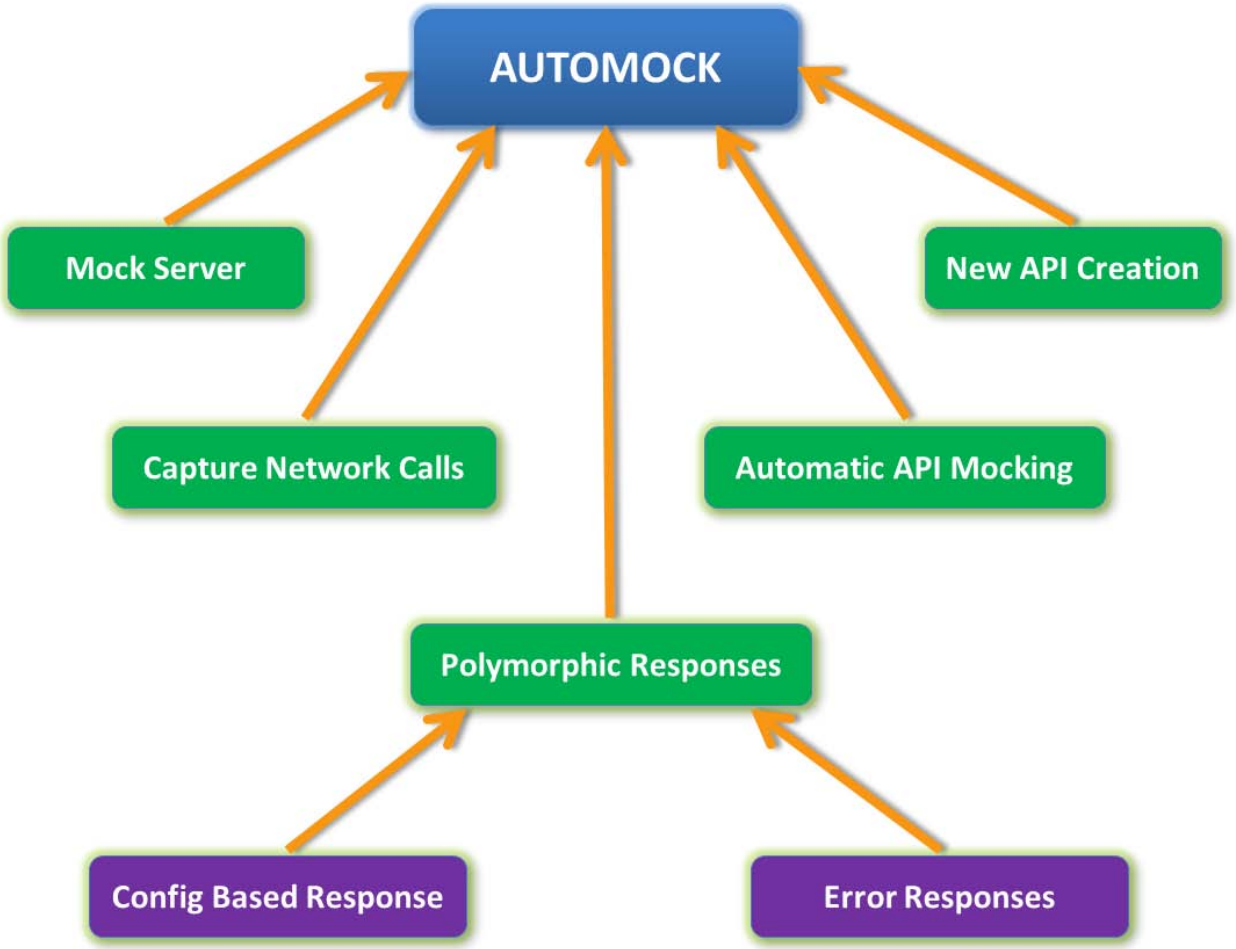

Figure 1: Overview of Automock features

Our approach is best suited for any medium to large-sized JavaScript web application including applications working with third-party components. It also designed for JavaScript unit testing. It is especially suited for interdependent teams working on the same web application in parallel.

As of now, the only limitation with our approach is that it only supports web development projects which use JavaScript.

Detailed description of our approach:

a) Fully functional mock server

A backend server comprises of a mapping between API calls and the corresponding responses for those calls. The frontend of a web application usually uses the AJAX (Asynchronous JavaScript and XML) protocol [6] to query the backend server. Though this allows the application to provide a user with a rich and interactive user experience, it also imposes certain challenges. The XML Http Request Spec [15] on which AJAX is based is browser implemented and hard for an application to control directly. To make a network call, the JavaScript code in the application calls the XML Http Request Object of the browser the application is running in directly. The interaction between the application and the XML Http Request Object is done through a series of callbacks. Once the network call is made, the server returns the appropriate response to the caller (based on the API request made). The browser then passes this information along to the application (through the aforementioned callback).

The XML Http Request Object according to the specification is meant to be immutable. Applications are not allowed to edit it directly without also manually implementing the overridden functionality. Our approach achieves the same functionality as a normal XML Http Request Object without the application realizing that the XML Http Request Object is being intercepted. Our approach achieves this in the following way. First, our approach intercepts some properties of the global XML Http Request object. This ensures that all AJAX network calls pass through Automock. On intercepting an AJAX network call, Automock checks if the response for the particular call is stored in its data file. Automock then checks if there are possible alternate responses. Based on configuration settings, Automock decides which response to return. If no specific configuration is set, Automock returns the default response. If a stored response is found, Automock returns the updated response. To achieve this, it replaces some properties

of the original XML Http Request Object. The following properties of the XML Http Request Object are immutable: response Text, ready State, response, status and status Text. Because these properties cannot be modified, Automock has to delete and replace them with the desired values in the XML Http Request Object. This XML Http Request object is then returned to the calling function. Since, the object is identical to the original XML Http Request Object, it works as expected and the application thinks that it made an actual asynchronous network call. In case there is no response present in the data file, Automock passes the call to the original XML Http Request object and makes the actual network call.

These steps ensure that the developer does not need to modify their code at all, while still achieving the functionality required. The mocked response is exactly identical to an actual response, enabling us to make AJAX calls in any preferred way; for example, through the j Query library, directly through an XML Http Request object, or even through any framework dependent-call, such as "fetch" in Backbone.js.

b) Very lightweight

Our approach comprises of just a single JavaScript file which basically comprises of the process outlined above and a socket communication library to interact with the User Interface and the data in real time. It requires no installation and has a very small memory footprint. All the saved AJAX responses are stored in a single flat file which is also minified and serialized. Since an actual server does not need to be run, it also does not consume much CPU memory.

c) Ease of integration

Unlike a traditional server which generally requires an application to be installed and run on one of the ports of the computer, Automock can be included in any web application that uses JavaScript with just a single line of code. As we intercept the native XML Http Request Object, we do not have to deal with issues such as port conflicts. It also does not require any build processes or any other external library to load itself into the system.

d) Flexibility to support as many API calls as required

A developer can mock as many API calls as required. If a mocked API call is not present, Automock forwards the request to the actual backend for resolution. This approach covers a vast variety of use cases wherein the developer can use Automock for only a small module or scale it up and use it for the entire application. This approach also allows the library to be integrated into the project at any stage of the development process. In addition to the above, since we modify the native XML Http Request Object, a user can use any popular library to make network requests such as j Query, Backbone.js, Angular's $http etc.

e) Automatic capture and mocking of existing API calls

Our approach provides the functionality to capture and mock any existing API calls within the application. It captures all outgoing AJAX requests and maps them to their corresponding incoming AJAX replies. First, it sets up a watch on all AJAX network calls. If any request is noticed by the watcher, it intercepts each returning AJAX network call and stores the response. This stored value is then mapped as the response to the URL for which the AJAX network call was made. Once it has the responses, it extracts each response and transforms the data into a format that the mock server can read. All such transformed responses are combined with our implementation of the mock server and stored in the JSON format. It records the URL, the response, the request type (Such as GET, PUT etc.) and some configuration options. This is serialized and converted into a file that is saved on the developer's system.

The developer can then simply mock all future calls to the same APIs. Thus, the developer can work without having to constantly query the server, speeding up development since no expensive network calls are necessary.

f) Significant performance boost to unit test case execution

Frontend (and JavaScript) testing is a complex subject with lots of research taking place. Regardless of the desired approach which may be either tool based (Such as Webmate [3] or ATUSA[10]) or automated [2], testing of asynchronous code and especially network requests is challenging.

Developers usually write multiple JavaScript unit test cases to test their modules. Running an entire suite of tests is usually very slow, because a large number of AJAX calls are made repeatedly. In our experience, the bottleneck while running a large number of test cases is the time taken by the network requests. By using our approach, the responses are instantaneous. During our testing, we have experienced a significant performance boost in our unit test cases.

g) No interaction with the database

An important requirement during the development phase is to avoid adding unnecessary data into the database. To combat this issue, developer teams either use local databases or setup a stage database. Both of these options are time consuming and possibly expensive as well. Since our approach does not make real API calls to the server, it solves this problem without the hassles of setting up a separate database

h) Supports alternate error responses for any API call

A developer must handle error responses during development. It is generally tricky to get error responses out of any good backend in a simple way. Our approach supports returning an error response for an API with some simple configuration settings. A developer can quickly and easily change API responses by either directly modifying the flat file or through the accompanying UI. This approach also helps ensure that a developer has handled all possible cases on the client facing UI.

i) Supports multiple responses for the same API call

Modern web applications now increasingly show different users different data based on the context. For example, when fetching the news feed for a user or fetching list of items for a particular category on an e-commerce site. Automock can be configured to return different responses for the same API call to simulate various situations.

III. Case Study

A version 2.0 prerelease web application was taken up for this case study. The project used an agile methodology and a timeline of about 6-8 weeks. The developers comprised two teams that worked in parallel. One team handled the backend and the other team handled the frontend of the web application. Each sprint was broken down into multiple stories/features being implemented. Here are the various phases we went through during our sprint where we made use of Automock:

a) Step 1: New feature implementation

At this point, both the frontend and the backend developers started development on the new feature. We used Automock quite effectively to make this process much more efficient. The backend developer would create the API stub (The name of the API and what parameters it takes) and use the Automock UI to set the typical response for the API. The frontend developer would then just run the fake server and implement their feature. When the actual API was ready, no more code changes were required for the frontend developer and they could just switch out the mock server for the real server. Since no developer was blocked, both the teams could pick up more features and utilize the entire sprint duration, thus requiring fewer sprints for the same set of features.

b) Step 2: Handling edge cases

Once the frontend developer had finished implementing a feature, they could work on handling edge cases and on handling error cases appropriately. To achieve this, they no longer needed hacks or workarounds. They could just modify the existing mock server response for that API with an error response and continue their development. Since this approach accurately simulates an API call, there is a much better end user experience when things go wrong at runtime.

Table 1: Comparison of time taken while developing for edge cases

	Without AUTOMOCK	With AUTOMOCK
Total Time (sec)	193	8

Notes:

- Time taken without Automock is calculated as: Time taken to modify backend code (~60 sec) + Time taken to build the .war file (76 sec) + Time taken to deploy the .war file (57 sec) = Total Time (193 sec)
- Time taken with Automock is calculated as: Time taken to modify frontend code; that is, changing the configuration variable (~8 sec) = Total Time (8 sec). The time taken to build and deploy the .war file is not required here as no backend changes are needed.
- All times are measured on a typical developer system.

c) Step 3: Adding functionality to pre-existing features

Some pre-existing areas of our code had to be modified to add new functionality. This is where we used one of Automock's best features - Automock can automatically capture and generate mock responses for all existing API calls. We captured all outgoing requests and stored the incoming responses. Since the application now no longer made time-consuming API calls, code edits and unit testing in these areas took much less time.

Results:

Table 2: Comparison of time taken to load four different modules of our application

Time Taken (sec)	Without AUTOMOCK	With AUTOMOCK
Module 1	14.11	0.31
Module 2	18.13	2.90
Module 3	31.63	0.21
Module 4	49.07	0.20

Notes:

- Modules in this table refer to a section/page of our application, each of which loads a different number of asynchronous AJAX calls.
- All times are measured on a typical developer system.

d) Step 4: Third-party services

Our application has dependencies on various third party services. We use these services for authentication, community forums, bug tracking etc. We encountered frequent outages from these third party services, especially on the stage environments. Using

Automock, we were able to mock all the related network calls and responses. Once this was done, we were no longer dependent on the availability of the third party service. This helped us mitigate any delays in development caused by the outages.

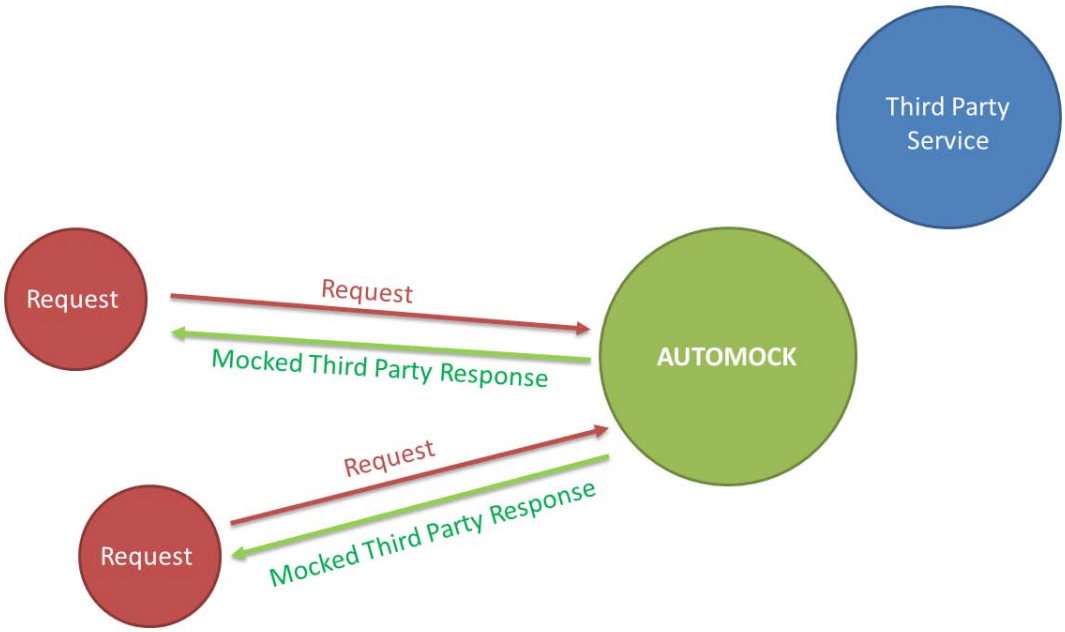

Figure 2: Third-party services

As observed in Fig 2, the third-party service was completely isolated. All requests that were intended for the third party service were easily captured and mocked by Automock. All that a developer had to do was to either let Automock capture a live call or set the response to a particular call manually.

e) Step 5: Unit Testing

Once the frontend developer has finished implementing a feature, they can then write the unit test cases for it. Generally, test cases that make network requests take a long time to complete. Such test cases are also time-consuming to write, since asynchronous logic is hard to implement in most testing frameworks. We have observed that most of the execution time of test cases is taken up by network requests.

Automock helped us solve this problem in a very elegant manner. Since mocked API calls return instantaneously, there was no need to handle asynchronous logic in the test cases. Also, since no expensive network calls were made, the test suite ran significantly faster. This gave us the double benefit of faster test case execution (with no messy workarounds for handling asynchronous calls) and faster test case creation. It also helped us write test cases with real-world data that was static and repeatable. Using Automock, we also avoided polluting the database with junk test data.

f) Step 6: Context based responses

Modern web applications are moving towards context sensitive responses. The same API call can return different responses based on multiple parameters. For example, our website returns different responses based on the credentials of a user. Using Automock, we were easily able to run the application as a different user. We set configuration parameters/flags and ran the application with different contexts. This allowed us to thoroughly handle all the cases that an end user might face, making our application much more robust and user friendly.

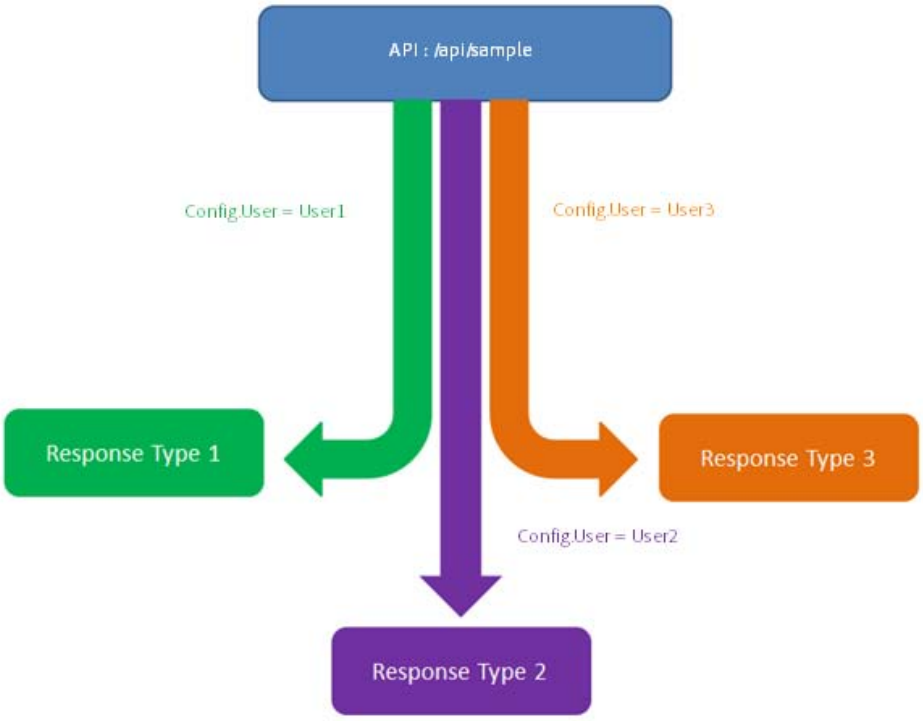

Figure 3: Configuration-based API responses

As seen in Fig 3, a developer would set a configuration parameter to modify the response to an API call. For example, we see that on setting config. user as User1, we get "Response Type 1" as the mocked response. However, on setting config. user as User2, we get "Response Type 2" as the mocked response. We could, similarly, set as many alternate responses as we required using configuration options.

Table 3: Comparison of time taken to load the application as a different user

Time Taken (sec)	Without AUTOMOCK	With AUTOMOCK
User: User1	108.56	3.51
User: User2	112.94	3.51
User: User3	121.27	3.51

Notes:

- Our application has user-specific data. Hence, the time taken without Automock varies for different users.
- The time taken mentioned in this table was the aggregate time taken to load all the four modules mentioned in table 2.
- All times were measured on a typical developer system.

IV. Related Work

JavaScript and Web Development in general are exciting fields for research and development. Our work is focused on easing the experience of web development and testing.

JavaScript application testing is a comparatively recent field due to the increasing size and complexity of modern web applications. More recently, there has been extensive research in the areas of automated testing [12; 13].However, this will still require having to either make the actual network call or write stubbing or mocking logic for the network call. Our approach helps us handle this problem easily and efficiently by mocking the API automatically. Since, the API calls are mocked using our approach, the actual network calls do not have to be made and no extra stubbing logic is required.

Along with research, there are existing libraries and tools to aid web development. Since it is an area of intense activity, there are some libraries already present in this space. In order to adequately put into context the related work in the field, it will be helpful to list down the minimum set of features that we required.

Any framework or library that we use should have a certain baseline of requirements. It should be independent of the development phase (Support use

during both testing and development). It should mock network calls without requiring a change in code. It should automatically capture existing network calls as well as allow for the creation of mocks for new network calls. It should support polymorphic responses to network calls. Lastly, it should be lightweight to include and should have zero interaction with the database.

Some of the libraries under consideration by us were:

a) SinonJS [14]
b) Jasmine-AJAX [7]
c) Api-mock [1]
d) Mockjax [8]

a) SinonJS

SinonJS is one of the most popular mocking/stubbing frameworks around. It is great at stubbing and mocking API calls. However, it is limited in its scope as it is a purely testing focused library. Though powerful as a test tool, it requires a great deal of setup and teardown to use in tests. However, SinonJS does not work at all during the development phase.

b) Jasmine-AJAX

Jasmine-AJAX solved one of the most pressing problems with SinonJS – easily mocking API calls. Jasmine-AJAX provides an easily customizable framework to modify the response to a network call. However, it also has a major limitation of only working with the Jasmine testing framework. Similar to SinonJS, this is also a testing focused library and does not work during the development phase.

c) API-Mock

API-Mock is an excellent tool to generate a mock server (running on Express) based on API blueprints. API-mock lets you document your API in the API blueprint format, generates mocks for your routes and sends the responses defined in the API spec. Since API-Mock generates a mock server, it can be used during both development and testing phases. However, it has the caveat of not working well with the existing server. Code changes are required to accommodate the generated API-mock server configuration. Due to this, it was not a good fit for our requirements.

d) Mockjax

Mockjax provides the easiest way of mocking API calls as compared to the other libraries listed above. One drawback of this library is that it is a manual process. The typical workflow for using Mockjax is to integrate the backend code and make the AJAX network call. Then a developer needs to copy the response for each call manually. Then they must transform the response into a Mockjax supported format. Finally, the developer must paste this formatted response into a file and integrate the library.

Though the process seems simple, the time taken to manually add calls using this workflow takes a large amount of time and effort. For a medium to large scaled project, this problem is compounded since a very large number of AJAX calls must be integrated into the application.

A combination of the factors above led to the development of Automock.

There has been some research where the XML Http Request Object is either monitored [16] or encapsulated [11]. To the best of our knowledge, Automock is the only original research paper that overrides a part of the native XML Http Request Object for automating the mocking of network calls. This not only aids in testing but also in development and achieves the goal of removing the dependency between frontend and backend team during agile sprints.

Table 4: Comparison of Automock with other related libraries

	SinonJS	Jasmine-AJAX	Api-Mock	Mockjax	Automock
Support testing and development			✓	✓	✓
Mock without code changes	✓	✓		✓	✓
Support polymorphic responses	✓	✓	✓	✓	✓
Automatic network call capture					✓
Support creation of new network requests			✓		✓

V. Conclusion and Advantages

As we have demonstrated through this paper and through the data provided in the tables, our approach realizes tangible and measurable benefits during development of a web application. It is most effective when interdependent teams are working together. Here are the key benefits:

- Makes development sprints more effective by efficiently utilizing developer time
- Speeds up website development by mocking network calls instead of making them every time
- Considerably speeds up test cases
- Aids in quicker development of new features when backend and frontend teams work in parallel

- Helps manage third-party service outages
- Makes development of error responses much more straightforward
- Helps in testing the application with different contexts (Polymorphic API responses)
- Avoids any database interaction during the development and testing phases

References Références Referencias

1. Api-Mock. Api-mock. https://github.com/localmed/api-mock, 2016.
2. Artzi, S., Dolby, J., Jensen, S.H., Moller, A., Tip, F. A framework for automated testing of javascript web applications. In *Proceedings of the 33rd International Conference on Software Engineering*, (ICSE '11), ACM New York, 571-580.
3. Dallmeier, V., Burger, M., Orth, T., Zeller, A. WebMate: a tool for testing web 2.0 applications. In *Proceedings of the Workshop on JavaScript Tools*, (JSTools '12), ACM New York, 11-15.
4. Dinakar, K. Agile development: overcoming a short-term focus in implementing best practices. In *Proceedings of the 24th ACM SIGPLAN conference companion on Object oriented programming systems languages and applications*, (OOPSLA '09), ACM New York, 579-588.
5. Ganis, M., Maximilien, E.M., Rivera, T. A brief report on working smarter with Agile software develop ment.*IBM Journal of Research and Development, 54* (4), 1 – 10.
6. Garrett, J. 2005. Ajax: A new approach to Web applications. Adaptive path. http://adaptivepath.org/ideas/ajax-new-approach-web-applications/, 2016.
7. Jasmine-AJAX. Jasmine-ajax.https://github.com/jasmine/jasmine-ajax, 2016.
8. Mockjax. Jquery-mockjax. https://github.com/jakerella/jquery-mockjax, 2016.
9. Kosk, A., Mikkonen, T. Rolling out a mission critical system in an agilish way: reflections on building a large-scale dependable information system for public sector. In *Proceedings of the Second International Workshop on Rapid Continuous Software Engineering*, (RCoSE '15), IEEE Press Piscataway, 41-44.
10. Mesbah, A., Deursen, A.V. Invariant-based automatic testing of AJAX user interfaces. In *Proceedings of the 31st International Conference on Software Engineering*, (ICSE '09), IEEE Computer Society Washington, 210-220.
11. Meyerovich, L.A., Guha, A., Baskin, J., Cooper, G.H., Greenberg, M., Bromfield, A., Krishnamurthi, S. Flapjax: a programming language for Ajax applications. In *Proceedings of the 24th ACM SIGPLAN conference on Object oriented programming systems languages and applications*, (OOPSLA '09), ACM New York, 1-20.
12. Mirshokraie, S., Mesbah, A., Pattabiraman, K. JSEFT: Automated Javascript Unit Test Generation. In *IEEE 8th International Conference on Software Testing, Verification and Validation*, (ICST '15), IEEE Graz, 1-10.
13. Negara, N., Stroulia, E. Automated Acceptance Testing of JavaScript Web Applications. In *19th Working Conference on Reverse Engineering*, (WCRE '12), IEEE Kingston, 318-322.
14. Sinon. SinonJS. http://sinonjs.org/, 2016.
15. XHR. XML Http Request. https://xhr.spec.whatwg.Org /, 2016.
16. Zheng, Y., Bao, T., Zhang, X. Statically locating web application bugs caused by asynchronous calls.In *Proceedings of the 20th international conference on World Wide Web*, (WWW '11), ACM New York, 805-814.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

The Wireless Body Area Sensor Networks and Routing Strategies: Nomenclature and Review of Literature

By V.T.Venkateswarlu, Dr.P. V. Naganjaneyu lu & Dr. D. N. Rao
Vasireddy Venkatadri Institute of Technology

Abstract- *WBASN* devices and the other significant condition like the coexistence of the systems among varied other wireless networks that are constituted in the proximity. In this study, scores of models that has been proposed pertaining to is an effective solution that has been proposed in terms of improving the solutions and there are varied benefits that have been achieved from the usage of *WBASN* solutions in communication, healthcare domain. From the review of stats on rising number of wireless devices and solutions that are coming up which is embraced by the people as wearable devices, implants for medical diagnostic solutions, etc. reflect upon the growing demand for effective models.

Keywords: *ieee 802.15.6, medium access control, physical layer, routing, wireless body area networks, wireless sensor networks, energy-efficiency.*

GJCST-E Classification: *C.2.1 I.2.9*

Strictly as per the compliance and regulations of:

The Wireless Body Area Sensor Networks and Routing Strategies: Nomenclature and Review of Literature

V. T. Venkateswarlu [α], Dr.P. V. Naganjaneyulu [σ] & Dr. D.N.Rao [ρ]

Abstract- $WBASN$ is an effective solution that has been proposed in terms of improving the solutions and there are varied benefits that have been achieved from the usage of $WBASN$ solutions in communication, healthcare domain. From the review of stats on rising number of wireless devices and solutions that are coming up which is embraced by the people as wearable devices, implants for medical diagnostic solutions, etc. reflect upon the growing demand for effective models. However, the challenge is about effective performance of such solutions with optimal efficiency. Due to certain intrinsic factors like numerous standards that are available, and also due to the necessity for identifying the best solutions that are based on application requirements. Some of the key issues that have to be considered in the process of $WBASN$ are about the impacts that are taking place from the wireless medium, the lifetime of batteries in the $WBASN$ devices and the other significant condition like the coexistence of the systems among varied other wireless networks that are constituted in the proximity. In this study, scores of models that has been proposed pertaining to MAC protocols for $WBASN$ solutions has been reviewed to understand the efficacy of the existing systems, and a scope for process improvement has been explored for conducting in detail research and developing a solution.

Keywords: ieee 802.15.6, medium access control, physical layer, routing, wireless body area networks, wireless sensor networks, energy-efficiency.

I. Introduction

$WBASN$, a Wireless Body Area Sensor Network comprises numerous factors like the low-power, either invasive or non-invasive, miniaturized, lightweight devices that has wireless communication features which operates in close proximity to human body. For instances, the wearable devices and other such devices that can be placed in or around the body comprises some kind of wireless sensor nodes that can monitor the bodily functions and characteristics based on certain environment, and parameters.

There are numerous devices and solutions that have emerged in the market on the basis of $WBASN$ that enable new applications; however, in terms of effective performance of such devices, there are numerous constraints that are envisaged in the process, which emphasize the need for contemporary solutions and protocols that could support in more effective implementation.

In terms of diversity that is envisaged in the applications right from the medical diagnostic and monitoring solutions to smart solutions for gaming, entertainment, communication and in varied domains, the scope of applications is on rise, however, the challenge is about the technical requirements in terms of wide variation that is taking place in the form of expected performance metrics, throughput or delay that is taking place, the levels of flexible architecture, and the protocols that are essential for successful functioning of the system.

Among the key communication standards that are adapted in the process of such devices, the reference standards are: $IEEE802.15.4$ [1], $IEEE802.15.6$ [2], and Bluetooth Low Energy [3]. $IEEE802.15.4$ (published in 2006), which emphasizes more about physical (PHY) and also the Medium Access Controls (MAC) layers which has short-range wireless communications that are devised for supporting in effective features like low power consumption, low bit rate networks and of low cost solutions.

The $IEEE802.15.6$ (published in 2012), is categorically designed for wireless communications in the vicinity of, or from inside or to a human body insertion. The $BTLE$ (Bluetooth Low Energy) model published in year 2010, has the ultra-low power consumption configuration for adaptation of bluetooth technology, and also in terms of targeting varied range of applications that are cost effective and the ones that has ultra-low power consumption configuration models, that are powered by button-cell batteries, and wireless sensors. Due to certain intrinsic factors like numerous standards that are available, and also due to the necessity for identifying the best solutions that are based on application requirements.

Some of the key issues that have to be considered in the process of $WBASN$ are about the

Author α: Associate Professor, Dept., of ECE, VVIT, Guntur, Andhra Pradesh 522508. e- mail: venki.vt@gmail.com
Author σ: Professor and Principal, Dept., of ECE MVRCET, Vijayawada, Andhra Pradesh. e-mail: pvnaganjaneyulu@gmail.com
Author ρ: Professor and Principal. e- mail: hrowrowv@gmail.com

impacts that are taking place from the wireless medium, the lifetime of batteries in the $WBASN$ devices and the other significant condition like the coexistence of the systems among varied other wireless networks that are constituted in the proximity.

The impact on radio wave propagation due to the human body presence is imperative, thus resulting in need for effective design of protocols and the peculiar radio channels. Also, the need for long battery lifetime has to be addressed using varied levels of energy efficient solutions as frequent replacement of batteries is a herculean task. The other critical factor that has to be taken in to consideration is about the outage occurrence which is resulting from the coexistence among the other wireless networks that are operating in similar frequency band. Majority of standard solutions for $WBASN$ shall operate in the way of license-free Industrial Scientific and Medical $(ISIM)$ band which is centered at 2.45 GHz and such factors leads to co-existence of the solutions with other networks that are operating in same band. (e.g., $WiFi\ IEEE802.11$).

In the proposed paper, the emphasis is on reviewing the taxonomy and the review of literature pertaining to recent developments in the kind of benchmarking routing protocols, MAC oriented protocols, pros and cons envisaged in terms of $WBASNs$ (Wireless Body Area Networks). In the process, the focus is upon initially outlining the properties which are very crucial for handling the $WBASN$ designs. Also identifying several sources contribute towards improving the QoS, qualitative comparisons of the protocol models shall be taken up in the process.

II. Nomenclature of The WBASN

Wireless Body Area Networks always could interact with the other existing range of wireless solutions like ZigBee, Bluetooth, $WSNs$, and $WLAN$ (Wireless Local Area Network), video surveillance solutions, Wireless Personal Area Network $(WPAN)$ and many other cellular networks. There are significant developments that are taking place in the advanced consumer electronic systems which are far more effective in terms of performance and features, for improving the quality of life [4].

In the $WBASN$ solutions, a paradigm shift is expected in how the solutions shall be adapted in the healthcare solutions, and with the rising trends of internet revolution, demand for such solutions are much higher. [5]. $WBASNs$ are very much effective in terms of facilitating information and communication technology solutions. [5]; Some of the significant functions like monitoring, processing information, sampling, relaying of vital signs communications, real-time feedback system are some of the critical functions that are carried out without any kind of interruptions or discomforts. [5] [6] [7].

Adapting the process of $WBASN$ shall support in effective adaption of one's physiological parameters and also in terms of offering effective mobility and flexibility for the users. The features of offering data from large time intervals, in specific to the natural environment, doctors shall have much better information to patient's status [8]. But the challenge is about the practical implementation, and acceptability of such solutions.

Such challenges lead to various issues pertaining to design and implementation related factors, as the key objectives for such system are about minimum delay, maximum throughput, network lifetime, and also in terms of reducing unnecessary communication pertaining to energy consumption. (e.g. control frame overhead, idle listening and frame collisions).

Also, the user oriented requirements of for the adoption of $WBASN$ are about certain factors like the privacy, value of such systems, ease of implanting or ease of using, and the safety conditions [5] [9].

a) Types of Nodes in a WBAN

A device that has communication scope and ability is considered as a node in $WBASN$. Nodes can be categorized in to three groups based on the functionalities, role in the network and implementation. Such classification of nodes in $WBASN$ is categorized in to following solutions.

Personal Devices (PD) – Such device is in charge of gathering information based on sensors and the actuators, and also plays a vital role in handling the interaction with the users. On the basis of such factors, the PD informs the users through an external gateway, focus on displaying information on the device or the actuators. There are many terminologies used for such devices as BCU (Body Control Unit), PDA or body gateway. [8].

Sensor – Sensors that are present in $WBASN$ focus on certain parameters in an individual's body from either internal or external factors. Such nodes gather and respond the data on basis of physical stimuli and only process the necessary data on the basis of response to information. Such sensors could be of various types like physiological sensors or ambient or biokinetics [8] [9]. Some of the profoundly used sensors are $EMG, EEG, ECG,$ Humidity detection sensors, blood glucose detection sensors, Temperature sensors, Plethysomgram sensors, motion sensors etc.

Actuators – Can be defined as a interaction system with the user for receiving data on the basis of sensors [8]. Also, the role of it is to offer feedback to the network by using the acting on sensor data, and plays a

vital role in the ubiquitous healthcare applications [10] As per the standards defined in $IEEE802.15.6$, another set of classification for nodes that are based on $WBASN$ have been depicted with the following factors [11] [12]

- Implant nodes: Such nodes are used as implanting in the body or under the skin.
- Body Surface Nodes are the ones that are usually placed on human body or near the human body
- External Node are the ones that never are in close physical contact to human system

'On the basis of nodes classification in $WBASN$, the role of network could be defined as:

Coordinator node can be defined as a communicator to the external world and the ones by which all the nodes communicate.

End Nodes in $WBASN$ are considered to be limiting performance to the embedded application, but they do not have the features of relaying messages from alternate nodes.

Relay is the intermediate nodes that are used for the process, and every relay node has a parent node, and also a child node, and some kind of relay messages. The essence of such a node is about the way the data is relayed to the other nodes before reaching the PDA. Such relay nodes are also effective in terms of data sensing.

b) Number of Nodes in a WBAN

In [13],[14],[15],[16], numerous solutions has been discussed pertaining to $IEEE$ standards in terms of technical requirements for $WBASN$ and the range focus on few actuators to sensor communicating alongside the portable handsets that are adapted high in numbers. In a typical medical network based $WBASN$ comprises 6 nodes that has scalable configuration for supporting even to the levels of 256 nodes [16].

There are varied ranges of operating range that is discussed in the factors, on the basis of support in the form of 256 nodes for each network within a 6m3 cube [17], [18], [19]. Only a single hub is permitted to focus on $WBASN$ while the number of nodes that are ranging from 0 to n MaxBanSize is defined to be 64 as per $IEEE802.15.6$ standards because of the transmission strategy factors. [20]. The value of this octet ranges between $x00$ and xFF (0-255).

Despite the fact that that there is no limitation to the number of nodes in $WBASN$, still the limitations is related to network in terms of communication protocols , architecture and the techniques of transmission that are adapted in the real-time scenarios. [8]

c) Topology used in $WBASNs$

The $IEEE802.15.6$ has adapted $WBASNs$ for operating either on the basis of one-hop or two-hop star based topology for effective communication by positioning at strategic location [21], [22]. The communication methods that are adapted is based on beacon mode or non-beacon model ones. The transmission takes place based on the beacons for beginning and ending at a super frame for enabling network association and also device synchronization. Carrier Sense Multiple Access with Collision Avoidance $(CSMA/CA)$ is adapted in non-beacon mode as and when essential for the process. [23]. In the case of $WBASN$, the coordinator is termed as sink node, and the ones that have one-hop start topology and for multi-hop architecture, nodes are usually connected to access points on the basis of other nodes. [24].

From the new version of standard protocol developed as per $IEEE$ standards, two hops are adapted in $IEEE\ WBASN$ standards for compliant communication. Also some of the proprietary systems which could adapt more than two hops are also considered in the process. However, the interoperability turns to be a major concern, as there is significant challenge in terms of standard compliant.

d) Communication Architecture of $WBASNs$

Communication Architecture of $WBASNs$ can be classified in to three tiers as:

- Tier-1: Intra-$WBASN$ communication
- Tier-2: Inter-$WBASN$ communication
- Tier-3: Beyond-$WBASN$ communication

Tier-1: depicts inputs on network interaction of the nodes and also the respective transmission ranges around the human body.

Tier-2: works as communication tier between PS and one or more access points (APs). The APs are an integral part of infrastructure that shall be posi- tioned in dynamic environment. Tier-2 communication shall interconnect $WBASNs$ for various networks and the ones that are easily accessed for daily life too. [4]. some of the paradigms that are considered as sub cate-gories for inter-$WBASN$ communication are infrastru- cture based architecture and the ad-hoc based architecture. [4].

Tier-3: Beyond-$WBASN$ Communication is about usage of metropolitan areas, and a gateway like the PDA can be adapted for bridging gap between Tier-2 and the Tier-3. Database is one of the most effective components for Tier-3, and tier-3 usually restores necessary information from a patient, which is used for treatment.

e) Layers of Wbans

Predominantly the PHY and MAC layers are the ones that are proposed as per the approved standards of $802.15x$, as they not have any network, or the application layer transport and hence the call for

other parties to focus upon them. In $IEEE802.15.6$ $(WBASN)$ working group has defined new PHY and MAC control layers with low complexity, reduced cost of operations and also in terms of offering ultra-low power and short range of wireless communication around human body. The introduction of logical node management and the hub management entity models were also developed to address such solutions.

i. *Physical Layer*

The activation and deactivation in the case of CCA (Clear Channel Assessment) and radio transceivers and data transmission is the accountability of PHY layers in $IEEE802.15.6$, for any kind of current channel data reception and transmission. Also, the choice of physical layer is more dependent on the levels of target applications that are established as implant in the body or in the off-body locations. Usually the PHY layer comprises a procedure for transformation of a PSDU (physical layer service data unit) towards PPDU (a physical layer protocol data unit). $IEEE802.15.6$ Specified varied layers of physical layers as HBC and the UWB (Ultra-Wide Band)

While $NB\ PHY$ plays a vital role in terms of data transmission or reception, deactivation or activation for Clear Channel Assessment (CCA) in a current channel. Using differential 8-phase shift keying $(D8PSK)$, and Differential Quadrature Phase-shift keying $(DQPSK)$ modulation techniques the requisite solutions are handled by the process.

$HBC\ PHY$ has supported with Electrostatic Field Communication (EFC) requirements that support in modulation and start frame delimiter (SFD), which are specified data pattern generated and sent before the packet header and payload. SFD Sequence shall be transmitted once while the preamble sequence is sent four times to ensure packet synchronization.

The UWB physical layer shall be used for communication amidst of on-body devices and the off-body devices. The physical header focuses on information from the scrambler seed, length of payload and also on the basis of rate of $PSDU$. Also, the receiver focuses on information in PHR for decoding $PSDU$.

In UBB PHY there are two frequency bands that exist like the high band and low band, which are divided in to two channels as bandwidth of 499.2 MHz. One of the channels is considered to be mandatory channel comprising support by UWB devices.

ii. *MAC Layer*

The $IEEE802.15.6$ working group defines a MAC layer on top of the PHY layer adapted for controlling the channel access, using the hub, which chooses the beacon periods of equal length for binding the super frame. Offsets in the beacon periods are also shifted by Hub, and the beacons are usually sent during each beacon period, if not prohibited by any kind regulations by $MICS$ band. [25].

The coordinator for the channel access coordination is evaluated on the basis of three access modes:

- Beacon Mode with Beacon Period Super-frame Boundaries
- Non-Beacon Mode with Super-Frame boundaries
- Non-Beacon Mode without super-frame boundaries

In each period of super frame, there are three categories of access mechanisms as

- Scheduled Access and Variants
- Unscheduled and Improvised Access
- Random Access Mechanism

f) Routing in $WBASN$

There are numerous routing protocols that has been developed for Ad Hoc Networks [26] and $WSNs$ [27]. Also the $WBASNs$ shall be similar to $MANETs$ which in terms focus on moving topology comprising group-based movement rather than any kind of node-based movement [28]. $WBASNs$ Comprising regular energy issues that are faced for power transmission when compared to traditional sensor for Ad Hoc networks, which are on the basis of node replacements categorically for implanting nodes, which depict more regulated energy factors. Also, in the case of $WBASN$ there are more changes in terms of topology and also in terms of higher moving speed, despite of static or low mobility scenarios [28]. Due to certain factors like the aforementioned factors and specific $WBASN$ challenges, the routing protocols that are designed for $MANET$ and $WSNs$ shall not be effective to $WBASNs$ [29].

g) Challenges of Routing in $WBASNs$

Some of the significant challenges in terms of routing for $WBASNs$ are:

i. *Physical Layer Challenges*

PHY layer of protocols are developed for minimizing the power consumption without compromising on reliability, but the crux is that current models of wireless technologies are having high peak current and also supports in minimizing the average current that is drawn by duty cycling of radio between active and sleep modes. [9]. Also, the interference is also the other major setback in $WBASN$ systems, despite of the developments that are taking place in terms of improving the co-existence. Also, the value of employing transmits power control for minimizing the interference and focusing on $WBASN$ node battery

lifetime has to be given importance. Off-body interference resulting from collision withexternal sensors is also a challenge envisaged in the process [30].

ii. *MAC Layer Challenges*

The mechanisms that are constituted in $IEEE802.15.6$ is not designed based upon complete MAC protocols and only the basis requirements towards addressing the interoperability issues are addressed in such factors, by developing message exchange protocols and packet formats, in terms of further research questions. Reliability which is a major factor in terms of design is also the other key challenge that has to be addressed in the process. In the instances where the reliability is not achieving from one-hop star topology, the relays are adapted for achieving the outcome. [31]. Also, $WBASNs$ require specific QoS requirements that are to be adhered by the MAC proposal [4].

h) Transport (QoS) Challenges

The QoS requirements of the applications in $WBASNs$ have to be addressed with any performance dwindling and without any kind of complexities in place. Also, in real-time, some of the $WBASNs$ are significantly impacted in terms of loss and relay, and the issue of limited memory impacts to great extent the outcome that is expected from the process. At times, the QoS features like the bandwidth, reliability and the delay in the process could impact in terms of performance of the system. In order to achieve a lower level of packet loss, the transmit power have to be increased which shall result in increased levels of relative power consumption.

III. Contemporary Affirmation of Benchmarking Routing Strategies in WBASN

Both in the $WSNs$ [32] and also in $MANETs$ [33], the routing protocol systems have been extensively reviewed in the earlier times, and it is imperative that significant standards in terms of $BANs$ have some impact in terms of constraints on the design for the routing protocol, which also results in significant challenges in terms of routing performance. In the implementation of $WSNs$ the energy efficient routing protocols are more sensitive in terms of data in terms of memory access, processing of data and other such kind of measurements. [34].

While WSN nodes are homogenous, the BAN nodes are heterogeneous and also have wide range scope in terms of data rate and available energy [35], the mobility might also vary. [34] [35]. Also, BAN routing must take in to account the variations in the body, impact of radiation on tissue heating and limited energy resources, in terms of adapting available resources for further reducing the intervals for batter charging, enhancing network lifespan and also for developing quality system. Despite the fact that the characteristics of $BANs$ are to an extent similar to $MANETs$ and $WSNs$, still the unique difference could be attributed to contemporary solutions that are essential in terms of routing protocols.

a) Temperature based Routing

Magnetic and electric fields are generated from the radio signals that are generated using wireless communication solutions. The high level of radiation emitting and the exposure to such levels of radiation, results in increased temperature levels in the human body. [36], which could impact to health implications. [37].

In the temperature oriented routing algorithms that are provided, the emphasis is on reducing the hot-spots. The levels of heating and radiation absorption in the body are some of the significant factors considered in the design of such routing protocols. $TARA$ (Thermal Aware Routing Algorithm) [36] is one of the effective models that has been proposed which works on addressing the temperature issues, however, the issue of reliability and packet loss rations, along with low network life time are some of the key issues in the model, which has been overcome in the other model proposed as Least Temperature Routing Algorithm (LTR) [38] and Adaptive Least Temperature Routing $(ALTR)$ [38]. But one of the challenges is about how the temperature of each need to understand the other node level temperature is one of the major drawbacks for the solution [8].

HPR [37] is another biomedical based sensor network routing algorithm proposed with the objective of reducing impact of delay-sensitive issues and the ones that work towards reducing the average packet delay and also in terms of avoiding hotspot formation. Also HPR chose the routes that constitute minimum hops from sender node levels to the destination nodes and Thermal-Aware Shortest Hop Routing $(TSHR)$ also provides similar kind of solutions., but the challenge with such models are about lifetime and reliability. Movassaghi et al. [39], have provided a detailed comparison amongst the routing protocols proposed thus far for $(WBASNs)$.

b) Cluster-based Routing

Among the contemporary routing protocols, the cluster based routing protocols that are adapted in WBANs divide the nodes in to varied clusters and for every cluster developed; cluster-head for each of the cluster is assigned. Using the cluster heads the data transmission from sensor to sink is carried out. Prime objective of such routing protocols are to focus on

reducing the number of direct transmissions that are taking place from the sensors to the base station. Also, the overhead and the delay related to cluster selection are considered to be key drawbacks for such protocols.

In [40], adapting a data generating protocol using "Anybody" has been proposed for reducing the quantum of direct transmissions in to base station. In the proposed model, LEACH [41] is used as fundamental model which focus on spreading energy dissipation at frequent intervals using the cluster-heads. Such data is used for gathering information and sending to the base station using the cluster heads. In the LEACH model, it is presumed that all nodes are in the sending range of the base station, but in the proposed model, the issue is addressed by changing the cluster-head selection and developing a robust network comprising of cluster-heads. But one of the key limitations is that the energy efficiency issues are not considered in the model. One of the other issues in the LEACH protocol is about Hybrid Indirect Transmissions (HIT) [42[which is resulting in improving energy efficiency, that is not considered in the process.

Culpepper et al [43], [44] discussed another effective model of data generating protocol which focus on reducing the number of direct transmissions towards the base station, and by using multi-hop indirect transmissions for a cluster and also for multiple clusters that are adjacent. The analysis of HIT and HITm has depicted some kind of network delay despite of high energy efficiency and network life time. It is imperative that HIT needs more effective communication energy while handling dense networks and the issues of reliability and conflicting interaction in the route is not addressed. [34].

c) Probabilistic Routing

There are other alternative routing protocols like the probable of cost factor in to account and work towards developing a route that is carried out with minimum cost, but such protocols require numerous transmissions for updating link-state information, which could be a constraint in terms of implementing blanket range of protocols.

Movassaghiet.al [45] proposed Energy Efficient Thermal and Power Aware routing $(ETPA)$ which has offered an effective solution for the proposed factors of relative costing solutions. Also, some of the other intrinsic aspects like the high depletion time which could result in lasting communication within the nodes are also considered in $WBASNs$.

PSR routing framework proposed by Liang et.al [46], $PRPLC$ [47] that is proposed in terms of Link Likelihood Factor (LLF) were also certain models along with contemporary solutions like $DVRPLC$ [48] is the other set of models that has been proposed in terms of addressing the probabilistic factors in the conditions.

d) Cross Layer Routing

Cross layover routing protocols can be stated as the ones that focus on challenges in the network layer and with the other layers. Despite the fact that such protocols have low energy consumption, still the issues could be more about high path loss and also impact on body motion. Some of the significant models like $WASP$ (Wireless Autonomous Spanning Tree Protocol) which is proposed in [49] focus addressing the issues of by focusing on $WASP$ cycles for effective distribution manner, for offering medium access coordination and also in terms of improving traffic routing.

The Controlling Access with Distributed Slot Assignment protocol $(CICADA)$ [50] is also another low energy cross layer routing protocol categorically designed for $WBASNs$ that are based on multi-hop $TDMS$ scheduling.

Timezone Coordinated Sleeping Mechanism $(TICOSS)$ [51] adjusts all nodes as Full Functional Devices (FDD) and enhances the $IEEE802.15.4$ standard by configuring the shortest path route to the $WBASN$ coordinator, preserving energy and minimizing hidden terminal collisions through V-scheduling (due to V-shape communication flow), which doubles the operational lifetime of $IEEE802.15.4$ for high traffic scenarios and extending $IEEE802.15.4$ to support mobility.

$BIOCOMM$ [52] is another cross layer routing protocol designed with the fundamental as interaction of the MAC and network layer in biomedical sensor networks to optimize overall network performance. This interaction is achieved through a Cross-layer Messaging Interface (CMI) via which the MAC layer sends its status information to the network layer and vice-versa.

e) Qos based Routing

Among the varied levels of routing protocols that are discuss QoS based routing protocols are some of the key models. There are numerous methods that has been proposed based on power efficiency model and also taking in to account varied range of metrics and parameters that could support in effective process of routing. A novel QoS related routing protocol $(LOCALMOR)$ is proposed in [53] for improving the biomedical applications for sensor networks.

It is imperative from the review of solutions that the key issue that is envisaged in the routing path is predominantly related to path routing, and geographic routing issues. Despite the fact that majority of such constraints has been addressed in the process of $RL - QRP$ algorithm, the impact in terms of

independent distributed reinforcement learning model $(IndRL)$ approach for QoS route calculations have to focus on sensor nodes, but the challenge with the proposed solutions are about lack of scope for global optimization in the large scale network conditions.

IV. MAC Protocols

Varied sources contribute to the energy inefficiency in the system, and collisions are one of the major factors that are leading to the energy inefficiency. Collisions result as a part of two or more sensor nodes attempting for data packets transmission in simultaneous manner. There are many over emission issues that result from the issues like prolonged transmission of message whilst the destination node not being comfortable in terms of accepting such transmission. Time Division Multiple Access $(TDMA)$ and the Clear Channel Assessment (CCA) models are some of the solutions that are developed, towards addressing such conditions of emission related implications.

There are wide ranges of Energy protocols that are adapted in terms of focusing on essential behavior of protocols, wherever possible. Contention-based MAC like the Carrier Sense Multiple Access/ Collision Avoidance $(CSMA/CA)$ protocols nodes competes for the channel to transmit data. $CSMA$ based MAC protocols defined in some of the related models [54] [55] [56] [57] [58] are very effective solutions, and the node defers for the transmission for making it idle. $CSMA/CA$ has the issues of protocol reliability Some of the critical models like the $TDMA$ related contention-free MAC protocols [59]-[62] are considered to be very effective and energy-efficient MAC protocols, but the stipulated standards of $WBASN$ are turning out to be some of the limitation for the model.

In the recent past, there are many MAC protocols that have been published for $WBASN$ solutions. $CDMA, FDMA, BSNs$ and many other such models has been proposed for successful implementation. [63]- [68]. In the table-1 comparative analysis of MAC protocols for $WBASN$ has been provided.

Table 1: CSMA based MAC Protocols

Protocols	MAC Approach/ Basic Operation	Time Synchronization Requirement	Benefits	Limitations	Views
S-MAC [54]	CSMA/Scheduling	No	High latency, simplicity, and scope for preventing sleep schedules related overhead issues	Scope of collisions if the packet is not destined for listening nodes and also issues of Low throughput Low throughput,	Effective for routine traffic application solutions.
T-MAC [55]	CSMA/Scheduling	No	Using Burst for packets dispatch resulting in under variable load.	Issues of sleep mode	Responsive to changes in the traffic conditions
B-MAC [56]	CSMA/Scheduling	No	Simplicity, good packet delivery rate, high throughput, low overhead	Scope of increased power consumption and overhearing problems	Effective for normal traffic application models.
P-MAC [57]	CSMA/Listening	No	High throughput	Might be slow in response to changes	Effective for delay sensitive solutions.
D-MAC [58]	CSMA/Scheduling	No	Is efficient model for energy saving and the impact of Good delay in the performance.	Utilization of collision avoidance solutions are poor	Resourceful for low delay applications

WiseMAC	np-CSMA/Listening	No	Adaptive for traffic loads and also in terms of mobility support	Decentralized system might lead to variations in the sleep and wake-up times.	Could be resourceful for Normal traffic applications

The table below indicates the scope of TDMA based MAC protocols that could be adapted for significant development in the solution.

Table 2: TDMA based MAC Protocols

Protocols	Performance Comparison	Time Synchronization Needed	Reasons for Energy-Efficiency	Comments
PACT[59]	TDMA/Passive Clustering	No	Lifetime of network shall be prolonged which is a better solution	High traffic overheads could be a major challenge. Effective for low delay applications
LEACH[60]	TDMA/Clustering	Yes	Distributed protocol performs better scope of system.	Additional overhead essential for dynamic clustering.
				WBAN coordinator shall work as cluster-head
FLAMA[61]	TDMA/Scheduling	Yes	Less delay, increased reliability and effective energy savings	Support issues for multi-channels synchronization. Resourceful for normal traffic conditions.
HEED[62]	TDMA/Clustering	Yes	Low overhead conditions, and increased lifetime	Optimal set of cluster heads shall be a constraint. WBAN coordinator shall work as cluster-head
Omeni[69]	Zigbee, Bluetooth and IEEE 802.11	NO	Centrally controlled system resulting in better energy consumption	Resourceful for Applications like ECG Machines and other similar monitoring solutions.
MedMAC [70]	IEEE 802.15.4 MAC	NO	Increased energy efficiency using dynamical adjustments for QoS requirements	Effective for low rate and medium Data rate and Medical applications
Marinkovic [71]	Protocols described in[69], [72]	YES	Reduced power consumption	Short bursts of data could be sent easily
BodyMAC [73]	IEEE 802.15.4 MAC	YES	Improved node energy efficiency.	Resourceful for periodic data sensing and event reporting

V. Conclusion

Wireless Body Area Networks are turning out to be very significant development and globally with the kind of demand for wearable devices and also the way wireless devices and solutions are being adapted in terms of medical, healthcare diagnostics and also in the process of communication, the *WBASN* related routing protocols has gained significant importance. Alongside

the positive developments, even the challenges and complexities in terms of handling such solutions are also rising to great extent. Right from ensuring that the *PHY* and *MAC* do not have impact from external factors to increasing the efficiency and performance, rising the standards of co-existence that is taking place in the system, there are various factors that has to be taken in to consideration.

In the proposed paper, the emphasis is on reviewing the taxonomy and the review of literature pertaining to recent developments in the kind of benchmarking routing protocols, *MAC* oriented protocols, pros and cons envisaged in terms of *WBASNs* (Wireless Body Area Networks). In the process, the from the outlining the properties that are very crucial for handling the *WBASN* designs. Many sources contributing towards improving the *QoS*, qualitative comparisons of the protocol models are reviewed in the process, and from the review of literature, it is imperative that despite of numerous models that has evolved, still in terms of improving the operational efficacy, there are potential solutions that could be achieved from the process.

References Références Referencias

1. IEEE 802.15.4 Standard, Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low- Rate Wireless Personal Area Networks (LR-WPANs). Piscataway, New Jersey, 08855-1331: IEEE, 2006. [Online]. Available: http://standards.ieee.org/getieee802/802.15.html
2. "IEEE standard for local and metropolitan area networks part 15.6: Wireless body area networks," IEEE Std 802.15.6-2012, pp. 1 –271, February 2012.
3. Specification of the Bluetooth System version 4.0. Bluetooth SIG, June 2010. [Online]. Available: http://www.bluetooth.com
4. Chen, M., Gonzalez, S., Vasilakos, A., Cao, H., & Leung, V. C. (2011). Body area networks: A survey. Mobile networks and applications, 16(2), 171-193.
5. Otto, C., Milenkovic, A., Sanders, C., & Jovanov, E. (2006). System architecture of a wireless body area sensor network for ubiquitous health monitoring. Journal of mobile multimedia, 1(4), 307-326.
6. Ullah, S., Shen, B., Riazul Islam, S. M., Khan, P., Saleem, S., & Sup Kwak, K. (2009). A study of MAC protocols for WBANs. Sensors, 10(1), 128-145.
7. Kwon, H., & Lee, S. (2009, September). Energy-efficient multi-hop transmission in body area networks. In 2009 IEEE 20th International Symposium on Personal, Indoor and Mobile Radio Communications (pp. 2142-2146). IEEE.
8. Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. Wireless Networks, 17(1), 1-18.
9. Hanson, M. A., Powell Jr, H. C., Barth, A. T., Ringgenberg, K., Calhoun, B. H., Aylor, J. H., & Lach, J. (2009). Body area sensor networks: Challenges and opportunities. Computer, 42(1), 58.
10. Wang, S., & Park, J. T. (2010). Modeling and analysis of multi-type failures in wireless body area networks with semi-Markov model. IEEE Communications Letters, 14(1), 6-8.
11. J. Xing and Y. Zhu, "A survey on body area network," in 5th Int. Conf.on Wireless Communications, Networking and Mobile Computing (WiCom '09), pp. 1 –4, Sept. 2009.
12. Yazdandoost, K. Y., & Sayrafian-Pour, K. (2009). Channel model for body area network (BAN). IEEE P802, 15, 08-0780.
13. "IEEE p802.15-07–0867-04-0ban," in 15-10-0245-06-0006, Oct. 2007.
14. "IEEE p802.15.6/d0 draft standard for body area network," IEEE Draft, 2010.
15. Lewis, D. (2010). IEEE P802. 15.6 D04 Draft Trial-Use Standard for Body Area Network. IEEE 802.15 WPAN.
16. "IEEE p802. 15-10 wireless personal area networks,," July, 2011.
17. Zhen, B., Patel, M., Lee, S., Won, E., & Astrin, A. (2008). Tg6 technical requirements document (TRD) IEEE p802. 15-08-0644-09-0006.
18. Zhang, A., Smith, D. B., Miniutti, D., Hanlen, L. W., Rodda, D., & Gilbert, B. (2010, April). Performance of piconet co-existence schemes in wireless body area networks. In 2010 IEEE Wireless Communication and Networking Conference (pp. 1-6). IEEE.
19. L. Hanlen, D. Miniutti, D. B. Smith, D. Rodda, and B. Gilbert, "Cochannel interference in body area networks with indoor measurements at 2.4 GHz: Distance-to-interferer is a poor estimate of received interference power.," IJWIN, vol. 17, no. 3-4, pp. 113–125, 2010.
20. Zasowski, T., Althaus, F., Stager, M., Wittneben, A., & Troster, G. (2003, November). UWB for noninvasive wireless body area networks: channel measurements and results. In Ultra Wideband Systems and Technologies, 2003 IEEE Conference on (pp. 285-289). IEEE.
21. Tachtatzis, C., Di Franco, F., Tracey, D. C., Timmons, N. F., & Morrison, J. (2010, December). An energy analysis of IEEE 802.15. 6 scheduled access modes. In 2010 IEEE Globecom Workshops (pp. 1270-1275). IEEE.
22. Shah, R. C., & Yarvis, M. (2006, September). Characteristics of on-body 802.15. 4 networks. In 2006 2nd IEEE Workshop on Wireless Mesh Networks(pp. 138-139). IEEE.
23. Sukor, M., Ariffin, S., Fisal, N., Yusof, S. S., & Abdallah, A. (2008, May). Performance study of wireless body area network in medical environment. In 2008 Second Asia International Conference on

2006 2nd IEEE Workshop on Wireless Mesh Networks(pp. 138-139). IEEE.
23. Sukor, M., Ariffin, S., Fisal, N., Yusof, S. S., & Abdallah, A. (2008, May). Performance study of wireless body area network in medical environment. In 2008 Second Asia International Conference on Modelling &# x00026; Simulation (AMS) (pp. 202-206). IEEE.
24. Natarajan, A., Motani, M., de Silva, B., Yap, K. K., & Chua, K. C. (2007, June). Investigating network architectures for body sensor networks. In Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments (pp. 19-24). ACM.
25. Kwak, K. S., Ullah, S., & Ullah, N. (2010, November). An overview of IEEE 802.15. 6 standard. In 2010 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies (ISABEL 2010)(pp. 1-6). IEEE.
26. Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1), 1-22.
27. Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. Ad hoc networks, 3(3), 325-349.
28. Cheng, S. H., & Huang, C. Y. (2013). Coloring-based inter-WBAN scheduling for mobile wireless body area networks. IEEE Transactions on parallel and distributed systems, 24(2), 250-259.
29. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I.,...& Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. Journal of medical systems, 36(3), 1065-1094.
30. Yuce, M. R., & Khan, J. (Eds.). (2011). Wireless body area networks: Technology, implementation, and applications. CRC Press.
31. Boulis, A., Smith, D., Miniutti, D., Libman, L., & Tselishchev, Y. (2012). Challenges in body area networks for healthcare: The MAC. IEEE Communications Magazine, 50(5), 100-106.
32. Akkaya, K., & Younis, M. (2005). A survey on routing protocols for wireless sensor networks. Ad hoc networks, 3(3), 325-349.
33. Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. Ad hoc networks, 2(1), 1-22.
34. Ullah, S., Higgins, H., Braem, B., Latre, B., Blondia, C., Moerman, I., ...& Kwak, K. S. (2012). A comprehensive survey of wireless body area networks. Journal of medical systems, 36(3), 1065-1094.
35. Latré, B., Braem, B., Moerman, I., Blondia, C., & Demeester, P. (2011). A survey on wireless body area networks. Wireless Networks, 17(1), 1-18.
36. Tang, Q., Tummala, N., Gupta, S. K., & Schwiebert, L. (2005). Communication scheduling to minimize thermal effects of implanted biosensor networks in homogeneous tissue. IEEE Transactions on Biomedical Engineering, 52(7), 1285-1294.
37. Bag, A., & Bassiouni, M. A. (2007, May). Hotspot preventing routing algorithm for delay-sensitive biomedical sensor networks. In Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on (pp. 1-5). IEEE.
38. Bag, A., & Bassiouni, M. A. (2006, October). Energy efficient thermal aware routing algorithms for embedded biomedical sensor networks. In 2006 IEEE International Conference on Mobile Ad Hoc and Sensor Systems (pp. 604-609). IEEE.
39. Movassaghi, S., Abolhasan, M., & Lipman, J. (2013). A review of routing protocols in wireless body area networks. Journal of Networks, 8(3), 559-575.
40. Watteyne, T., Augé-Blum, I., Dohler, M., & Barthel, D. (2007, June). Anybody: a self-organization protocol for body area networks. In Proceedings of the ICST 2nd international conference on Body area networks (p. 6). ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
41. Heinzelman, W. R., Chandrakasan, A., & Balakrishnan, H. (2000, January). Energy-efficient communication protocol for wireless microsensor networks. In System sciences, 2000. Proceedings of the 33rd annual Hawaii international conference on (pp. 10-pp). IEEE.
42. Moh, M., Culpepper, B. J., Dung, L., Moh, T. S., Hamada, T., & Su, C. F. (2005, December). On data gathering protocols for in-body biomedical sensor networks. In GLOBECOM'05. IEEE Global Telecommunications Conference, 2005. (Vol. 5, pp. 6-pp). IEEE.
43. Culpepper, B. J., Dung, L., & Moh, M. (2004). Design and analysis of Hybrid Indirect Transmissions (HIT) for data gathering in wireless micro sensor networks. ACM SIGMOBILE Mobile Computing and Communications Review, 8(1), 61-83.
44. Moh, M., Culpepper, B. J., Dung, L., Moh, T. S., Hamada, T., & Su, C. F. (2005, December). On data gathering protocols for in-body biomedical sensor networks. In GLOBECOM'05. IEEE Global Telecommunications Conference, 2005. (Vol. 5, pp. 6-pp). IEEE.
45. Movassaghi, S., Abolhasan, M., & Lipman, J. (2012, September). Energy efficient thermal and power aware (ETPA) routing in body area networks. In 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications-(PIMRC) (pp. 1108-1113). IEEE.
46. Liang, X., Li, X., Shen, Q., Lu, R., Lin, X., Shen, X., & Zhuang, W. (2012, March). Exploiting prediction to enable secure and reliable routing in wireless body area networks. In INFOCOM, 2012 Proceedings IEEE (pp. 388-396). IEEE.

47. Quwaider, M., & Biswas, S. (2009, October). Probabilistic routing in on-body sensor networks with postural disconnections. In Proceedings of the 7th ACM international symposium on Mobility management and wireless access (pp. 149-158). ACM.
48. Quwaider, M., & Biswas, S. (2010). DTN routing in body sensor networks with dynamic postural partitioning. Ad Hoc Networks, 8(8), 824-841.
49. Braem, B., Latre, B., Moerman, I., Blondia, C., & Demeester, P. (2006, July). The wireless autonomous spanning tree protocol for multihop wireless body area networks. In 2006 Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (pp. 1-8). IEEE.
50. Braem, B., Latré, B., Blondia, C., Moerman, I., & Demeester, P. (2008, August). Improving reliability in multi-hop body sensor networks. In Sensor Technologies and Applications, 2008. SENSORCOMM'08. Second International Conference on (pp. 342-347). IEEE.
51. Ruzzelli, A. G., Jurdak, R., O'Hare, G. M., & Van Der Stok, P. (2007, June). Energy-efficient multi-hop medical sensor networking. In Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments (pp. 37-42). ACM.
52. Bag, A., & Bassiouni, M. A. (2009). Biocomm–A cross-layer medium access control (MAC) and routing protocol co-design for biomedical sensor networks. International Journal of Parallel, Emergent and Distributed Systems, 24(1), 85-103.
53. Djenouri, D., & Balasingham, I. (2009, September). New QoS and geographical routing in wireless biomedical sensor networks. In 2009 Sixth International Conference on Broadband Communications, Networks, and Systems (pp. 1-8). IEEE.
54. Ye, W., Heidemann, J., & Estrin, D. (2002). An energy-efficient MAC protocol for wireless sensor networks. In INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 3, pp. 1567-1576). IEEE.
55. Van Dam, T., & Langendoen, K. (2003, November). An adaptive energy-efficient MAC protocol for wireless sensor networks. In Proceedings of the 1st international conference on Embedded networked sensor systems (pp. 171-180). ACM.
56. Polastre, J., Hill, J., & Culler, D. (2004, November). Versatile low power media access for wireless sensor networks. In Proceedings of the 2nd international conference on Embedded networked sensor systems (pp. 95-107). ACM.
57. Khan, N. P., & Boncelet, C. (2006, October). PMAC: Energy efficient medium access control protocol for wireless sensor networks. In MILCOM 2006-2006 IEEE Military Communications conference (pp. 1-5). IEEE.
58. Lu, G., Krishnamachari, B., & Raghavendra, C. S. (2004, April). An adaptive energy-efficient and low-latency MAC for data gathering in wireless sensor networks. In Parallel and Distributed Processing Symposium, 2004. Proceedings. 18th International (p. 224). IEEE.
59. Pei, G., & Chien, C. (2001). Low power TDMA in large wireless sensor networks. In Military Communications Conference, 2001. MILCOM 2001. Commu- nications for Network-Centric Operations: Creating the Information Force. IEEE (Vol. 1, pp. 347-351). IEEE.
60. Heinzelman, W. B., Chandrakasan, A. P., & Balakrishnan, H. (2002). An application-specific protocol architecture for wireless microsensor networks. IEEE Transactions on wireless communications, 1(4), 660-670.
61. Rajendran, V., Garcia-Luna-Aveces, J. J., & Obraczka, K. (2005, November). Energy-efficient, application-aware medium access for sensor networks. In IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005. (pp. 8-pp). IEEE.
62. Younis, O., & Fahmy, S. (2004). HEED: a hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks. IEEE Transactions on mobile computing, 3(4), 366-379.
63. H.M. Li and J.D. Tan. "Heartbeat driven MAC for body sensor networks", In Proc of the 1st ACM SIGMOBILE international workshop on systems and networking support for healthcare and assisted living environments, San Juan, Puerto Rico, pp. 25-30, Jun. 2007.
64. Changle, L. I., Huan-Bang, L. I., & Kohno, R. (2009). Reservation-based dynamic TDMA protocol for medical body area networks. IEICE transactions on communications, 92(2), 387-395.
65. Otal, B., Alonso, L., & Verikoukis, C. (2009). Highly reliable energy-saving MAC for wireless body sensor networks in healthcare systems. IEEE Journal on Selected Areas in Communications, 27(4), 553-565.
66. Su, H., & Zhang, X. (2009). Battery-dynamics driven TDMA MAC protocols for wireless body-area monitoring networks in healthcare applications. IEEE Journal on selected areas in communications, 27(4), 424-434.
67. Li, C., Wang, L., Li, J., Zhen, B., Li, H. B., & Kohno, R. (2009, September). Scalable and robust medium access control protocol in wireless body area networks. In PIMRC (pp. 2127-2131).
68. Li, C., Li, J., Zhen, B., Li, H. B., & Kohno, R. (2010). Hybrid unified-slot access protocol for wireless body area networks. International Journal of Wireless Information Networks, 17(3-4), 150-161.

69. Omeni, O., Wong, A. C. W., Burdett, A. J., & Toumazou, C. (2008). Energy efficient medium access protocol for wireless medical body area sensor networks. IEEE Transactions on biomedical circuits and systems, 2(4), 251-259.
70. Timmons, N. F., & Scanlon, W. G. (2009, May). An adaptive energy efficient MAC protocol for the medical body area network. In Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology, 2009. Wireless VITAE 2009. 1st International Conference on (pp. 587-593). IEEE.
71. Marinkovic, S. J., Popovici, E. M., Spagnol, C., Faul, S., & Marnane, W. P. (2009). Energy-efficient low duty cycle MAC protocol for wireless body area networks. IEEE Transactions on Information Technology in Biomedicine, 13(6), 915-925.
72. Ye, W., Silva, F., & Heidemann, J. (2006, October). Ultra-low duty cycle MAC with scheduled channel polling. In Proceedings of the 4th international conference on Embedded networked sensor systems (pp. 321-334). ACM.
73. Fang, G., & Dutkiewicz, E. (2009, September). BodyMAC: Energy efficient TDMA-based MAC protocol for wireless body area networks. In Communications and Information Technology, 2009. ISCIT 2009. 9th International Symposium on (pp. 1455-1459). IEEE.

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Securing Cluster Head Selection in Wireless Sensor Networks

By Rupinder Singh, Dr. Jatinder Singh & Dr. Ravinder Singh
Khalsa College

Abstract- Wireless Sensor network routing protocols are prone to various attacks as these protocols mainly provide the function of routing data towards the sink. LEACH is a one of the routing protocol used for clustered implementation of wireless sensor network with Received Signal Strength based dynamic selection of Cluster Heads. But, as with other routing protocols, LEACH is also prone to HELLO flood attack when the malicious sensor node becomes the Cluster Head. Cryptographic and non-cryptographic approaches to detect the presence of HELLO flood attack also exist but they lack efficiency in some way. In this paper, an efficient protocol is proposed for the detection and prevention of HELLO Flood attack in wireless sensor network. Cluster heads are vulnerable to various malicious attacks and this greatly affects the performance of the wireless sensor network. Cryptographic approaches to prevent this attack are not so helpful though some non-cryptographic methods to detect the HELLO Flood attack also exist but they are not too efficient as they result in large test packet overhead.

Keywords: *wireless sensor networks, leach, hello flood attack, armstrong number, aes, encryption, decryption, cluster head.*

GJCST-E Classification: *C.2.1, I.2.9*

Strictly as per the compliance and regulations of:

Securing Cluster Head Selection in Wireless Sensor Networks

Rupinder Singh [α], Dr. Jatinder Singh [σ] & Dr. Ravinder Singh [ρ]

Abstract- Wireless Sensor network routing protocols are prone to various attacks as these protocols mainly provide the function of routing data towards the sink. LEACH is a one of the routing protocol used for clustered implementation of wireless sensor network with Received Signal Strength based dynamic selection of Cluster Heads. But, as with other routing protocols, LEACH is also prone to HELLO flood attack when the malicious sensor node becomes the Cluster Head. Cryptographic and non-cryptographic approaches to detect the presence of HELLO flood attack also exist but they lack efficiency in some way. In this paper, an efficient protocol is proposed for the detection and prevention of HELLO Flood attack in wireless sensor network. Cluster heads are vulnerable to various malicious attacks and this greatly affects the performance of the wireless sensor network. Cryptographic approaches to prevent this attack are not so helpful though some non-cryptographic methods to detect the HELLO Flood attack also exist but they are not too efficient as they result in large test packet overhead. In this paper, we propose HRSRP (Hello flood attack Resistant Secure Routing Protocol) extension to LEACH protocol so as to protect the cluster head against Hello flood attack. HRSRP is base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of cluster head. The proposed technique is implemented in NS2, the experimental results clearly indicate the proposed technique has significant capability for the detection of hello flood attack launched for making the malicious node as the cluster head.

Keywords: wireless sensor networks, leach, hello flood attack, armstrong number, aes, encryption, decryption, cluster head.

I. Introduction

Wireless Sensor Network (WSN) is an infrastructure-less and self-configured wireless networks which is used to monitor physical conditions or environment such as sound, humidity, temperature, pressure, speed, pollutant levels etc. and so on. Sensors in WSN pass the data gathered to Base Station (BS) so that it can be further analyzed for further processing to take different decisions. Figure 1 shows the structure of a typical WSN. Sensor nodes in a WSN are very resource constrained and are susceptible to various attacks due to limited capacity of data processing, speed, storage, communication bandwidth etc. The complication of the implemented security algorithms also adds to the trouble of providing security to WSNs.The past proposed security techniques for WS Ns assumed that almost all sensor nodes are reliable and helpful, but the same is not true for most of the cases for many sensor network applications today. A large number of attacks are possible in WSN including jamming, tampering, exhausting, hello flood, collision, sinkhole, Sybil, denial-of-service, flooding, cloning etc.

Hello flood attack is a network layer attack in WSN caused when hello packets used for neighbour discovery are sent or replayed by an attacker with high transmission power. In this way, the attacker creates an illusion of being a neighbour to other sensor nodes so that the underlying routing protocol can be disrupted, which smooth the progress of launching further types of attacks. The attacker broadcast packets with such a high transmission power that a large number of sensor nodes in the WSN choose it as the parent node or cluster head (CH) in case of clustered implementation. All messages to be broadcasted in the WSN are routed through this parent sensor node that increases delay. The attacker broadcast these hello messages to a large number of sensor nodes in a wide area of the WSN. These sensor nodes are then forced to be convinced that the attacker node in the network is their neighbour. All the sensor nodes are going to reply to this HELLO message from the attacker and are going to waste their energy. This usually results in a confusion state in the WSN.

Heinzelman et al. [2] introduced a dynamic hierarchical clustering protocol called LEACH (Low Energy Adaptive

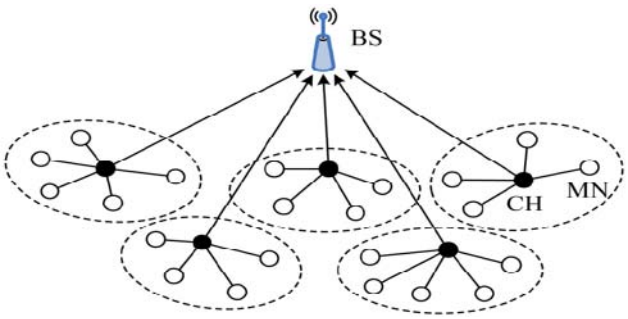

Figure 1: A typical WSN

Clustering Hierarchy) protocol for sensor networks. LEACH divides the WSN into small clusters of which one is the CH head and others sensor nodes are the cluster members. The cluster sensor node members send their gathered data to the CH, which in turn send it to the BS

Author α: Research Scholar, IKG PTU, Kapurthala, Punjab.
e-mail: rupi_singh76@yahoo.com
Author σ ρ: IKG PTU, Kapurthala, Punjab.
e-mail: bal_jatinder@rediffmail.com

by aggregating all the received data from its cluster members so as to reduce the redundancy. In LEACH the CH sensor nodes are periodically re-elected so that the same sensor node is not repeatedly used for the high energy job of the CH. LEACH operations are divided into two phases of Setup phase and Steady phase. In the setup phase, the formation of clusters with CH and cluster members is done for the WSN while in the steady phase; data are sensed and sent to the BS. The steady phase is longer than the setup phase and is done in order to minimize the overhead cost.

LEACH protocol is a more secure protocol as compared to the conventional multi-hop protocols as in conventional multi-hop protocols, the sensor nodes around the BS are more attractive to compromise as they are the major points of aggregation and forwarders of all packets to the BS. While in LEACH protocol, the CH are the only node that directly communicate with the BS and the location of these CH can be anywhere in the WSN irrespective of the BS. More over these CHs are regularly randomly changed. Therefore, spotting these CHs is very hard for the adversary in WSN. However, as LEACH is a cluster-based protocol, depending exclusively on the CHs for aggregation of data and its routing, attacks on the CH are the most harmful. If any adversary node becomes a CH, then it can make possible attacks like HELLO flood attack, Sybil attack, selective forwarding etc.

Hello packets in WSN are used for neighbour discovery but they can be used by a malicious node with high transmission power to launch Hello flood attack on CHs in WSN. A number of countermeasures against Hello flood attack in WSN have been proposed in the literature that we discussed in our previous work [1]. Most of the proposed countermeasures have limitation and need improvement for producing more efficient one. In this paper, we propose a HRSRP (Hello flood attack Resistant Secure Routing Protocol), an extension to LEACH protocol and is base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of the CH so as to prevent the WSN from Hello flood attack. The remaining paper is organised as follows: In section II, we discuss related works; the section III describes the working of HRSRP. In section IV, we provide the simulation of proposed protocol in NS2 while we end with the conclusion in section V.

II. Related Works

In this section of the paper, we discuss the work proposed in the past for providing secure formation of clusters by LEACH protocol in WSN, and the proposed work for selecting CHs in a secure way.

Heinzelman et al. [2] proposed LEACH in which every sensor has a probability of becoming a CH without message exchange. This technique attempted to extend the network life time by making all sensor nodes play a role of CH. In LEACH, some sensor nodes with a high chance declare themselves as CHs and other sensor nodes join in one of them. Since, this method assumes no compromised sensor nodes in the WSN; it has no method to protect the cluster formation from the malicious sensor nodes. F-LEACH [3] was proposed in order to defend the cluster formation in LEACH protocol. In this proposal, when a sensor node declares itself as a CH, it employs the use of common keys shared with the BS so as to check the authentication of the CH declaration to the BS. Then, the sink securely broadcasts the authenticated CHs using μTESLA [4]. Normal sensor nodes in WSN join in only one legitimate CH. However, this method has no means to validate the normal sensor nodes which join in any cluster. To resolve this problem, Oliveira et al. [5] proposed SecLEACH in which the BS authenticates the CH nodes and further the CHs authenticate the joining sensor nodes. In both F-LEACH and SecLEACH, sensors nodes are pre-assigned some keys for verification before their deployment. However, both F-LEACH and SecLEACH can help in preventing only external attackers from joining of the process of cluster formation i.e. they cannot avoid internal attacks from capturing CHs.

Many extensions to LEACH [7-11] have been proposed in the past but, most of them focus on balancing the consumption of energy over all sensor nodes and extending the lifetime of the network. A few of them [8] deals with electing a CH securely. However, this technique cannot prevent a malicious node from declaring itself as a CH as it can defraud other nodes that it has a short distance to the BS along with a large amount of residual energy. Liu proposed a cluster formation method in which only pre-determined nodes can declare themselves as CHs while other nodes can join any cluster either directly or via a relay node [13]. As any CH declaration or cluster join is authenticated by some pre-assigned polynomial share, the method avoids any external attacker from participating in the process of cluster formation. In this method, a compromised relay node can invoke a Denial of Service (DoS) attack by removing the connection between CH and its serving nodes. Pre-determined CHs become the targets of attackers because their roles are fixed. Sun et al. [14] proposed a protected scheme for cluster formation which checks the protocol conformity of nodes in order to discriminate mean nodes from usual nodes. In this method, physical network is transformed into cliques and members are openly connected to each other in a clique. After the formation of clique, each node checks that all members have the similar view of the clique membership. Even though the method of [19] has enhanced the safety of [14], it supposed that no collisions are possible during the cluster formation. This assumption is difficult to satisfy without the use of any special measure such as TDMA schedule assignment and code separation. Nishimura et al. [21] proposed a method where all nodes allocate a trust value to each

candidate of CH and the most trusted nodes are allowed to become CH. Otherwise, the nodes join a close cluster to form clusters in the network. The drawback of this scheme is that it produces a lot of communication overhead for the building of trust evaluation system. So, this method is not appropriate for resource-constrained WSNs.

Rifà-Pous et al. [20] proposed a protected cluster formation method that is based on public key cryptography. The scheme is composed of three phases; cluster discovery phase, CH designation phase, and cluster maintenance phase. In the phase of cluster discovery, all nodes in a cluster have the same view on the membership of cluster with each other. In the phase of cluster designation, a CH is elected considering the number times it performed the CH and number of its neighbours. In the phase of cluster maintenance, the elected CHs provide an authorization certificate to every member in the cluster. But, this method assumes that no nodes depart from the cluster discovery protocol. For example, if a malicious node transmits its message to part nodes in the phase of cluster discovery, the sufferers have a dissimilar view on the membership of cluster. Consequently, it divides a cluster into multiple clusters, and the divided clusters elect their CH respectively in the phase of CH designation. That is to say, this method can produce a lot of clusters under the selective transmission attack. Crosby et al. [21] proposed a trust based CH election design where every node provides a trust value to other nodes according to their behaviour and extremely trustworthy nodes become CHs. Every node's behaviour is calculated by counting the occurrence of successful node transmissions and the occurrence of unsuccessful node transmissions. That is, the more a node succeeds in its transmission, the superior reputation value the node has. During the election of new CH, nodes with a more reputation value are suggested for the role of CH by cluster members and one of these is selected as a new CH. A malicious CH can put in a not guilty victim into a blacklist to take away its candidacy for CH in the cluster that is, with the number of blameless victims rises up, a malicious node can enlarge its winning chance.

Buttyan et al. [22] also proposed a CH selection method which conceals the process of election from outside nodes using cryptographic techniques. However, the concealment works only for external attackers as a compromised node can with no trouble expose the selection result. Moreover, the malicious node can announce itself as a CH even though it is not eligible. Sirivianos et al. [24] proposed the Secure Aggregator Node Election (SANE) protocol in which all eligible CH members in a cluster contribute to the production of a random value and a CH is elected randomly using this random value. SANE is classified into further three sub-schemes according to generating and distributing the random value. They are based on Merkle's puzzle scheme, commitment based scheme, and seed based scheme. Dong et al. [25] proposed a method that prevents outside attackers from taking part in a CH election process through its ID assignment scheme, which firmly binds a node's ID, its commitments, and its polynomial shares. In this scheme, the nodes that do not broadcast participation message for CH election or explicitly transmit a non-participation message are excluded from the CH candidates. The final CH is selected by arbitrarily selecting one node amongst the rest of the candidates. However, an inside attacker can change CH election result by avoiding the distribution of its participation message; it can also generate numerous CH election results by the process of distributing its contribution message only to a subset of CH candidates. Even though this method has a recovery system to combine numerous election results into one result, it requires the voluntary co-operation of the CH candidates.

III. Framework and Working of HRSRP

In this section of the paper, we describe our proposed HRSRP for the detection and isolation of Hello flood attack in WSN. We first discuss the WSN model and assumption and then we describe the working of proposed protocol.

a) Network Model

The clustered sensor network selected in the paper consists of N static sensor nodes, including CH, member nodes, and BS. CHs are responsible for collecting the information within their clusters and passing it to the BS so as to make decisions and judgments. The formation of clusters is based on LEACH protocol. Every sensor node has a unique identity (ID). Following assumptions of the WSN are used in the proposed protocol HRSRP.

1. Hello flooding attack node, formed by the compromise of CH.
2. The compromised node has a high transmission power.
3. Except the malicious sensor node, all the nodes in wireless sensor network are isomorphic with the same initial energy, transmission power, computing power and internal storage structure.
4. Once each node's ID is allocated, it cannot be changed.
5. Each sensor node is allocated unique Armstrong number.
6. The sensor nodes of the network consume the same energy in the same stage of the work, e.g. the transmission and reception of data packets in the process of detection.

b) Implementation of HRSRP

The HRSRP is an improved secure extension to the LEACH protocol, so the implementation of the

proposed protocol has to take advantage of the characteristic of LEACH clustering. LEACH protocol is mainly divided into two phases of set-up phase and stable phase. In the set-up phase, all the sensor nodes have to follow the two guidelines of fairness criterion and randomness criterion. In fairness criteria all sensor nodes in the network have same probability to become a CH. While in randomness criterion, the election of the CH is done in a random way. The chance for a sensor node to become a CH in the round entirely depends on whether the sensor node has ever been elected as CH in the recent rounds and the percentage of the CH sensor in the WSN. When the election of the CH is over, every member node chooses the cluster to join on the basis of the maximum received signal strength until all the clusters are completed. In general, the implementation of LEACH has a longer stabilization phase.

Each member sensor node is responsible for sensing the surrounding environment and forwarding the data to their respective CHs. After collecting information from cluster member nodes, each CH forwards it to the BS. It is vulnerable for LEACH against Hello flood attack due to these characteristics of clustering. Hello flood attack is a common routing attack in the network, which broadcasts a large number of hello message with higher transmission power to nodes in the network. Any sensor node that receives the hello message with high signal will consider the malicious node as CH. This malicious node may damage the network by selectively modifying, discarding information received from its neighbours.

c) *Determination of malicious CH*

The BS maintains record of CHs, cluster members, malicious nodes in the registration table as different sets. The values are updated as per the changes in the clusters and CHs. The initial values of these sets are

Set CH_{node} = {null}, the CHs in the network.

Set CH_{member} = {null}, the members of each cluster in the network.

Set $CH_{malicious}$ = {null}, which means the malicious nodes in the network.

Each sensor node with a certain probability (p) try for becoming CH based on the criterion of randomness and fairness. The sensor node that becomes a CH broadcasts the message of self-clustering in order to attract neighbouring sensor nodes so as to join it. The cluster head CH(i) is selected according to the level of the Received Signal Strength (RSS) to join in a certain range of area. The members of the cluster as calculated by each CH are added to the set CH_{member}.

i. *Allocation of unique ID*

The BS allocates a unique ID to each sensor in the network. Whenever any sensor node request for becoming CH, it has to send this ID to the BS so that the node identification can be validated.

ii. *Allocation of unique Armstrong number*

The BS also allocates a unique Armstrong number against each ID for each of the sensor node in the network. An Armstrong number is an m-digit base n number such that the sum of its (base n) digits raised to the power m is the number itself. For example number 371 is an Armstrong number as $3^3+7^3+1^3 = 27 + 343 + 1 = 371$ which is equals to number itself. Whenever any sensor node request for becoming CH, it has to send encrypted hello message with this Armstrong number. Table 1 shows example registration table maintained at BS.

Table 1: Registration table at BS

Sensor number	Allocated unique ID	Allocated Random Armstrong Number
001	S0001	153
002	S0002	407
.	.	.
.	.	.
N		54748

The flowchart in figure 2 describes the working of HRSRP for authentication of CH by the BS.

As LEACH is fragile to hello flooding attacks because of its characteristics and nature. The compromised non–cluster head sensor nodes have less effect on the performance of network with limit range. But, once it becomes a CH with higher transmission power, a large number of sensor nodes will be appealed for becoming one of its members in a cluster. If the malicious node discards or alters the packets, the circumstances would seriously smash the honesty and precision of the information in the network. The HRSRP can detect the presence of malicious node with fewer energy and small error rate, which can efficiently get better the network performance.

IV. Simulation Results

In this section of the paper, we present the results of the simulation to show the effectiveness of HRSRP. The simulation is carried out in ns2.35 with the parameters shown in table 2.

a) *Throughput*

In the first experiment, we measure the sensor network

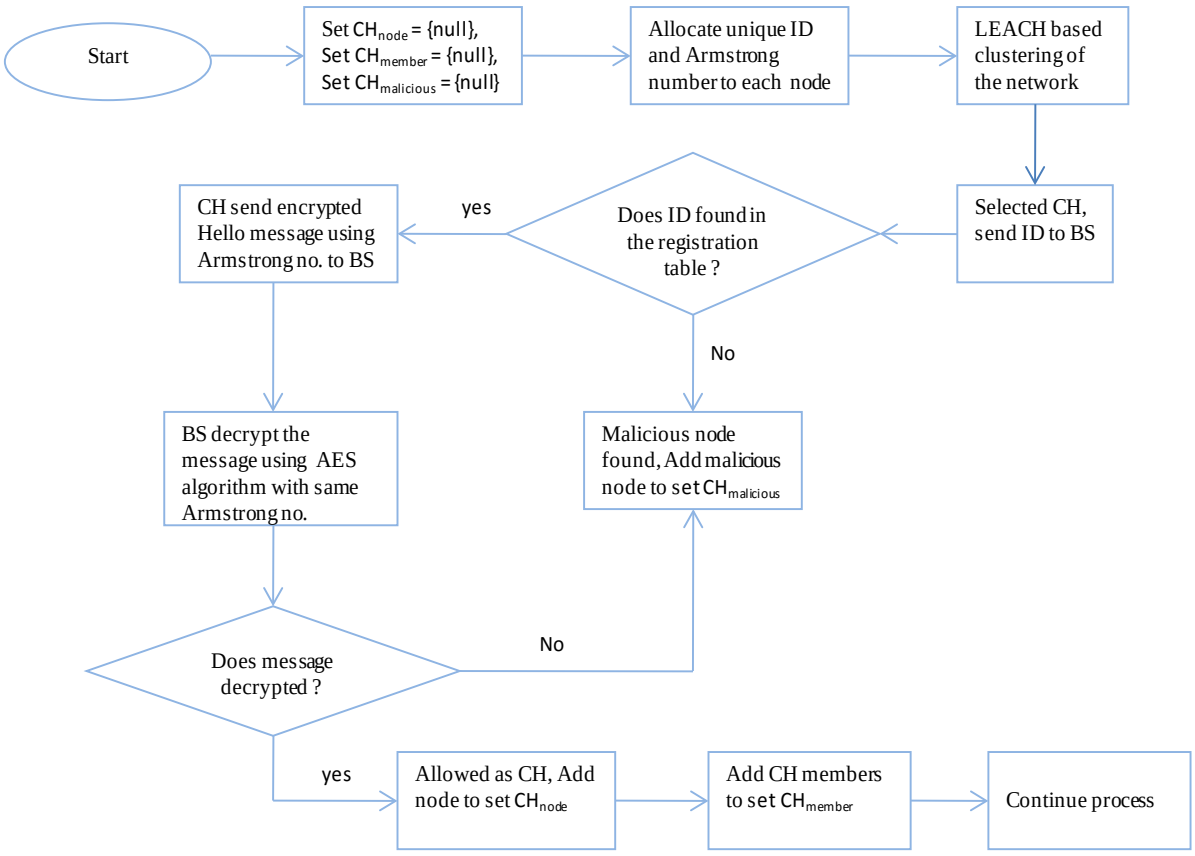

Figure 2: Flow chart of proposed HRSRP

Table 2: Simulation parameters

Parameter	Value
Simulator used	NS 2.35
Area (meter)	800X800
No. of nodes	50
Routing protocol	LEACH
Channel type	Wireless
Packet size	512 byte
Mobility model	Two ray ground propagation model

throughput as this is one of the crucial network parameters. Network throughput refers to the average rate of successfully delivered packets. Throughput is calculated depending on a total number of packets received at the destination in sensor network per unit of time. Throughput is calculated as

Throughput = (Total number of packets received at the destination) / (simulation time)

Figure 3 shows the throughput analysis in the case of the sensor network without Hello flood attack, under Hello flood attack, and after implementation of proposed HRSRP. The figure clearly shows that the proposed protocol after the isolation of the Hello flood attack results in the increase of throughput.

b) Packet delivery ratio

Packet delivery ratio (PDR) of a network is defined as the ratio of the total received packets at the destination to total packets generated by the source node. PDR is calculated as

PDR = (Packets received/packets generated) * 100

Figure 4 shows the PDR analysis in the case of the sensor network without Hello flood attack, under Hello flood attack, and after implementation of HRSRP. The figure clearly shows that the proposed protocol after the isolation of the Hello flood attack results in the increase of PDR. A high value of PDR is an indication that there is less packet loss in the sensor network.

c) Delay

The delay is defined as the average time taken by a packet (data) to arrive at the destination. The delay also includes any delay that is caused by the process of route discovery along with queue in data packet transmission. The data packets successfully delivered to the destinations are only counted. It is calculated as:

Delay =∑ (arrive time – send time) ∑ Number of connections

The lesser value of delay is an indicator of the better performance of the protocol. Figure 5 shows the end to end delay in the case of sensor network without Hello flood attack, under Hello flood attack, and after

implementation of HRSRP. The figure shows that the proposed protocol results in the decrease in end-to-end delay.

d) Overhead

Overhead is the excess time taken by the protocol to deliver the packets to the destination. Hello flood attack increases the overhead in the sensor network. The routing overhead is defined as the count of packets used for routing in the sensor network. Figure 6 shows overhead in the case of sensor network without Hello flood attack, under Hello flood attack, and after implementation of HRSRP. The proposed protocol results in decreasing the overhead of the network as shown in figure 6.

V. Conclusion

Cluster head selection in a secure way in clustered implementation of wireless sensor network is vital as all the cluster sensor members data to the base station is communicated through cluster head. Hello flood attack in wireless sensor network can be used for making a cluster head compromised by making use of high transmission power used for sending or replaying hello packets which are used for neighbour discovery. LEACH protocol is hard to attack by adversary excluding the case when it can become cluster head. In this paper, a new approach to detect and prevent HELLO Flood attack in LEACH protocol in wireless sensor networks is proposed. We propose a HRSRP (Hello flood attack Resistant Secure Routing Protocol) extension to LEACH protocol base on encryption using Armstrong number and decryption using AES algorithm to verify the identity of cluster head. HRSRP improves the network performance by early discovery of adversary and preventing the sensor nodes from associating with such a malicious cluster head. The implementation of the proposed technique in NS2 shows its efficiency for the factors of throughput, packet delivery ratio, delay, overhead. The simulation results prove that HRSRP expels more compromised nodes from clusters and suppresses the separation of clusters. Other simulation results also represent that HRSRP raises the quality of clusters and more energy efficient than an opponent scheme. Additional simulation will be done in the future by increasing the number of sensor nodes.

VI. Acknowledgement

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab for providing opportunity to conduct this research work.

References Références Referencias

1. Rupinder Singh, Dr. Jatinder Singh, and Dr. Ravinder Singh, “Hello flood attack Countermeasures in Wireless Sensor Networks,” International Journal of Computer Science and Mobile Applications, Vol. 4, Issue 5, April 2016, pp. 1-9.
2. W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy-efficient communication protocol for wireless microsensor networks," In the proceedings of the 33rd Annual Hawaii International Conference on System Sciences, Vol. 2, Jan. 2000.
3. A.C. Ferreira, M. A. Vilaca, L. B. Oliveira, E. Habib, H.C. Wong, and A. A. Loureiro, “On the security of cluster-based communication protocols for wireless sensor networks,” Proc. of 4th IEEE Int’l Conf. on Networking, Reunion Island, France, Apr. 17-21, 2005.
4. A. Perrig et al., “SPINS: Security Protocols for Sensor Networks,” Wireless Networks, Vol. 8, No. 5, pp. 521 -534, Sep. 2002.
5. L. B. Oliveira, H.C. Wong, M. W. Bern, R. Dahab, and A. A. Loureiro, “SecLEACH-a random key distribution solution for securing clustered sensor networks,” Proc. of 5th IEEE Int’l Symp. on Network Computing and Applications, Cambridge, Massachusetts, USA, Jul. 24-26, 2006
6. Yaya Shen, Sanyang Liu, Zhaohui Zhang, “Detection of Hello Flood Attack Caused by Malicious Cluster Heads on LEACH Protocol,” International Journal of Advancements in Computing Technology (IJACT), Volume 7, Number 2, March 2015.
7. S. Kang and T. Nguyen, “Distance Based Thresholds for Cluster Head Selection in Wireless Sensor Networks,” IEEE Communications Letters, vol. 16, no. 9, pp. 1396-1399, Sep. 2012.
8. Y. Han, M. Park, and T. Chung, “SecDEACH: Secure and Resilient Dynamic Clustering Protocol Preserving Data Privacy in WSNs,” Proc. of the 2010 Int’l Conf. On Computational Science and Its Applications, LectureNotes in Computer Science, vol. 6018, pp. 142-157, 2010.
9. V. Katiyar, N. Cand, G. C. Gautam, and A. Kumar, “Improvement in LEACH Protocol for Large-scale Wireless Sensor Networks,” Proc. of Int’l Conf. On Emerging Trends in Electrical and Computer Technology, pp. 1070-1075, Mar. 2011.
10. M. Saadat , R. Saadat, ang G. Mirjality, “Improving Threshold Assignment for Cluster Head Selection in Hierarchical Wireless Sensor Networks,” Proc. of Int’l Symposium on Telecommunications, pp. 409-414, Dec. 2010.
11. P. Ren, J. Qian, L. Li, Z. Zhao, and X. Li, “Unequal Clustering Scheme based LEACH for Wireless Sensor Networks,” Proc. of Fourth Int’l Conf. on Genetic and Evolutionary Computing, pp. 90-93, Dec. 2010.
12. Gayatri Devi, Rajeeb Sankar Bal, Nibedita Sahoo, “Hello Flood Attack Using BAP in Wireless Sensor Network,” International Journal of Advanced

Engineering Research and Science, Vol. 2, Issue 1, ISSN: 2349-6495, Jan. 2015.
13. D. Liu, "Resilient Cluster Formation for Sensor Networks," Proc. of 27th Int'l Conf. on Distributed Computing Systems (ICDCS '07), pp.40-48, 2007
14. K. Sun et al., "Secure Distributed Cluster Formation in Wireless Sensor Networks," Proc. of 22nd Annual Computer Security Applications Conference (ACSAC'06), pp. 131-140, 2006
15. S. Mayur, H. D. Ranjith, "Security Enhancement on LEACH Protocol From HELLO Flood Attack in WSN Using LDK Scheme," International Journal of Innovative Research in Science, Engineering and Technology, Vol. 4, Issue 3, ISSN (Online): 2319 – 8753, ISSN (Print): 2347 – 6710, March 2015.
16. S. Rawan, M. Suhare, A. Manal, "Intrusion Detection of Hello Flood Attack in WSNs Using Location Verification Scheme," International Journal of Computer and Communication Engineering, Volume 4, Number 3. May 2015.
17. Dilpreet Kaur, Rupinderpal Singh, "Energy level based Hello Flood attack Mitigation on WSN," International Journal of Embedded Systems and Computer Engineering, ISSN 23213361, July 2015.
18. Jyoti, Ashu Bansal, "Detection of Hello Flood Attack on Leach Protocol Based on Energy of Attacker Node," International Journal of Innovations & Advancement in Computer Science, Volume 4, ISSN 2347 – 8616, September 2015.
19. G. Wang, D. Kim, and G. Cho, "A Secure Cluster Formation Scheme in Wireless Sensor Networks," Int'l Journal of Distributed Sensor Networks, vol. 2012, Article ID 301750, 14 pages, 2012.
20. H. Rifà-Pous and J. Herrera-Joancomartí, "A Fair and Secure Cluster Formation Process for Ad Hoc Networks,"
Wireless Communications, Vol. 56, No. 3, pp. 625-636, 2011.
21. G. V. Crosby and N. Pissinou, "Cluster-based Reputation and Trust for Wireless Sensor Networks," Proc. of the 4th IEEE Consumer Communications and Networking Conference (CCNC '07), pp. 604-608, 2007.
22. L. Buttyan and T. Holczer, "Private Cluster Head Election in Wireless Sensor Networks," Proc. of the Fifth IEEE Int'l Workshop on Wireless and Sensor Network Security (WSN '09), IEEE, pp. 1048-1053, 2009.
23. Shikha Magotra, Krishan Kumar, "Detection of HELLO flood Attack on LEACH Protocol," IEEE International Advance Computing Conference (IACC), 2014.
24. M. Sirivianos et al., "Non-manipulable Aggregator Node Election Protocols for Wireless Sensor Networks," Proc. of Int'l Sympo. on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt '07), Cyprus, pp. 1-10, Apr. 2007.
25. Q. Dong and D. Liu, "Resilient Cluster Leader Election for Wireless Sensor Networks," Proc. of IEEE 6th Annual Comm. Society Conf. on Sensor, Mesh and Ad Hoc Communications and Networks(SECON), pp108-116, 2009.
26. I. Nishimura, T. Nagase, Y. Takehana, and Y. Yoshioka, "Secure Clustering for Building Certificate Mangement Nodes in Ad-Hoc Networks," Proc. of 14th Int'l Conf. On Network-Based Information Systems (NBiS), Tirana, Albania, Sep. 07-09, 2011
27. J. Steffi, Agino Priyanka, S. Tephillah, and A. M. Balamurugan, "Attacks and countermeasures in WSN," International Journal of Electronics & Communication, Volume 2, Issue 1, ISSN 23215984, January 2014.
28. Satwinder Kaur Saini, Mansi Gupta, "Detection of Malicious Cluster Head causing Hello Flood Attack in LEACH Protocol in Wireless Sensor Networks," International Journal of Application or Innovation in Engineering & Management (IJAIEM), Volume 3, Issue 5, ISSN 2319 – 4847, May 2014.
29. Akhil Dubey, Deepak Meena, Shaili Gaur, "A Survey in Hello Flood Attack in Wireless Sensor Networks," International Journal of Engineering Research & Technology (IJERT), Vol. 3, Issue 1, ISSN: 2278-0181, January 2014.
30. Virendra Pal Singh, S. Aishwarya, Anand Ukey, and Sweta Jain, "Signal Strength based Hello Flood Attack Detection and Prevention in Wireless Sensor Networks," International Journal of Computer Applications, Volume 62, No.15. January 2013.
31. Nusrat Fatema, Remus Brad, "Attacks and counterattacks on wireless sensor networks," International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol. 4, No. 6. December 2013.
32. A.Anup wanjari, Vidya Dhamdhere, "Evading Flooding Attack in MANET Using Node Authentication," International Journal of Science and Research (IJSR), Volume 3, Issue 12, ISSN (Online): 2319-7064, December 2014.
33. Mohammad Sayad Haghighi, Kamal Mohamedpour, Vijay Varadharajan, and Barry G. Quinn, "Stochastic Modeling of Hello Flooding in Slotted CSMA/CA Wireless Sensor Networks," IEEE transactions on information forensics and security, Vol. 6, No. 4, December 2011.
34. Virendra Pal Singh, Sweta Jain, and Jyoti Singhai, "Hello Flood Attack and its Countermeasures in Wireless Sensor Networks," International Journal of Computer Science Issues, Vol. 7, Issue 3, No. 11, ISSN 1694-0814, May 2010.
35. C.Venkata, Mukesh Singhal, James Royalty, and Srilekha Varanasi, "Security in wireless sensor networks," Wireless communications and mobile computing Published online in Wiley Inder Science, 2006.

36. Mohamed Osama Khozium, "Hello Flood Counter Measure for Wireless Sensor Network," International Journal of Computer Science and Security, Volume 2, Issue 3, May 2008.
37. A. Hamid, Mamun Rashid, Choong Seon Hong, "Defense against lap-top class attacker in wireless sensor network," The 8th International Conference Advanced Communication Technology, Print ISBN: 89-5519-129-4, IEEE, 2006.
38. Waldir Ribeiro Pires J´ unior Thiago H. de Paula Figueiredo Hao Chi Wong, "Malicious Node Detection in Wireless Sensor Networks," 18th International Parallel and Distributed Processing Symposium, Print ISBN:0-7695-2132-0, IEEE, 2004.
39. Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A MAC Layer Based Defense Architecture for Reduction-of-Quality (RoQ) Attacks in Wireless LAN," International Journal of Computer Science and Information Security, Vol. 7, No. 1, 2010.
40. Jatinder Singh, Dr. Savita Gupta, and Dr. Lakhwinder Kaur, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks," The International Arab Journal of Information Technology, Vol. 9, No. 3. May 2012.

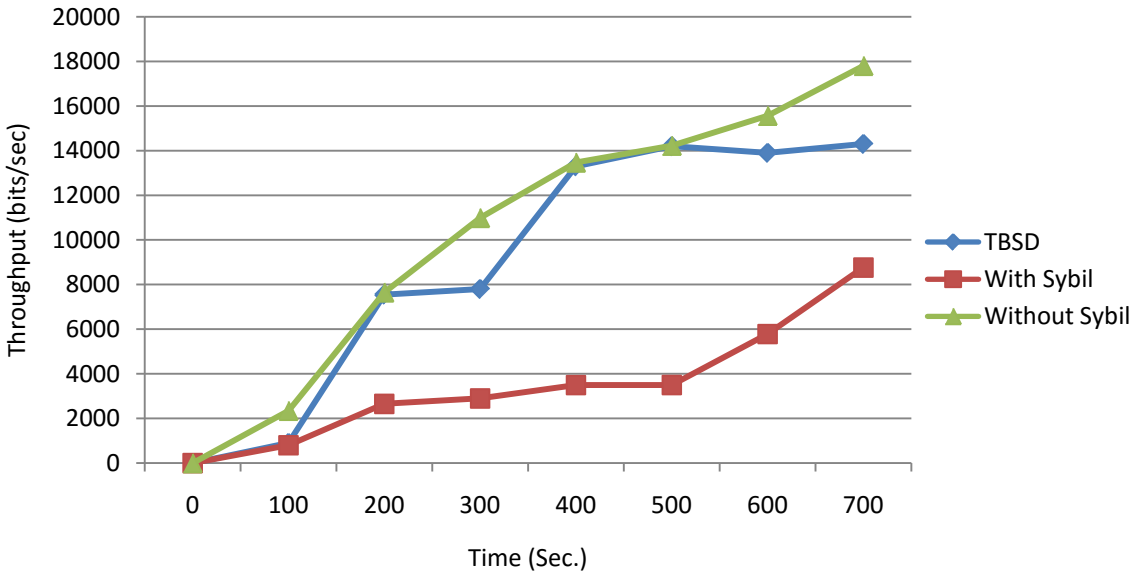

Figure 3: Throughput

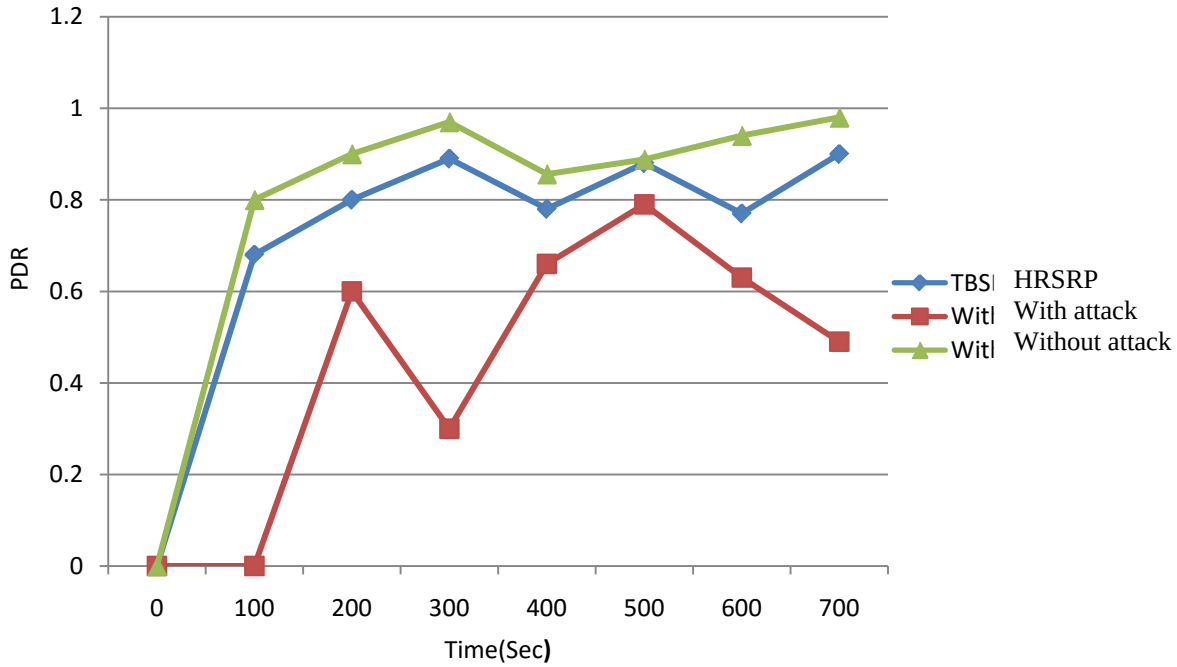

Figure 4: PDR

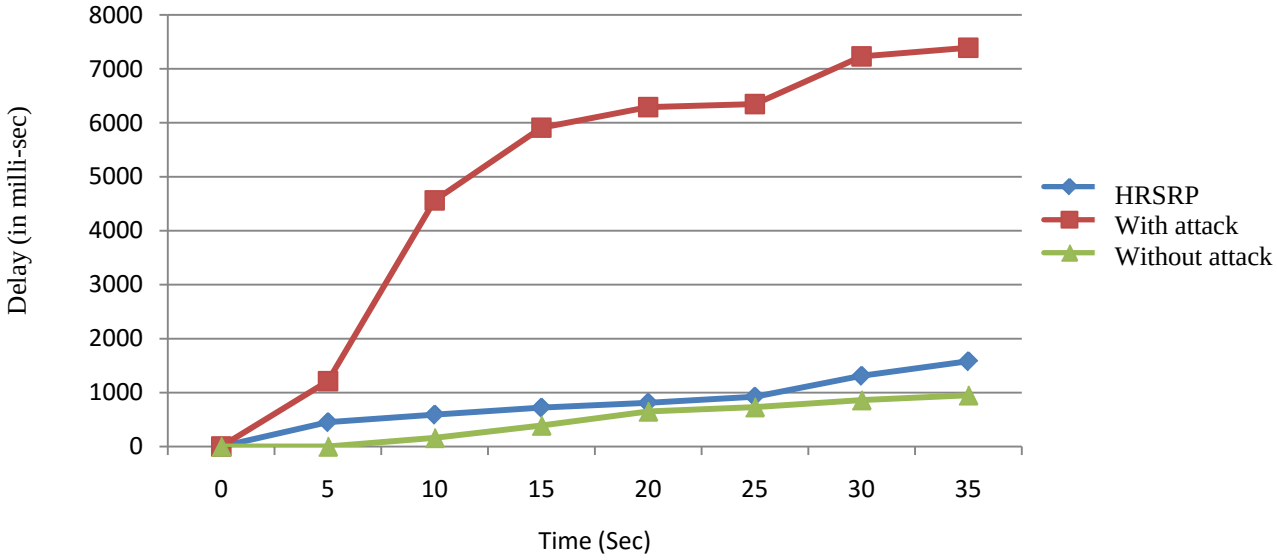

Figure 5: Delay

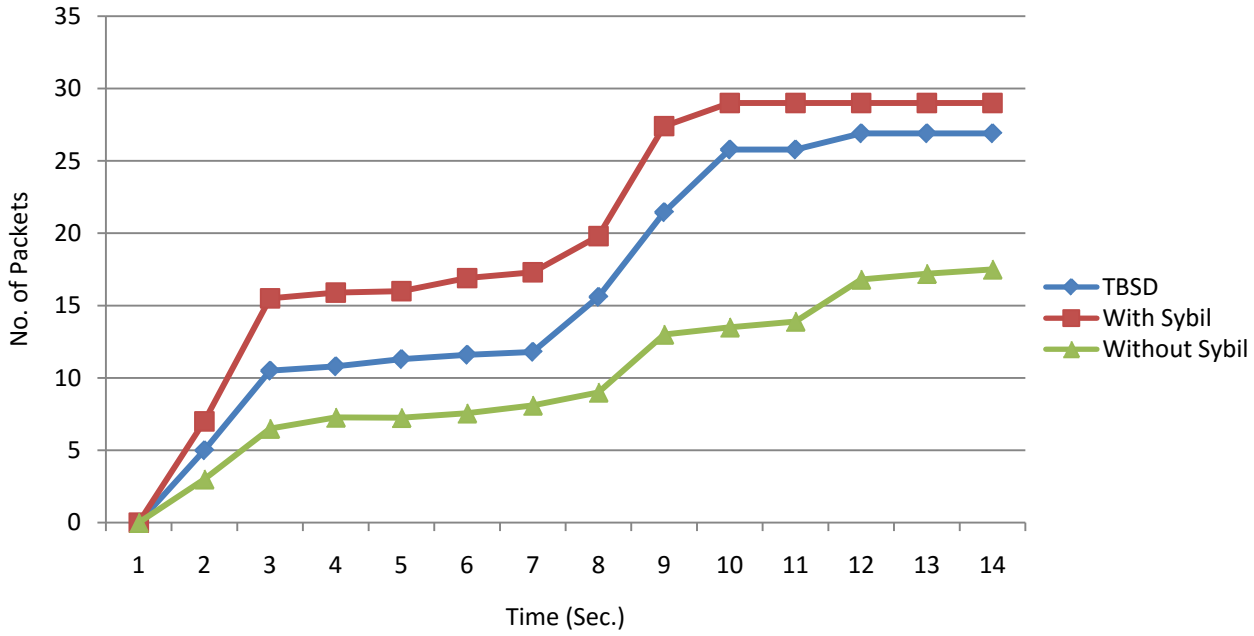

Figure 6: Overhead

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Multi-Channel Scheduling with Optimal Spectrum Channel Hole Filling (MCS-OSHF) for Cognitive Radio Wireless Networks

By N. Shribala, Dr. P. Srihari & Dr. B. C. Jinaga

Abstract- In this study, a contemporary method of scheduling algorithm has been proposed for working on scheduling of varying size data-frames transmission in CR based wireless networks. The objective of the proposed model is to achieve maximum throughput, and also reduction of loss of data-frames in the transmission. Some of the key elements that are considered in the development of the model are optimal bandwidth and idle channel availability. Using the three level hierarchical approach, the scheduling strategy is constructed. The optimal idle channel allocation, allocation with considerable transmission intervals allocation and optimal multiple channels models are considered at respective levels in the hierarchy in the proposed algorithm.

Keywords: secondary spectrum usage, cognitive radio network, quality of service, spectrum sensing, channel scheduling, spectrum hole filling.

GJCST-E Classification: I.3.7,C.2.1,I.2.9

Strictly as per the compliance and regulations of:

Multi-Channel Scheduling with Optimal Spectrum Channel Hole Filling (MCS-OSHF) for Cognitive Radio Wireless Networks

N. Shribala [α], Dr. P. Srihari [σ] & Dr. B. C. Jinaga [ρ]

Abstract- In this study, a contemporary method of scheduling algorithm has been proposed for working on scheduling of varying size data-frames transmission in CR based wireless networks. The objective of the proposed model is to achieve maximum throughput, and also reduction of loss of data-frames in the transmission. Some of the key elements that are considered in the development of the model are optimal bandwidth and idle channel availability. Using the three level hierarchical approach, the scheduling strategy is constructed. The optimal idle channel allocation, allocation with considerable transmission intervals allocation and optimal multiple channels models are considered at respective levels in the hierarchy in the proposed algorithm. The proposed model while tested under simulated environment in comparison to the other two bench marking models, the outcome depicts that the process is more efficient and supports in improving the overall process of scheduling of data-frames as per the desired objectives of the model.

Keywords: secondary spectrum usage, cognitive radio network, quality of service, spectrum sensing, channel scheduling, spectrum hole filling.

I. Introduction

Wireless communication systems are emerging much faster in terms of performance and efficiency, and the public radio spectrum bands do not have the scope of service for such advancements, as the bands were already licensed to the service providers earlier. Despite that, still there are many licensed spectrum bands that are underutilized in the spatial domain and also time domain [1].In order to utilize the unutilized spectrum band as opportunistic access for improving the efficiency of the spectrum usage, Cognitive Radio (CR) solutions are providing quality solutions. [2][3]. Spectrum and Channel sensing methods are introduced to handle one of the key issues envisaged with CR is about the protection of Primary Users (PUs) from any kind of interference resulting from Secondary Users (SUs) communications.

In the case of opportunistic access, SU shall identify any idle channels for the service, and can utilize the channel, but the crux is that irrespective of whether it focuses on the idle channel, still it has to ensure that current channel and additional channels are sensed. Only in such conditions, when a PU channel appears, SU can recover immediately the service channel. During the process of channel sensing, SU can't communication with other channels.

As per IEEE 802.16e Worldwide Interoperability for Microwave Access (WiMax) [4], the system allows the mobile station to perform channel scanning, by allowing mobile station to cut the communication with the base station, the efficacy of the process for QoS can be assured. But, in the case of IEEE 802.11 WLAN [5], such process is not facilitated unlike WiMax, and hence there shall be issues of packet losses and disruptions emerging due to channel scanning. To achieve the system with minimal QoS disruption, the interface of SU equipped with WLAN models has to be designed effectively.

This paper proposes the model of channel sensing scheduling which ensures interests of PUs are addressed, with the emphasis on sensing the channels only during the pre-defined time schedule, whilst managing the QoS for SUs for the delay and packet loss issues. As the interests of the PUs have to be given priority, certain level of SUs QoS may not be satisfied in the model.

In the further sections of this report, the emphasis is on, the literature pertaining the subject is discussed in section 2 and in section 3, the inputs related to proposed model of QoS-aware multichannel scheduling that has Optimal Spectrum Hole Filling model is proposed. Section -4 depicts the experimental results, and is followed by Section 5 with conclusion of the proposed model.

II. Related Work

Medium-Access-Control (MAC) protocols are adapted in using the DSA scheme for CRNs. In the case of MAC protocol, there are usually two phases predominantly, as contention phase and data transmission phase. In the contention phase, SUs rather than focusing on the common control channel shall focus on the idle licensed channels, through which successful SUs which shall take over the idle channels in the transmission phase. There is numerous protocol solutions defined in for MAC protocols. [6]-[9].

Author α: Department of ECE, BRECW ,Hyderabad, Telangana, India.
e-mail: shribalanagul71@gmail.com
Author σ: Department of ECE, GCET, Hyderabad, Telangana, India
e-mail: mail2pshari@yahoo.com
Author ρ: Department of ECE, JNTUH Hyderabad, Telangana, India.
e-mail: jinagabc@gmail.com

In [6], distributed MAC protocol was proposed which comprise the SUs having common channels for forming groups and for multiple groups some SUs performing as gateways. The data is transmitted by SUs using the data based on their success in the contention phase.

In the distributed MAC protocol proposed by Chen et al [7], SUs shall form clusters that are controlled by a group leader for each cluster, which conducts the contention and data transmission process. Also in another model proposed in [8], the distributed multi-channel MAC protocol was proposed in which SU pair gets the opportunity to sense and access during the contention phase, and use the available channels for the hardware constraint. In the case of distributed multi-channel MAC discussed in [9], all the available access channels that are sensed using the sensing policies are accessed by the SU paid during the contention phase.

In all the aforesaid conditions, there is high quantum of control overheads as the SUs usually contend in random manner for channels, certainly the outcome shall be much lower with the MAC protocols. [10] -[15]Whereas in the case of DSA that are implemented using scheduling algorithms that can achieve higher throughput. DAS system has the process in which at the beginning of every slot, information regarding bandwidth requirement is collected from the SUs by scheduler and it is broadcasted to common control channels. From the received schedule, the SUs access the corresponding channels for the slot time that is remaining, and the model is defined as slot-based scheduling schemes.

[10] Proposes the scheduling algorithm which is based on integer linear programming (ILP), which is a unique channel user pair that is activated for varied time instants within the slot. Models in [11] –[15] presents numerous scheduling algorithms which can support in maximizing the transmission capacity for the SUs which are presented. In the scheduling algorithm discussed in [11], certain factors like the fairness, traffic demand to the SUs, link capacity, and Signal-to-interference-and-noise ratio (SINR) are considered. Whereas, in [12], the factors like fading, interference, and packet waiting times are considered, unlike [13] in which the focus is upon throughput, maximum frequency and packet waiting time. In [14], that achieves proportional fairness for SUs, focus on packet waiting time and the interference caused due to SU to the PUs receiver, but in [15], the model focus on assigning the idle channels to SUs depending on if the signal-to-noise ratio (SNR_ shall be used at the receiving SU which could be highest for any given channel.

The information exchange taking place by the scheduler in the slot based scheduling schemes are even comprised in the scheduling overhead for the SUs in the beginning. Considerable quantum of slot time is lost in the communication to the scheduling overhead due to low bandwidth in the common control channel and because of such model, the effective transmission to the data channels are getting reduced and are constraining the throughput achievable. Also, the scheduling overhead works on increasing the number of channels that can work on SUs, and not any of the aforesaid [10]-[15] shall focus on issuing of scheduling overhead.

Review of the earlier models and the literature reflect that the scheduling overhead could majorly impact the system performance, and hence such issues have to be addressed in the scheduling scheme design.

III. Multichannel Scheduling with Spectrum Hole Filling for Cognitive Radio Networks:

The proposed model of Multichannel scheduling with Optimal Spectrum Hole Filling (MCS-OSHF), has emphasis on medium access control strategy which shall function in Spectrum Access Controller. The key objective in the model is about QoS aware and also on dynamic channel allocation for different data-frame size that are to be transmitted in cognitive Radio wireless Networks which could enable the spectrum hole usage. The term spectrum hole usage can be defined as idle time amidst the schedules for sequence that is observed in a channel under Primary User levels. MCS-OSHF model presents the multichannel scheduling for hierarchy, and the following are the key processes adapted.

- The CR nodes shall assemble the varying size data-frames that are to be transmitted.
- For every data-frame in the transmission queue, a specific control frame shall be sent to the spectrum access controller, which shall inform to common controller, the requirement of each of the data-frame.
- Message mainly comprise the inputs like channel time, size of the data-frame, requisite bandwidth and the tentative time for transmission that is essential for reaching the spectrum access controller.
- The data-frame arrival time shall be calculated as the aggregate value of cumulative average time taken for a data-frame to reach the possible spectrum access controllers and the process-time (time taken for analyzing the message frame)

Let $\rho_{mf}(w_i)$ seen as process-timefor analyzing acontrol frame mf for a specificdata-frame w_i.

Let $a\tau_{mf}(w_i)$ seen as control frame arrival time mf atspectrum access controller ap. The time taken by the data-frame tentatively for transmission time w_i to reaching an access point ap, the outcome is estimated as:

$$\tau_{w_i} = \frac{\sum_{j=1}^{|AP|} \tau_{w_i}(ap_j)}{|AP|}$$

// |AP| shall be spectrum access controllers of count that is observed as w_i with the average of the tentative arrival times of a data-frame

w_i atspectrum access controller ap is estimated as follows:

$a\tau_{w_i} = a\tau_{mf}(w_i) + \rho_{mf}(w_i) + \tau_{w_i}$ // the cumulative value of arrival time $a\tau_{mf}(w_i)$ of the message frame mf, process time $\rho_{mf}(w_i)$ and tentative transmission time τ_{w_i} of the data-frame w_i.

As per the message evaluated from Data-frame mf of data-frame w_i, the spectrum access controller shall schedule channels using proposed model of MCS-OSHF.

a) MCS-OSHF Scheduling Strategy

In MCS-OSHF, the channel scheduling for respecttive data-frame w_i is carried out as:

The selection criteria for the channels are that of desired bandwidth and the ones that are idle for time slot transmission expected. If none of the channel exists in such criteria, under considering other such conditions like, the arrival time of a data-frame and the channel scheduling time is not being sync, or in the case where the multiple channels meet scheduling criteria, or multiple data-frames arriving with same criteria, or if less number of channels are identified with desired criteria, in such conditions, the data-frame segmenting and channel allocation shall be carried out by MCS-OSHF.

However, the data-frame transmission time w_i if realized to be much lesser than the available transmission time frame for a target channel, and also if the opportunity for a channel usage is found to be extremely high, in such conditions the following processes are performed by the spectrum access controller.

The process of scheduling an infrequent channel, with the extremely high transmission time frame shall be adapted rather than desired transmission time frame for data-frame w_i.

In case of failing to trace a channel with the given criteria, selection of the infrequent channel sets that has some kind of lower time frame that the desired time frame for the data-frame w_i, in order to aggregate the transmission time slots for the selected channels, which shall be greater than desired transmission time frame.

Also segments the data-frame w_i multiple data-frames as to each partition in the data-frame shall transmit by one of the channels, from the set of channels that are selected.

Also, if the spectrum access controller do not achieve the schedule under above criteria, channels with idle times are selected which could meet the criteria for transmission time frame w_i

In the case of idle time frame is not found sufficient, then the data-frames are segmented in to minimum number of data-frames, so as the new data-frames shall be transmitted using the minimum channels that are compatible with the idle time slots.

Also, in the instances where the spectrum access controllers fail to schedule channels using any of the above criterions, then the data-frame is buffered and in frequent intervals the attempts are made to schedule. Despite of such process, if the scheduling fails within the lifetime of data-frame, then such data-frames are dropped and acknowledgment to CR nodes are sent about failure.

Mathematical notations and the process flow algorithm for MCS-OSHF model has been depicted in the following section.

b) Pseudo representation of scheduling algorithm

MCH: Begin

1. Let mf_i be the control frame representing the data-frame w_i to be transmitted by spectrum access controller ap_j,
2. $oc \leftarrow \phi$
   //representation of optimal channel initialized to null
3. $oc = selectOC(a\tau_{w_i}, db_{w_i}, etf_{w_i}, |w_i|, \{C\})$
   //finding the optimal channel and passing parameters are varying size data-frame arrival time $a\tau_{w_i}$, desired bandwidth db_{w_i}, expected transmission time frame etf_{w_i}, data-frame size $|w_i|$ and vector of channels available $\{C\}$
4. If $(oc \neq \phi)$ Begin //optimal channel found for varying size data-frame w_i
5. channel oc scheduled tovarying size data-frame w_i
6. *Exit*
7. End // of condition in line 4
8. Else Begin //of condition in line 4
9. Set $ocl \leftarrow \phi$
   // ocl is the set of optimal channels initialized to null, which contains selected optimal channels to transmit multiple segments of data-frame w_i
10. Set $s(w_i) \leftarrow \phi$
    // $s(w_i)$ represents the set of data-frame segments formed from the varying size data-frame w_i that initialized with ϕ
11. $< o\ \mathfrak{k}, s(w_i) >= MCList(w_i, \{C\})$
    // finding the set of optimal channels to transmit data-frame segments of data-frame w_i
12. If $(ocl \neq \phi \,\&\, s(w_i) \neq \phi)$ Begin

13. For-each $ws \leftarrow s(w_i)$ & $oc \leftarrow ocl$ Begin
14. Schedule oc to ws
15. End //of iteration in line 13
16. Exit // since scheduling completed
17. End //of condition in line 12
18. Else Begin
19. $< ocl, s(w_i) >= SCHF(w_i, \{C\})$
20. If $(ocl \neq \phi \,\&\, s(w_i) \neq \phi)$ Begin
21. For-each $ws \leftarrow s(w_i)$ & $oc \leftarrow ocl$ Begin
22. Schedule oc to ws
23. End //of iteration in line 21
24. Exit // since scheduling completed
25. End // of condition in line 20
26. Varying size data-frame loss inevitable
27. End //of condition in line 18
28. End //of condition in line 8
29. End // of the function

c) Pseudorepresentation of channel selection algorithm

$selectOC(a\tau_{w_i}, db_{w_i}, etf_{w_i}, |w_i|, \{C\})$ Begin

1. $ec \leftarrow \phi$ // vector of eligible channels is set to ϕ
2. $oc \leftarrow \phi$ // resultant optimal channel set null initially
3. Foreach $c \leftarrow \{C\}$ begin
4. if $(itf_s(c) + \lambda) > (a\tau_{w_i} - \varphi)$ Begin //channel c is not idle by the arrival time of data-frame, here $itf_s(c)$ is the next idle frame start time of channel c, λ and φ are elapsed time thresholds respective to idle time frame start time and data-frame arrival time respectively.

a. *continue //to next iteration of line* 3

5. End // of the condition in line 4
6. Else Begin //of condition in line 4

b. $ec \leftarrow c$ // move channel c to vector ec

7. End //of condition in line 6
8. $ritf_{\min} \leftarrow \infty$ // represents minimal residual idle time frame set to ∞ initially
9. $rbw_{\min} \leftarrow \infty$ // represents minimal residual bandwidth set to ∞ initially
10. For-each $\{c \exists c \in ec\}$ begin

a. $ritf = ((itf_e(c) - itf_s(c)) - (ttf_{w_i} + \varphi)$

b. $rbw = bw_c - (db_{w_i} + \beta)$ // residual bandwidth observed for channel c to transmit data-frame w_i with desired bandwidth $(db_{w_i} + \beta)$, here β is elapsed threshold of the bandwidth desired.

c. $if\ (0 < ritf < ritf_m) \wedge (0 < rbw < rbw_m)$ begin

i. $ritf_m \leftarrow ritf$
ii. $rbw_m \leftarrow rbw$
iii. $oc \leftarrow c$

d. End // of condition in line a

11. End //of iteration in line 10
12. Return oc
13. End //of the function

d) Pseudo representation of data-frame segmenting and Multiple Channels selection Algorithm

1. $MCList(w_i, \{C\})$:Begin
2. $ocl \leftarrow \phi$ //optimal channel list initialized with null
3. $s(w_i) \leftarrow \phi$ //varying size data-frame segment list initialized with null
4. For-each $c \leftarrow \{C\}$ begin
5. if $(itf_s(c) + \lambda) > (a\tau_{w_i} - \varphi)$ Begin //channel c is not idle by the arrival time of data-frame, here $itf_s(c)$ is the next idle frame start time of channel c, λ and φ are elapsed time thresholds respective to idle time frame start time and data-frame arrival time respectively.

a. continue //to next iteration of line 4

6. End // of the condition in line 5
7. Else Begin //of condition in line 5

b. $ec \leftarrow c$ // move channel c to vector ec

8. End //of condition in line 7
9. Sort ec in descending order of $|itf|$
   // sorting the eligible channels in descending order of their idle time frame size.
10. For-each $\{c \exists c \in ec\}$ begin

a. $ocl \leftarrow c$

b. $s(w_i) \leftarrow \overline{w}_i$
   // $\overline{w}_i$ is the segment of the data-frame w_i such that $[(((itf_e(c) - itf_s(c)) - (ttf_{\overline{w}_i} + \varphi)) > 0] \wedge [(bw_c - (db_{\overline{w}_i} + \beta)) > 0]$

a. $w_i \leftarrow w_i - \overline{w}_i$

11. $if\ (w_i \equiv \phi)$ Begin
12. Break // the loop in line 10
13. End //of the condition in line 11
14. Return $< ocl, s(w_i) >$
15. End // of the function

e) Pseudo representation of data-frame segmenting and multiple channels with spectrum channel holesalgorithm

1. $SCHF(w_i, \{C\})$:Begin
2. $ocl \leftarrow \phi$ // indicates optimal channels list for idle time usage, which initialized with null
3. $s(w_i) \leftarrow \phi$ //varying size data-frame segment list bsl initialized with null
4. Sort channels in ascending order of buffer time between data-frame arrival time and channel idle time frame start time.

The buffer time of the data-frame w_i under channel c can be measured as

$b_{w_i}(c_i) = (itf_s(c_i) + \lambda) - (a\tau_{w_i} + \varphi)$

5. For-each $c \leftarrow \{C\}$ begin

a. $ocl \leftarrow c$

b. $s(w_i) \leftarrow w_i$
   // w_i is the segment of the data-frame w_i such that

$[(((itf_e(c) - itf_s(c)) - (ttf_{w_i} + \varphi)) > 0] \wedge$

$[(bw_c - (db_{w_i} + \beta)) > 0]$

c. $w_i \leftarrow w_i - w_i$

6. $if\,(w_i \equiv \phi)$ Begin
7. Break // the loop in line 5
8. End //of the condition in line 6
9. Return $< ocl, s(w_i) >$
10. End //of the function

Towards performing the channel scheduling, MCS-OSHF focus on tracking possible optimal channel (Sec 3.3), and in the instance of failure, attempts the further selection criteria like the minimal number of idle channels (3.4), and the process as detailed in the aforesaid section (3.5). Process of segmenting is carried out on the basis of demand, thus leading to minimal overhead. In the instances of MCS-OSHF failing to schedule any of the channels, the failure acknowledgment is communicated to CR nodes after dropping the data-frames.

IV. Experimental Setup and Empirical Analysis

Using the simulation study the performance of proposed model of MCS-OSHF is assessed in comparison to the benchmarking models like QoS-aware Channel Sensing Scheduling (QCSS) [16] and the other model of Novel Spectrum Scheduling Scheme (NSSS) [17]. Using the NS2 simulation methods, CR based wireless network is simulated and the metrics used in the simulation process is detailed in the following tabulation (table.1)

Table1: Metrics for Simulation

No of cognitive radio nodes as users	50
The range of Varying size data-frame generation threshold	32KB to 512KB
Number of spectrum access controllers	8
Usage of elapsed threshold values	0.05% of actual
Channels per spectrum access controller	16
Simulation time	12 minutes
Bandwidth Range	512MB to 1536MB

There is huge deviation in the varying size data-frames that are formed in the data size of 10GB to 25GB. In the range of 32kb to 512kb, there is variation in the data-frame size. In the comparison of model to QCSS [16] and NSSS [17], performance of OCA-UTI is assessed using QoS metrics – data-frame loss against transmission data - frame loads (see figure -1), and also the transmission throughput that is achieved in data frame load (see figure-2). Also the process overhead that is observed in the transmission data-frame load (see figure-3) is also depicted.

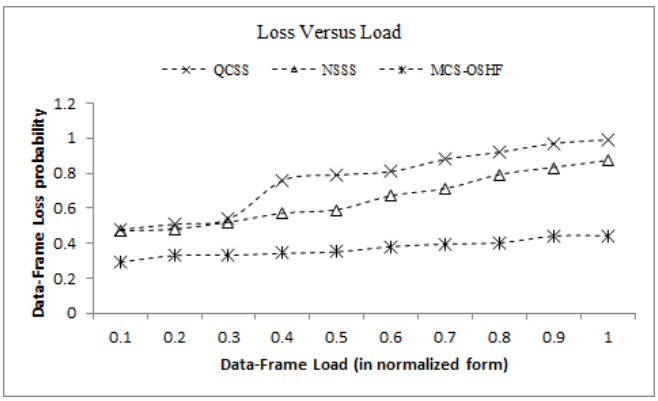

Figure 1: Varying size data-frame Loss vs. Varying size data-frame Load

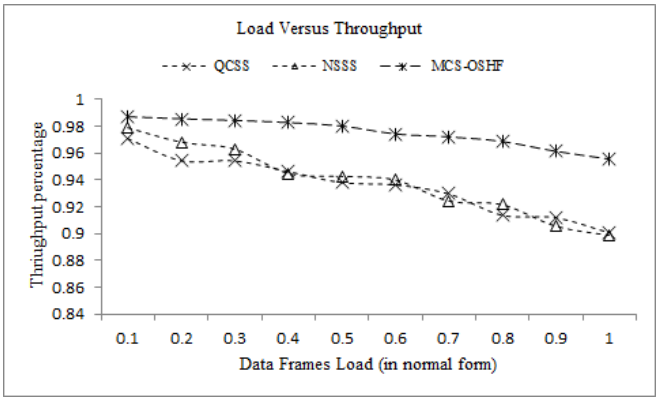

Figure 2: Throughput vs. varying size data-frame Load

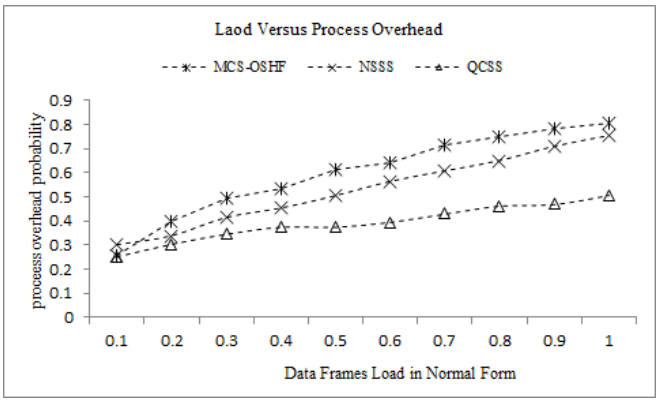

Figure 3: varying size data-frame load vs. Process overhead

The quantum of data-frame loss in correlation to data-frame load is depicted in Figure.1 and it is imperative that the data-frame load is normalized amid the value of 0 and 1 that depicts the number of data-frames per second. The study reflects that MCS-OSHF shall certainly reduce the data-frame loss compared to the other models opted for simulation. (See Figure-1). However, in terms of multiple channel selection, and the process of data-frame segmentation too, MCS-OSHF still leads the minor process overhead rather than the other two models considered in the study. (See figure 3).For achieving the maximum throughput using the minimal data-frame loss, such mechanism is certainly tolerable.

V. Conclusion

MCS-OSHF (Multichannel scheduling with spectrum hole filling) model is focused on improving the channel scheduling protocol for CR based wireless networks. The emphasis in the model is about maximizing optimal channel allocation for better throughput and also minimal transmission loss of data-frames. Using the hierarchical approach which facilitates the optimal idle channel, using a specific process, in terms of following the order in the hierarchy the process of data-frames scheduling is carried out. From the detailed experimental studies that are carried out in comparison with other such models like NSSS and QCSSS, the inputs from the study depict much more efficient performance from the proposed model compared to the other two models. In terms of futuristic study or expansion of the model, emphasis shall be on minimize the process overhead, and in the other way, model could be developed for optimal channels allocation by preempting the allotted channels, which could support in rescheduling towards achieving stable throughput and minimal loss of data-frames in CR based wireless networks.

References Références Referencias

1. Force, F. S. P. T. (2002). Report of the spectrum efficiency working group.
2. Akyildiz, I. F., Lee, W. Y., Vuran, M. C., &Mohanty, S. (2006). NeXt generation/dynamic spectrum access/cognitive radio wireless networks: a survey. *Computer networks*, *50*(13), 2127-2159.
3. IEEE LAN/MAN Standards Committee. (2006). IEEE Standard for local and metropolitan area networks Part 16: Air interface for fixed and mobile broadband wireless access systems amendment 2: Physical and medium access control layers for combined fixed and mobile operation in licensed bands and corrigendum 1. *IEEE Std 802.16-2004/Cor 1-2005*.
4. IEEE 802.11 Working Group. (2010). IEEE Standard for Information Technology–Tele communications and information exchange between systems–Local and metropolitan area networks–Specific require-

ments–Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Wireless Access in Vehicular Environments. *IEEE Std*, *802*, 11p.
5. Zhao, J., Zheng, H., & Yang, G. H. (2005, November). Distributed coordination in dynamic spectrum allocation networks. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.* (pp. 259-268). IEEE.
6. Chen, T., Zhang, H., Maggio, G. M., &Chlamtac, I. (2007, April). CogMesh: A cluster-based cognitive radio network. In *2007 2nd IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks* (pp. 168-178). IEEE.
7. Jia, J., Zhang, Q., & Shen, X. S. (2008). HC-MAC: A hardware-constrained cognitive MAC for efficient spectrum management. *IEEE journal on selected Areas in Communications*, *26*(1), 106-117.
8. Su, H., & Zhang, X. (2008). Cross-layer based opportunistic MAC protocols for QoSprovisionings over cognitive radio wireless networks. *IEEE Journal on Selected Areas in Communications*, *26*(1), 118-129.
9. Thoppian, M., Venkatesan, S., Prakash, R., & Chandrasekaran, R. (2006, June). MAC-layer scheduling in cognitive radio based multi-hop wireless networks. In *Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks* (pp. 191-202). IEEE Computer Society.
10. Tang, J., Misra, S., &Xue, G. (2008). Joint spectrum allocation and scheduling for fair spectrum sharing in cognitive radio wireless networks. *Computer networks*, *52*(11), 2148-2158.
11. Hamdi, K., Zhang, W., &Letaief, K. B. (2007, March). Uplink scheduling with QoS provisioning for cognitive radio systems. In *2007 IEEE Wireless Communications and Networking Conference* (pp. 2592-2596). IEEE.
12. Gözüpek, D., &Alagöz, F. (2009). Throughput and delay optimal scheduling in cognitive radio networks under interference temperature constraints. *Journal of Communications and Networks*, *11*(2), 148-156.
13. Tian, C., & Yuan, D. (2009, May). A novel multiuser diversity based scheduler with QoS support for cognitive radio networks. In *Communication Networks and Services Research Conference, 2009. CNSR'09. Seventh Annual* (pp. 310-316). IEEE.
14. Huang, S., Liu, X., & Ding, Z. (2008, April). Opportunistic spectrum access in cognitive radio networks. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*. IEEE.
15. Choi, J. K., Kwon, K. H., &Yoo, S. J. (2009, October). Qos-aware channel sensing scheduling in cognitive radio networks. In *Computer and Information Technology, 2009. CIT'09. Ninth IEEE International Conference on* (Vol. 2, pp. 63-68). IEEE.
16. Tumuluru, V. K., Wang, P., &Niyato, D. (2011). A novel spectrum-scheduling scheme for multichannel cognitive radio network and performance analysis. *IEEE transactions on Vehicular Technology*, *60*(4), 1849-1858.

This page is intentionally left blank

Global Journal of Computer Science and Technology: E Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

ECARDM: Energy Consumption Aware Route Discovery for Multicasting in Mobile Ad hoc Networks

By K. Seshadri Ramana & Dr. A.A. Chari
Rayalaseema University

Abstract- Consideration of energy consumption in the case of wireless ad hoc networks leads to effective reduction of energy consumption by the nodes and increases the lifetime of the batteries for nodes. It is imperative from the existing models that there is significant scope for improvement in the energy-consumption based route discovery models. A model of Fuzzy based marginal energy disbursed multicast route discovery model for MANETs can support in reducing the power consumption has been proposed in our earlier research paper. In the present paper, a contemporary solution termed "Energy Consumption Aware Route Discovery for Multicasting for MANETs" has been proposed, which is profoundly a fuzzy reasoning and genetic algorithm based model that focus on both the energy consumption and also the element of end-to-end delay whilst discovering the route.

Keywords: *fuzzy reasoning, crossover tree, fitness function, end-to-end delay, signal to noise ratio.*

GJCST-E Classification: *C.2.1, C.1.4*

Strictly as per the compliance and regulations of:

ECARDM: Energy Consumption Aware Route Discovery for Multicasting in Mobile Ad hoc Networks

K. Seshadri Ramana [α] & Dr. A.A. Chari [σ]

Abstract- Consideration of energy consumption in the case of wireless ad hoc networks leads to effective reduction of energy consumption by the nodes and increases the lifetime of the batteries for nodes. It is imperative from the existing models that there is significant scope for improvement in the energy-consumption based route discovery models. A model of Fuzzy based marginal energy disbursed multicast route discovery model for MANETs can support in reducing the power consumption has been proposed in our earlier research paper. In the present paper, a contemporary solution termed "Energy Consumption Aware Route Discovery for Multicasting for MANETs" has been proposed, which is profoundly a fuzzy reasoning and genetic algorithm based model that focus on both the energy consumption and also the element of end-to-end delay whilst discovering the route. The experimental study of the model in comparison to BWDCMR and GAEEQMR models depicted that the proposed algorithm is very effective and can certainly be result oriented.

Keywords: fuzzy reasoning, crossover tree, fitness function, end-to-end delay, signal to noise ratio.

I. Introduction

MANETs (Mobile ad hoc networks) are predominantly a self-configured network of mobile nodes that can easily develop its dynamic topology. Predominantly, all the nodes are part of maintaining the network connectivity irrespective of any kind of fixed infrastructure requirements like the base stations or the access points for communication. Every node in the network takes part in the routing process, and using the routing function forwards the packets to the other nodes using the intermediate nodes. When two nodes are in the range of transmission for each other, communication takes place directly; else using the support of other nodes the packets are forwarded.

Non-restricted mobility and also the ease of deployment are some of the profound features of MANETs that are vividly used in the services. Also, the challenge of power awareness is also another crucial segment in the mobile wireless networks which has been a crux factor in the implementation of MANETs.

It is very important that the power consumption by the nodes has to be limited for ensuring that the battery lifetime of the nodes endures. To ensure that battery energies are not wasted, it is very important that the transmission power have to carefully handled, and it has become a significant area of research. From the review of numerous models of source based energy efficient multicast trees oriented algorithms that are depicted, it is evident that significant volume of research is carried out in the domain. [1].

Majority of the multi-media applications are delay-sensitive and it is very important that whilst planning to offer better QoS, issues like end-to-end delay has to be considered. But in the majority of the energy-efficient multicast routing models the scope and issue of "delay" has not been considered as a metric. Even in the case of QoS multicast routing that are developed, some of the multi-constrained metrics (degree-constrained least-cost multicast routing [2] or multi-constrained cost multicast problem [3]) has hardly ever considered the issues of energy consumption. It is imperative that QoS multicast routing schemes shall not be directly adapted in the case of MANETs.

In [4] it is imperative that the issue of QoS multicast routing with multiple QoS constraints can be NP-Complete. NP-Completion problem is predominantly addressed in the artificial intelligence domain, using an effective solution of genetic algorithm model. Despite the fact that the genetic algorithms may not be so effective in handling the delay sensitive applications due to the huge volume of iterations [5], still the scope of computation is much faster. Considering such scope and limitations, in this paper, the proposed model of genetic algorithm is designed to be quite promising in terms of multicast routing in MANETs.

In [6] the authors have presented a model of genetic algorithm for solving the multi-constrained routing problem related to the transmission delay and success ratio. Younes in [7] [8] has also proposed a genetic algorithm for determining the shortest paths envisaging the bandwidth constraints. Liu et.al [9] has also presented an oriented, spanning tree (OST) that is based on genetic algorithm (GA) for addressing the MSPP (multi-criteria shortest path problem). Ting Lu et.al [10] has proposed a different set of energy efficient genetic algorithm for finding the delay-constrained multicast tree and reduces the scope of total energy consumption of tree.

Author α: Research Scholar, Rayalaseema University, Kurnool-518002, A.P., India. e-mail: ramana.Kothapalli @gmail.com
Author σ: Emeritus Professor, Dept of OR & SQC, Rayalaseema University, Kurnool-518002, A.P., India.

The proposed source based algorithm shall take in to account energy consumption and also the end-to-end delay in route selection. Algorithm applies the crossover and also the mutation operations on the trees directly, and it simplifies the coding/decoding process. Heuristic mutation technique shall improve the levels of total consumption of multicast tree.

In all the aforesaid works, the authors have focused upon finding efficient and feasible path depending on energy consumption for the multicast routing in MANETs. But the performance of these models fall downwards, if number of nodes in network and number of initial routes are increased. Also limited to one or two QoS metrics. Hence, the proposed work shall focus on optimal energy-efficient multi-metric QoS multicast routing using GA

By reviewing the existing models of source-based multicast routing problems that are adapted using a genetic algorithm, in this paper, the proposal is a genetic algorithm about an energy efficient and delay-constrained multicast tree discovery. Testing under simulated conditions evinced the efficacy of the proposed model.

a) Energy Consumption Model

In [11] the energy consumption required for an effective link amid of two nodes has been studied. In the instance of transmission of a unit message, the quantum of minimum energy that is essential amid of minimum energy that is essential amid of nodes v_i and v_j is $P_{i,j} = k_1(r_{i,j})^{\beta} + k_2$, in which $r_{i,j}$ is Euclidean distance amid of v_i and v_j, k_1 shall be constant dependent on the properties constituted by the antenna, β shall be the path loss exponent which is dependent on the level of propagation losses taking place in the medium, and k_2 shall be a constant that accounts for the overheads taking place from the digital processing and electronics. In the above instance, one of the presumption is that each of the multicast session shall be multicasting only a unit length message.

b) Network Model and Problem Description

It is presumed that every node of the MANET shall evaluate the distance between them and the other neighbour nodes using some kind of distance estimation methods [12]. Transmission power of a node has direct impact on the connectivity of the network, and every node can alter its transmission power levels in a dynamic way. Every node can use the different set of power level for each of the multicast tree in which the node functions and predominantly the nodes use Omni-directional antennas. Every node in a network shall have two coverage areas like the control coverage area (CR_i); and data coverage area $\{DR_i \exists DR_i \subseteq CR_i\}$. Such coverage areas mostly rely upon the transmission power chosen by the selected node v_i for transmitting its control and data packets categorically.

As per the control coverage area for every node, a MANET can be depicted as a graph $G(V,E)$, in which $V = \{v_1, v_2, ..., v_n\}$ shall be a set of nodes (mobile hosts) and $E = \{(i,j) \mid v_i, v_j \in V\}$ is a set of links. $(i,j) \in E$ Denotes that v_i and v_j shall be in the limits of control coverage area of each other. Every link (i,j) is constituted with a delay $d_{i,j}$ and distance $l_{i,j}$. $d_{i,j}$ Indicates the delay of data transmission between v_i and v_j, also comprising inputs on queuing delay and propagation delay. $l_{i,j}$ denotes the Euclidean distance amid of v_i and0 v_j. Both $d_{i,j}$ and $l_{i,j}$ shall be real numbers that are positive.

If $s \in V$ be a multicast source and $D \subseteq V - \{s\}$ shall be set of destinations. A multicast tree $T(s,D) \subseteq G$ will be a tree rooted at s and reaching all of the destinations in D. The delay of a path on T from s to a destination $v_t \in D$, indicated as delay $(pT(s,v_t))$, is delay $(pT(s,v_t)) = (i,j) \in pT(s,v_t) d_{ij}$. In such conditions, the delay-constrained minimum Steiner tree problem is all about finding minimum cost multicast tree $T^*(s,D)$ such that delay $(pT^*(s,v_t)) \leq \delta, \forall v_t \in D$, in which δ is the overall permissible delay from s to a destination $v_t \in D$. Once $T^*(s,D)$ is identified, every node on T^* works on adjustments of its transmission power effectively for transmitting data packets along the tree.

II. Energy Consumption aware Multicast Route Discovery by GA

a) Coding

In the process of developing an effective and well-performing genetic algorithm, representation of candidate solutions play a vital role. In the case of number of representations for a tree which is like one-dimensional binary code [13] or the Prefer numbers [14], alongside the sequence and topology encoding

(ST encoding) [15], has been developed in a significant manner.

But many of these representations could lead to generation of more illegal trees, or the ones that has very poor neighbourhood or even the ones that have very low efficiency leading to surge in the required search space whenever there is rise in the network size. Some of the recent studies that have focused on network optimization [16] have overcome the problem by adapting the tree manipulation. For instance, processes like using a data structure of a tree for defining the chromosome as an option. Such processes are resulting in the omission of tree structure coding methods where the chromosomes denote the multicast tree directly.

b) Initial Population

In the population initialization, two of the significant issues that are considered are about population size NP and the population formulation method. NP is effectively set by a system. In the algorithm proposed, random multicast trees which are formed as initial population is completely on the basis of MAODV [17].

c) Fitness Function

Individual performance has to be depicted in the fitness function: For the proposed model, the inference is that the good individual has better fitness than the bad ones. Also, the definition of the fitness function is profoundly based on set of heuristics that are devised in [18]. Following are the set of heuristics considered for defining the fitness.

The proposed heuristics for the selection of optimal nodes in each hierarchy of the set shall be quoted as $H = \{h_1, h_2, ...h_{|H|}\}$ are

i. *Ratio of Battery Depletion* [18]

This is one among the heuristics which define the quantum of mediocre energy that is essential for transmitting each unit of data for the nodes that comprised in routing path. Also, the average levels of energy that is essential for transmitting the frame by a node in the hierarchy h_i for all optimal nodes that are selected in consecutive hierarchy h_{i+1}.

ii. *Foreseen Residual Battery Life* [18]

This heuristic shall support in forecasting the residual life of a node nd towards the completion of the routing process that is already scheduled. The sum (aec) of Battery Depletion (bd) expected for transmissions amid of the node nd and towards its hop level successor nodes, at node's idle time (ibd) the levels of batter depletion time and obligatory battery depletion (obd) which reflects the energy consumption resulting from factors like retransmissions, jitter and control packets. Also, the resultant sum aec shall be deducted from the present residual battery life ($prbl$). Such resultant values have to be more of positive and should be greater than the threshold values defined.

iii. *Assessing Opportunistic multicast range* [18]

This metric shall be an effective heuristic signifying the hop level multicast link amid of the optimal nodes for a hierarchy h_i to the quantum of optimal nodes in continual hierarchy h_{i+1}.

iv. *Assessment of Signal to Noise Ratio*

In the signal to Noise ratio (snr) of a node n_i shall be the average loss of signal ration pertaining to noise that is observed at the links amid of node of node n_i and all the successive nodes that are connected.

v. *Assessing Fitness of the Given Multicast Route* [19]

In terms of fitness that is considered for an individual node which is assessed by adapting the fuzzy logic which is applied in terms of battery depletion ratio, signal to noise ration and the foreseen residual battery life, and also the levels of opportunistic multicast range.

Fuzzy notations that are used for the heuristics that are proposed, for performing the fuzzy reasoning which are ranged with the ranks that are of scale 1 to 5, with most optimal ranked as high in the scale (5) and for the least optimal it is range as low which is 1. The divergent fuzzy state ranking of the heuristics are depicted in the Table-1

Table 1: Notations adapted for performing fuzzy reasoning using the proposed heuristics

	Foreseen Residual Battery Life ($frbl$)	Opportunistic Multicast Range (omr)	Battery Depletion Ratio (bdr)	Signal to Noise Ratio (snr)
Very Low	1	1	5	1
Medium	3	3	3	3
Very High	5	5	1	5
High	4	4	2	4
Low	2	2	4	2

In terms of membership function, which is adapted for fuzzy reasoning in terms of estimating the fitness for a given tree is:

The mean m of the low l and high h values for a heuristic observed for all nodes comprised in the given route shall be estimated initially as follows

- $m = \frac{(l+h)}{2}$
- But in the lower value l to $\frac{m}{2}$ it shall be considered as the range of very low,
- $\frac{m}{2}$ to $3 \otimes \frac{m}{4}$ will be considered as the range of low,
- $3 \otimes \frac{m}{4}$ to m is observed as the moderate,
- m to $m \oplus \frac{m}{2}$ is observed as range of high
- and $m \oplus \frac{m}{2}$ to h is observed as range of very high.

Also, the average of ranks that are observed towards a heuristic h for all nodes in a given route shall be assessed and is also normalized by divided with max rank (5 is the max rank proposed in the model). The resulting normalized values towards the respective heuristic at the route level shall be either > 0 and ≤ 1. Similar process shall be applied for all of the heuristics that are considered for fuzzy reasoning. Also, the route level values that are observed for every heuristic shall be aggregate and divided by the total volume of heuristics (4 is the notion value in the proposal) with resulting values being in the range of > 0 and ≤ 4, depicting the fitness value of the given route.

d) Energy Consumption Aware Multicast Route Discovery

The initial population in terms of discovering all the possible multicast routes shall be carried out using the bench marking routing strategies like MAODV [17].

Also, the incremental genetic algorithm towards redefining the multicast route discovery for QFSRD [20] shall be adapted for optimal route discovery.

To accomplish the evolutionary strategy, adapting Genetic Algorithm comprising incremental evolution process is focused upon. An incremental evolution strategy which is adapted on set of possible routes P which is found between the source and also the destination nodes and the number of evolutions at the initial level shall be limited to max evolution count provided.

i. *The Optimal Route Discovery Function*

Repeat {

$tT \leftarrow T$ /clone the initial multicast trees discovered in route request phase

$\overline{T} \leftarrow \phi$

$\forall_{i=1}^{|T|} \{t_i \exists t_i \in T\}$ Begin // for each multicast tree t_i discovered in route request phase

$\forall_{s=1}^{|T|} \{t_j \exists t_j \in T \wedge i \neq j\}$ Begin// for each multicast tree t_j discovered in route request phase, which is not equal to t_i

$\overline{T} \leftarrow GAPE(t_i, t_j)$

//see sec ii

//Invoking the function that performs Genetic Algorithm with progressive evolutions on given multicast trees

End

End

If $\left(|T| \square \left| T \cup \overline{T} \right| \right)$ Begin

$T = \phi$

$T \leftarrow \overline{T}$

} Until $\left(tT \square T \right)$ // repeat the process till tT and T become approximately equal under given threshold Δ

ii. *The Genetic Algorithm with Progressive Evolutions*

GAPE (t_i, t_j) BEGIN

Consider a set RT to preserve the resultant multicast trees from progressive evolutions

Consider the set cn to store the resultant crossovers, which are sub trees exists in both given trees t_i and t_j

i. $\forall_{p=1}^{|t_i|} \{st_p \exists st_p \in t_i\}$ // for each subtree st_p such that $st_p \in t_i$ Begin

ii. $\forall_{q=1}^{|t_j|} \{st_q \exists st_q \in t_j\}$ // for each node st_q such that $st_q \in t_j$ Begin

iii. $if\,(st_p \equiv st_q \,\&\, p \equiv q \neq 1)$ Begin // if sub trees $\{st_p \exists st_p \in t_i\}$ and $\{st_q \exists st_q \in t_j\}$ are identical and p, q are not equal to 1

a. $cn \leftarrow st_p$ //move subtree st_p to set cn

End // end of iii

End // of ii

End // of i

Split the given multicast tree t_i in to two subtrees lt_i and rt_i , //where lt_i is the subtree, which is predecessor to st_p, rt_i is the sub tree, which is successor of st_p

Split the given multicast tree t_j in to two subtrees lt_j and rt_j , //where lt_j is the subtree, which is predecessor to st_q, rt_j is the sub tree, which is successor of st_q

Then create new multicast tree, such that new multicast tree ct_1 is created by concatenating the left part lt_i of the tree t_i, crossover subtree st_p and right part rt_j of the tree t_j , which is as follows

$ct_1 \leftarrow lt_i$

$ct_1 \leftarrow st_p$

$ct_1 \leftarrow rt_j$

Further, create new multicast tree ct_2, by concatenating the left part lt_j of the tree t_j , crossover sub tree st_p and right part rt_i of the tree t_i, which is as follows

$ct_1 \leftarrow lt_i$

$ct_1 \leftarrow st_p$

$ct_1 \leftarrow rt_j$

Find fitness of the routes $t_i, t_j, ct_1, and\ ct_2$ //Assessing fitness as explored in section-c(v).

Order the $t_i, t_j, ct_1, and\ ct_2$ in the descending order of their fitness

Move first two routes in the ordered list to RT

Return RT

END

In accordance to [22, theorem 2.7], algorithm shall be resourceful in converging as a global optimal solution. In a large-scale network, it shall be much time consuming for obtaining the optimal solution to an NP-complete problem, still such issues could be overcome if there is proper iteration time set in the genetic algorithm. By carrying out such process, obtaining near-optimal solution within a reasonable time limit can be expected.

III. Experimental Study and Performance Anaysis

In the experimental process of the proposed genetic algorithm, the process adapted is to implement in expression language R [21].

Experimental study is carried out on a PC with configuration of Pentium Dual-Core 2.5 GHz CPU and the Ram capacity of 2GB memory. Preliminary tests that are carried out with the 20 initial multicast routes discovered under route request phase. The proposed algorithm model is evaluated and compared with least delay multicast tree algorithm model of Bandwidth and Delay Constrained Multicasting by GA (BWDCMR) [8] and Genetic Algorithm for Energy-Efficient QoS Multicast Routing (GAEEQMR) [10]. As BWDCMR and GAEEQMR are among the most effective models found in recent literature, which is in terms of connecting the source and the destination with the least possible delay in the path, such a model is considered for comparison. The RRSR (route request success ratio) of an algorithm can be defined as the numerous requests that are successfully routed which are divided by the total number of routing requests. In the case of the multicast tree if the delay constraints are addressed, then the routing request is considered to be effectively and successfully routed.

The results from the experiments that are carried out are depicted for random networks. The process of simulation that is conducted depicts the outcome for the random networks to be between 20-100 nodes and the distance for each of the link shall be distributed in uniform manner in the range of 10 to 200 units (pixels in simulation) and the delay for each of the link is between 0 and 50 milliseconds focused upon. Also, the maximum permissible delay in the process is uniformly distributed as in the range of 30 to 160 milliseconds.

Source and destinations are randomly generated for every request. MANETs that are considered can be adapted in vivid sectors under the real-time conditions. Also, the network comprised in the application shall be of various sizes which range from small to medium and even in the levels of tens of nodes. Simulation process considered in the experiment depicts the realistic conditions

Max Lifetime of the Route, Energy Consumption Ratio and the Route Discovery process Completion Time are key elements that are tested in the experiments. Results are the outcome of 10000 randomly generated requests of routing for each network. For every request, the source and destination are generated randomly.

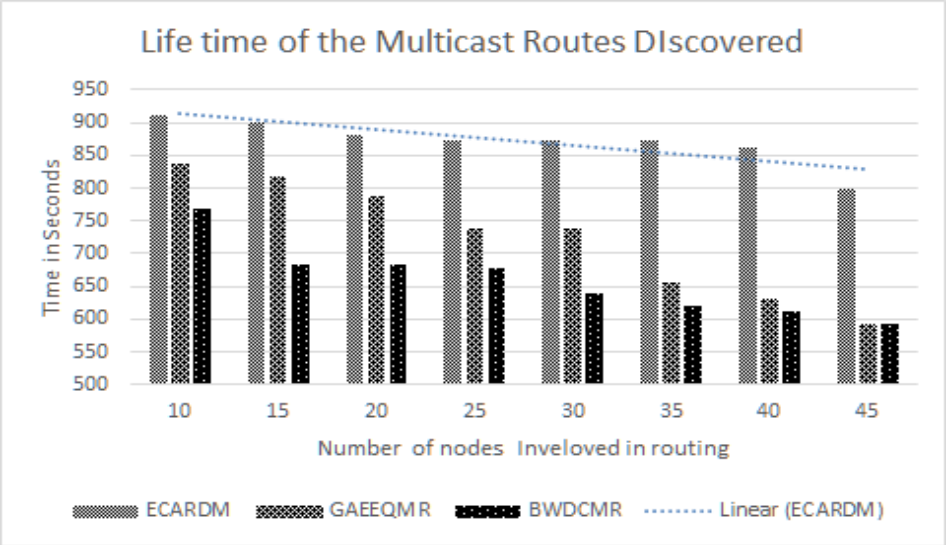

Figure 1: Lifetime of the Routes Discovered

In the Fig 1 depicts the comparative results of delay bound and energy efficient routes discovered by the proposed and other two benchmarking algorithms BWDCMR and GAEEQMR. It is imperative from the figurative representation that the proposed model is outperformed the other two with an average of 25% and 17% max route life than BWDCMR and GAEEQMR respectively.

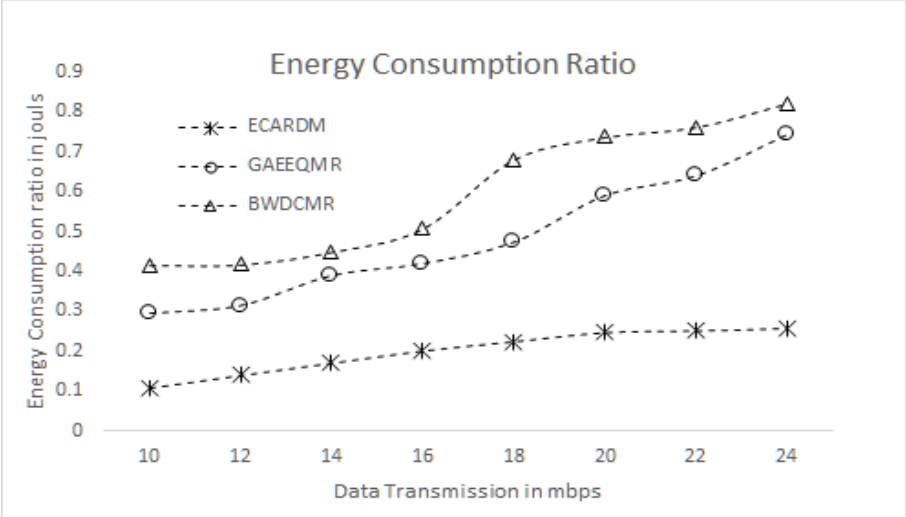

Figure 2: Energy Consumption Ratio Observed

Also, in Fig.2, the comparative results of ratio of energy consumption observed for proposed and other two models is denoted. It is evident from the results that the energy consumption ratio in the proposed model is significantly minimal than the other two models, which emphasizes that the proposed model can support in finding the multicast tree that consumes minimal energy.

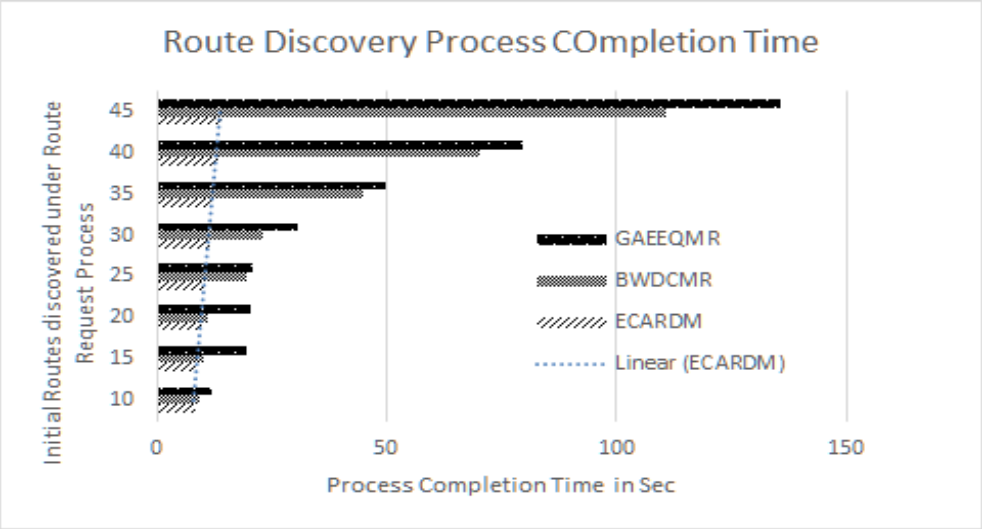

Figure 3: The Process Completion time observed

In the Fig.3, the route discovery process completion time obtained by all three models has been depicted. The results reflect the fact that the Route discovery time of the proposed algorithm and BWDCMR are linear and equal by approximate against to the number of initial routes given as input, whereas in the case of GAEEQMR, the route discovery time is multifold if number of initial routes increased.

IV. Conclusion

Power awareness is very important element in mobile wireless networks, categorically in the case of MANETs. It is predominantly important that the nodes have to significantly reduce their power consumption to envisage endured battery lifetime. Considering the existing models of energy consumption aware route discovery models, it is imperative that though some of the models are turning to be very effective, still there is scope for improvement. Even in the case of some of the bench marking models like the BWDCMR and GAEEQMR, the computational complexity levels are high and NP-hard. There is need for improved ways of finding the multicast route discovery with less complexity.

The algorithm that is proposed in this paper is the energy-efficient delay-constrained multicast routing algorithm. The source-based algorithm that is proposed considers the level of energy consumption and also the end-to-end delay in route selection. Crossovers and the mutation operations are directly applied on trees, by the proposed algorithm. Such a process results in simplification of coding operation and results in scope of omitting the coding/decoding process.

Heuristic mutation techniques shall result in improved total energy consumption for a multicast tree. Some of the experiments that are performed for verifying the convergence performance, S R and also the running time for the proposed algorithm and when compared to the BWDCMR and GAEEQMR models for comparative analysis, the results depict that the proposed model has linear computational complexities and NP-Complete. Also it can be very resourceful in improving the route discovery based on source-based routing trees. In the future works even the shared multicasting trees can be focused upon.

References Références Referencias

1. Nutov, Z., & Segal, M. (2012). Improved approximation algorithms for maximum lifetime problems in wireless networks. Theoretical Computer Science, 453, 88-97.
2. Tseng, S. Y., Huang, Y. M., & Lin, C. C. (2006). Genetic algorithm for delay-and degree-constrained multimedia broadcasting on overlay networks. Computer Communications, 29(17), 3625-3632.
3. Molnár, M., Bellabas, A., & Lahoud, S. (2012). The cost optimal solution of the multi-constrained multicast routing problem. Computer Networks, 56(13), 3136-3149.
4. Wang, Z., & Crowcroft, J. (1996). Quality-of-service routing for supporting multimedia applications. IEEE Journal on Selected areas in communications,14 (7), 1228-1234.
5. Ahmadi, F., Tati, R., Ahmadi, S., & Hossaini, V. (2011,August). New hardware engine for genetic algorithms. In Genetic and Evolutionary Computing (ICGEC), 2011 Fifth International Conference on (pp. 122-126). IEEE.
6. Lu, T., & Zhu, J. (2013). A genetic algorithm for finding a path subject to two constraints. Applied Soft Computing, 13(2), 891-898.
7. Hamed, A. Y. (2010). A genetic algorithm for finding the k shortest paths in a network. Egyptian Informatics Journal, 11(2), 75-79.

8. Younes, A. (2011). Multicast routing with bandwidth and delay constraints based on genetic algorithms. Egyptian Informatics Journal, 12(2), 107-114.
9. Liu, L., Mu, H., Yang, X., He, R., & Li, Y. (2012). An oriented spanning tree based genetic algorithm for multi-criteria shortest path problems. Applied Soft Computing, 12(1), 506-515.
10. Lu, T., & Zhu, J. (2013). Genetic algorithm for energy-efficient QoS multicast routing. IEEE Communications letters, 17(1), 31-34.
11. Feeney, L. M., & Nilsson, M. (2001). Investigating the energy consumption of a wireless network interface in an ad hoc networking environment. In INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Vol. 3, pp. 1548-1557). IEEE.
12. Lee, W. C. (1982). Mobile communications engineering. McGraw-Hill Professional.
13. Xiang, F., Junzhou, L., Jieyi, W., & Guanqun, G. (1999). QoS routing based on genetic algorithm. Computer communications, 22(15), 1392-1399.
14. Haghighat, A. T., Faez, K., Dehghan, M., Mowlaei, A., & Ghahremani, Y. (2002). A genetic algorithm for Steiner tree optimization with multiple constraints using Prüfer number. In EurAsia-ICT 2002: Information and Communication Technology (pp. 272-280). Springer Berlin Heidelberg.
15. Yen, Y. S., Chao, H. C., Chang, R. S., & Vasilakos, A. (2011). Flooding-limited and multi-constrained QoS multicast routing based on the genetic algorithm for MANETs. Mathematical and Computer Modelling, 53(11), 2238-2250
16. Tseng, S. Y., Huang, Y. M., & Lin, C. C. (2006). Genetic algorithm for delay-and degree-constrained multimedia broadcasting on overlay networks. Computer Communications, 29(17), 3625-3632.
17. Royer, E. M. (2000). Routing in ad-hoc mobile networks: On-demand and hierarchical strategies. University of California, Santa Barbara.
18. Ramana, K. S., & Chari, A. A. (2016). Heuristics to Multicast Route Discovery (HMRD): Energy Efficient Multicast Routing Topology for Mobile Ad Hoc Net works. International Journal of Applied Engineering Research, 11(7), 4844-4848.
19. Ramana, K. S., & Chari, A. A. (2016). MEDMR: Fuzzy based Marginal Energy Disbursed Multicast Route Discovery for Mobile Ad Hoc Networks. Indian Journal of Science and Technology, 9(34).
20. Chandra, M. R. C. D. P., & Reddy, S. (2015). QFSRD: Orthogenesis Evolution based Genetic Algorithm for QoS Fitness Scope aware Route Discovery in Ad hoc Networks. Global Journal of Computer Science and Technology, 15(3).
21. Team, R. C. (2013). R: A language and environment for statistical computing.
22. Guoliang, C., Xufa, W., Zhenquan, Z., & Dongsheng, W. (1996). Genetic algorithm and its application. People's Posts and Telecommunications Press.

Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 7 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Webgis based Decision Support System for Disseminating Nowcast based Alerts: Opengis Approach

By Shweta Mishra & Neha Sharma
Space Applications Center (ISRO)

Abstract- WebGIS is a kind of distributed information system which holds the potential to make geographic information available worldwide. It is cost effective and provides an easy way of disseminating geospatial data. This paper outlines the design and development of a WebGIS based Decision Support System (DSS) for disseminating Nowcasting of Extreme Orographic Rain events generated at regular intervals from (NETRA) model. Dissemination of events include heavy rainfall alerts all over India and cloudburst alerts over Western Himalayan Region every half an hour. In India, natural calamities like flood and cloudburst results in lot of causalities. If any early Heavy rain alerts dissemination system is developed then it will protect several lives and mitigate damage of property or infrastructure in affected areas. The development of such WebGIS based decision support system originates from this concept.

Keywords: web gis, open source, geoserver, openlayers, cloudburst, spatial decision support system, postgresql database.

GJCST-E Classification: H.3.5, H.5.3

Strictly as per the compliance and regulations of:

Webgis based Decision Support System for Disseminating Nowcast based Alerts: Opengis Approach

Shweta Mishra [α] & Neha Sharma [σ]

Abstract- WebGIS is a kind of distributed information system which holds the potential to make geographic information available worldwide. It is cost effective and provides an easy way of disseminating geospatial data. This paper outlines the design and development of a WebGIS based Decision Support System (DSS) for disseminating Nowcasting of Extreme Orographic Rain events generated at regular intervals from (NETRA) model. Dissemination of events include heavy rainfall alerts all over India and cloudburst alerts over Western Himalayan Region every half an hour. In India, natural calamities like flood and cloudburst results in lot of causalities. If any early Heavy rain alerts dissemination system is developed then it will protect several lives and mitigate damage of property or infrastructure in affected areas. The development of such WebGIS based decision support system originates from this concept. Objective of this paper is to describe the near real time WebGIS based Decision support System developed for disseminating rainfall alerts to the general public and administrators about heavy rain (all over India) and cloud burst (over Western Himalayan region) using interactive maps. Users can also get non spatial information like number of affected cities and their names, district level population (census 2011), forecast date and time, Radius of influence etc. This WebGIS based decision support system can help government agencies, NGO's and general public in planning to save lives, properties and can be used for decision making to reduce economic and material loss from the resulting floods.

This paper also illustrates use of open source technologies for developing such WebGIS -DSS at low cost. The principal development component includes: GeoServer, Java, PostgreSQL, OpenLayers, and GeoExt. The framework of the system can be divided into two categories:(1) Dissemination system which includes visualization of centroid and precise locations of Heavy Rain all over India and cloudburst over Western Himalayan Region along with related information and other overlay layers like State, District and Taluka boundaries, Roads, Rivers, Railway Tracks, National Highway, District Population as WMS (Web Map Service) Layers, Previous rainfall forecast events. It also provides various GIS functionalities to users such as zooming, panning, On/Off layers, print maps and many more. (2) Fetching the NETRA model output and storing the same in a database.

Presently, the Application can be accessed from Meteorological and Oceanographic Satellite Data Archival Centre (MOSDAC) through url i.e. www.mosdac.gov.in.

Keywords: web gis, open source, geoserver, openlayers, cloudburst, spatial decision support system, postgresql database.

Author α σ: Space Applications Centre, Ahmedabad.
e-mail: jaiswals@sac.isro.gov.in

I. Introduction

Recent advancements in internet and interactive content of the World Wide Web (WWW) have made them a powerful means for people to access, exchange and process information (Peng and Tsou 2003). The fast growing technology like Internet provides an ideal platform to empower the general public with the GIS technology through WebGIS. WebGIS (also known as Internet GIS) denotes a type of Geographic Information System (GIS), whose client is implemented in a Web browser (Yang C. et. al 2004). It combines the power of the Internet and GIS. It refers to the use of WWW as a primary means to exchange data, perform GIS analysis, and present results. Also the increased popularity of web mapping in recent years has sparked the development of many Open Source WebGIS projects with the similar aim of bringing GIS technology to the general public at little or no cost (Caldeweyher et. al 2006, Sharma and Mishra 2012).

The open source softwares are developed in collaborative manner and are available with source code for reuse, modification and redistribution as per technology-neutral published license (Karnatak et. al 2012). This study illustrates a method of using Open Source technology to design this WebGIS based DSS. It analyses the Web Map Service (WMS), Styled Layer Descriptor (SLD) features of GeoServer platform and builds the framework for publishing spatial information over web.

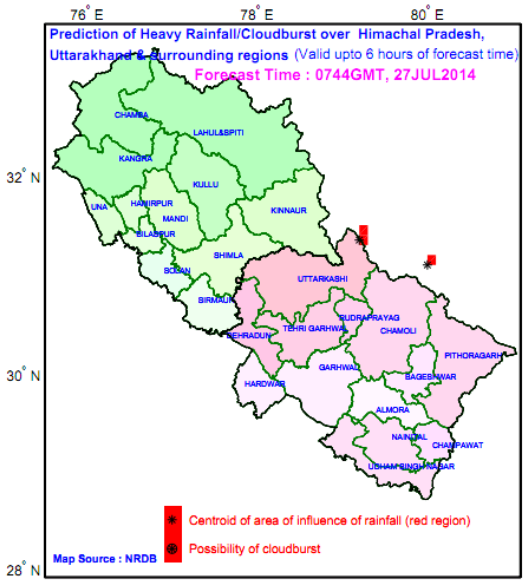

Figure 1: pdf representation

We have comprehensively utilized the advantages of WebGIS techniques to design a Web-based system for disseminating near real time forecast alerts. Previously the half hourly forecast was presented as static maps in pdfs hosted in MOSDAC as shown in Figure_1. Adding collateral information in terms of Administrative boundaries, Roads, Rivers, District headquarters etc in this type of map would result in a cluttered or un-interpretable map. GIS Functionalities like zooming, panning, measuring distance/area, querying or searching back dates events was not possible in such static maps. Hence, it was proposed to develop WebGIS based application where visualization is supported with a choice for the decision maker to add or remove the layers of interest. The value added information has been implemented through overlay of different layers. User can also search back date forecast events for more analysis. This WebGIS based DSS is a tailored GIS application whose purpose is to interactively visualize and disseminate NETRA alerts. This near real time WebGIS based forecast dissemination system not only provide very simple way of getting forecast information but can also be used by decision makers to mitigate casualties andeconomic losses. The users of this system include those ranging from general public, professionals or administrator making spatial decisions to Government Agencies or NGO's.

a) Input for WebGIS based Spatial Decision Support System

This application disseminates the NETRA model output at 8 km spatial resolution. The output predicts location of severe rainfall and has also tried to improve relationship between topography and rainfall intensity. The model uses thermal channel observations from KALPANA-1 satellite which consists of a Very High Resolution Radiometer (VHRR) operating in visible (0.55–0.75 μm) , water vapour (WV) (5.7–7.1 μm) and thermal infrared (TIR) (10.5–12.5 μm) bands (Kaila et al. 2002)). In addition, daily precipitation on a 0.1 latitude/longitude grid over South Asia (70oE-110oE; 5oN35oN) from the Climate Prediction Center (CPC) of NOAA (National Oceanographic and Atmospheric Administration, USA) for the years 2001 to 2012 has also been used for model development and validation. The model was configured and tested on the Western Himalayan over the whole monsoon season of 2012 with Probability Of Detection (POD), Probability Of False Detection (POFD) and accuracy of 66.15%, 17.00% and 82.78% respectively, for more details refer Shukla et al (2014).

Developed model has also been applied for the fateful day of June 16, 2013. Area with centroid at 30.44 N, 78.69 and radius of influence of 58.71 kms was predicted for intense rainfall activity which was the location (i.e Kedarnath) where cloudburst has actually occurred.

b) Web-based Architecture of the System

Figure_2 shows the basic architecture of the system. This system uses an extension of the client/server concept, known as Multi-tier architecture. It consists of the client (Web Browser), Web Server, Map Server and Data Server or Database. A Client is typically a Web Browser which allows users to interact with spatial objects and analysis functions in WebGIS based system. It is also the place to present output to the users (Peng and Tsou 2003). When user requests map or data through application, an HTTP request is sent to the Web Server. In present system, Apache Tomcat 7.0.41 Server is used as Web Server. Apache Tomcat Server recognizes the request and passes it to the Map Server. Map Server also called spatial server, is a major component designed for map rendering and spatial analysis. Here, GeoServer is used as a Map Server for processing spatial requests. The output of the map server can be a feature data or map image in graphical format. This output is then delivered to the Web server and ultimately to the user in his/her Web browser. GIS Database or Database server is also an important component which store spatial and non spatial data in spatially enabled relational database management system.

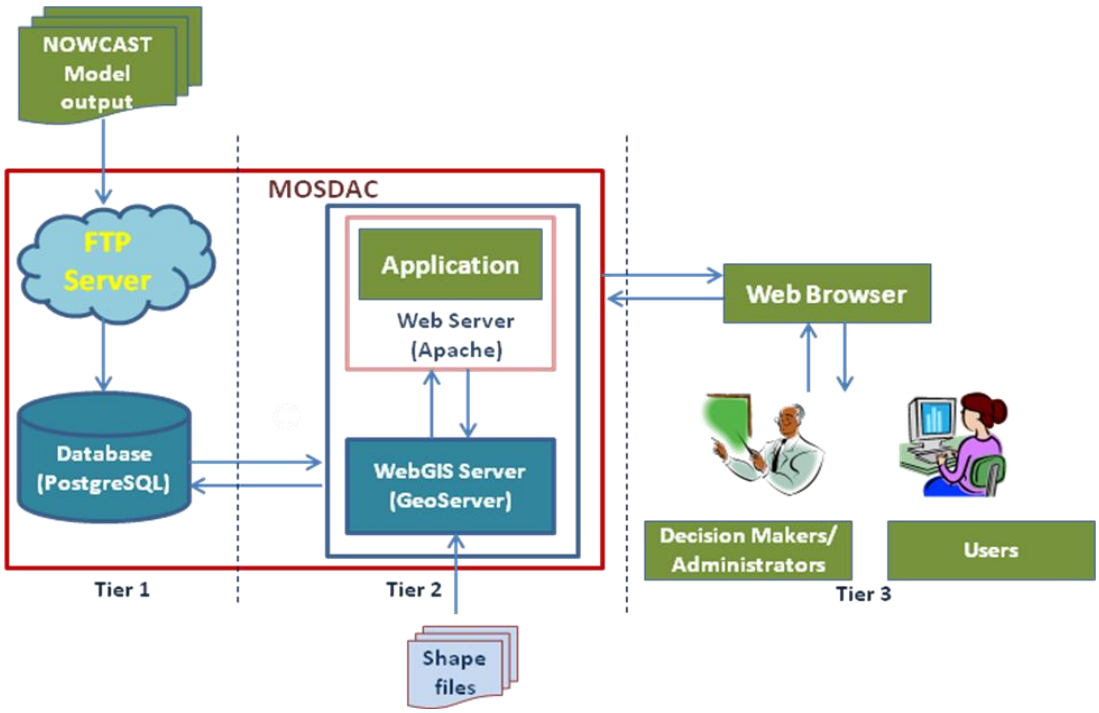

Figure 2: Three-tier architecture for WebGIS based Decision support System

c) System components

To visualize the data obtained from various sources, we require a platform that represents the data in visual forms like WebGIS enabled maps for better understanding and analysis. This WebGIS decision support System provides an intuitive interface for decision-making. The system is developed in Java/JSP platform as it is platform independent. This system is built using Open Source softwares and components including:

- Apache Tomcat 7.0.41 (http://tomcat.apache.org) as Web Server
- GeoServer 2.3.3 (http://geoserver.org) as Web Map Server
  - OpenLayers 2.11 (http://openlayers.org)
  - GeoExt 1.0 and ExtJS 3.2.1 (http://geoext.org)
- PostgreSQL9.1(http://www.postgresql.org)/Post GIS 2.0.3 (http://postgis.net) as the spatial database.
- uDig 1.4.0 (http://udig.refractions.net) for SLD generation

1. Apache Tomcat

The Jakarta Tomcat server is an open source, Java-based Web application container that was created to run servlet and JavaServer Page Web applications. It is very stable and has all of the features of a commercial Web application container.

2. GeoServer

GeoServer allows users to share and edit geospatial data. Designed for interoperability, it publishes data from any major spatial data source using open standards. GeoServer is the reference implementation of the Open Geospatial Consortium (OGC) Web Feature Service(WFS) and Web Coverage Service (WCS) standards, as well as a high performance certified compliant Web Map Service (WMS). GeoServer forms a core component of the Geospatial Web (http://geoserver.org). It is an open source WebGIS development platform with perfect functions, and it follows the OGC open standards (Huang Z. and Xu Z. 2011). GeoServer is used to publish raster and vector data, it supports Vector data sources such as Shapefile, PostGIS, Web Feature Server and Raster data sources such as Arc Grid Coverage Format, GeoTIFF, Gtopo30, ImageMosaic and other spatial data storage format, so it is easy to implement web publishing and sharing of spatial data.

3. OpenLayers

OpenLayers is client side JavaScript library for making interactive web maps, viewable in nearly any web browser. Since it is a client side library, it requires no special server side software or settings. The only thing required to make OpenLayers work is the OpenLayers code itself and a web browser. OpenLayers is also defined as an API (Application Programmer Interface) which provides users with tools to develop their own web maps (Hazzard E. 2011).

4. Geospatial Extension (GeoExt) and ExtJS

GeoExt is a rapidly-developing library for building rich, web-based GIS applications. The library is built upon Ext JS (Extended Java Script) and OpenLayers. The former provides User Interface (UI) components for building web applications along with solid underlying data components, the later is the de-facto standard for dynamic web mapping.

5. User-friendly Desktop Internet GIS (uDig)

The OpenGIS Styled Layer Descriptor (SLD) Profile of the OpenGIS Web Map Service (WMS) Encoding Standard defines an encoding that extends the WMS standard to allow user-defined symbolization and coloring of geographic feature and coverage data. SLD addresses the need for users and software to be able to control the visual portrayal of the geospatial data. It has ability to define styling rules that both client and server can understand. uDIG is open source desktop GIS development platform used for SLD generation.

Spatial Database Management System

GIS is the principal technology motivating interest in Spatial Database Management Systems. Before a GIS can carry out any analysis of spatial data, it accesses that data from Spatial Database Management System (SDBMS). An efficient SDBMS can greatly increase the efficiency and productivity of a GIS (Shekhar S. and Chawla S. 2003). For thisapplication, PostgreSQL database is used for storing both spatial and non spatial data. PostgreSQL is a powerful, open source object-relational database system. It is fully ACID (Atomicity, Consistency, Isolation, Durability) compliant, has full support for foreign keys, joins, views, triggers, and stored procedures (in multiple languages). PostGIS add support for geographic objects to the PostgreSQL object-relational database. In effect, PostGIS "spatially enables" the PostgreSQL server, allowing it to be used as a backend spatial database for geographic information systems (GIS), much like ESRI's SDE or Oracle's Spatial extension.

System Design

The framework of the developed system can be divided into two parts: (i) Fetching NOWCAST based output and storing same in database. (ii) WebGIS based Data Dissemination.

1. Data Download and Organization

Data Downloading: Text files containing location of Heavy Rainfall and cloudburst alerts and related information like number of cities affected with their names, radius of influence, forecast date and time are received at predefined Server at thirty minutes interval. Automatic Script is developed for downloading these files to server where database resides whenever files arrive.

Data Organization: Script written for downloading text files also contain one module for extracting locations of alerts and related information. This script is also responsible for inserting data into PostgreSQL database.

The purpose of physical database design is to translate the logical description of data into the technical specification for storing and retrieving data. Database organization for present system requires spatially enabled database, capable of storing and managing both spatial (location of heavy rain and cloudburst alerts) and non spatial data (number of affected cities, their name, forecast date and time, radius of influence etc). For this, PostgreSQL database is chosen which is capable of handling both Spatial and Non Spatial data in efficient way. GeoServer can be connected to database by creating data store and specifying the database connection parameters i.e. database name, host, port, user name and password etc. After establishing connection between GeoServer and PostgresSQL database, spatially enabled tables having alerts information get published through GeoServer as WMS layers that can be displayed in a browser application. The WMS defines the interface for accessing geospatial data uniformly from remote servers in a standard format, such as Portable Network Graphics (PNG) and Graphics Interchange Format (GIF), through HTTP. Three WMS operations are defined and used in the following sequence: (1) 'GetCapabilities' requests the service metadata; (2) 'GetMap' requests a static map according to given geospatial and other parameters; and (3) 'GetFeatureInfo' requests data of selected features (Li Wenwen et. al 2010). Information contained in published layers automatically gets updated with new dataarrival. Other thematic layers such as State, District and Taluka Boundary, Rivers, National Highways and other roads, District Headquarters, Airports, Railway Tracks and Digital Elevation model (DEM) have been published through GeoServer as WMS layers. All Shapefiles have been taken from Natural Resources Data Base (NRDB) (www.nnrms.gov.in) having GCS WGS84 projection. In order to display Geospatial data, it must be styled. Styled Layer Descriptor is used for visual portrayal of the geospatial data.

2. WebGIS based Data Dissemination system

User interface of system was designed in such a way that it provides a very simple and interactive way of visualizing heavy rainfall and cloudburst alerts along with related information. Currently Cloudburst forecast is provided for Western Himalayan Region and Heavy Rainfall alerts are provided for All India and surroundings. To disseminate these forecasts, separate frontend applications are designed. In both applications, basic information related to the locations of points of heavy rain and cloudburst is depicted through separate icons and a popup window with details available on-click of the icon. The value addition is in terms of interactive overlay of District boundaries, Taluka boundaries, Roads, Rivers and Digital Elevation Model (DEM) etc. WMS Layers of All India Landuse 2012-13, Himachal Pradeh and Uttarakhand Wasteland 2008-09 and Himachal Pradesh Erosion 2005-06 from Bhuvan (bhuvan.nrsc.gov.in) have also been incorporated as

overlay layers for providing more information to the users. These value additions will help users in making better decisions. GIS functionalities like panning, zooming, on/off layers, print map, measure distance/ area have been incorporated. User is also provided with functionality to search back dated forecast events for better analysis. Combination of Open source components OpenLayers, GeoExt and ExtJS is used in designing of rich user interface. The System Diagram is shown in Figure_3.

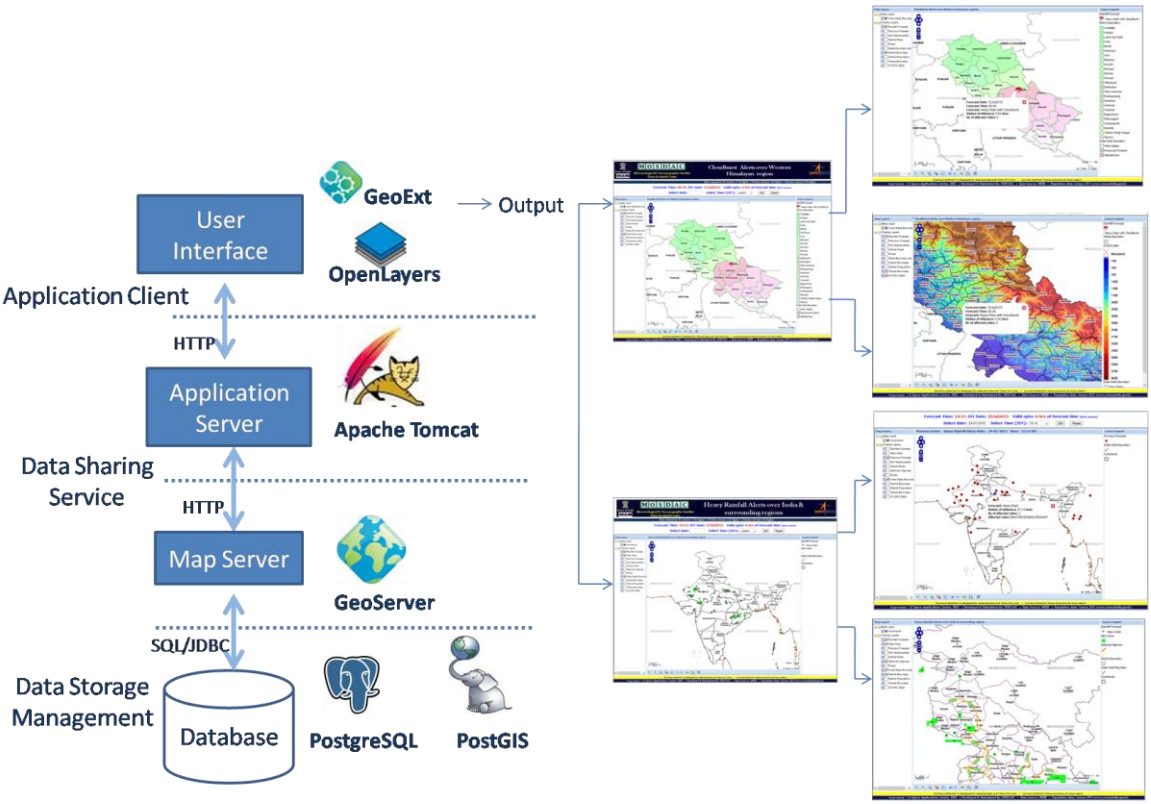

Figure 3: System Diagram

3. Results and Discussion

This section covers several aspects and results which make the WebGIS based decision support system unique compared to other web-based mapping applications and map viewers.

Functionality present in the System

Web Interface of system is shown in Figure_4. Forecast Date and Time shows time for current forecast generated. Forecast Alerts are disseminated in Map Viewer in Figure_4. It is divided into different panels like Layer Panel in left, Map panel (Map Window) at center and Legend panel in right. Each frame can be resized to give a better view of the information contained therein. Layer Panel shows overlay layers and provides basic GIS functionality of turning on and off layers. User can also visualize back date forecast events by selecting date and time (from calendar) for which forecast information is available in database. Dates highlighted in red color are those for which forecast information is stored in database. Heavy Rainfall and Cloudburst Alert maps along with other overlay layers are shown in Map Panel. Toolbar is provided with various GIS functionalities like zooming in and out, panning, identifying, selecting and measure distance/area. User can click on the map and display its attributes in the feature info popup.

Furthermore, District and Taluka boundaries maps use selective labeling. That is, as the user zooms into the detail of the map, the name of the district and taluka will be shown on the map. This makes it easy to browse around the map to find more information about the surrounding area and region. User Interface of application along with functionalities present in the application are shown below from Figure 4 to 7.

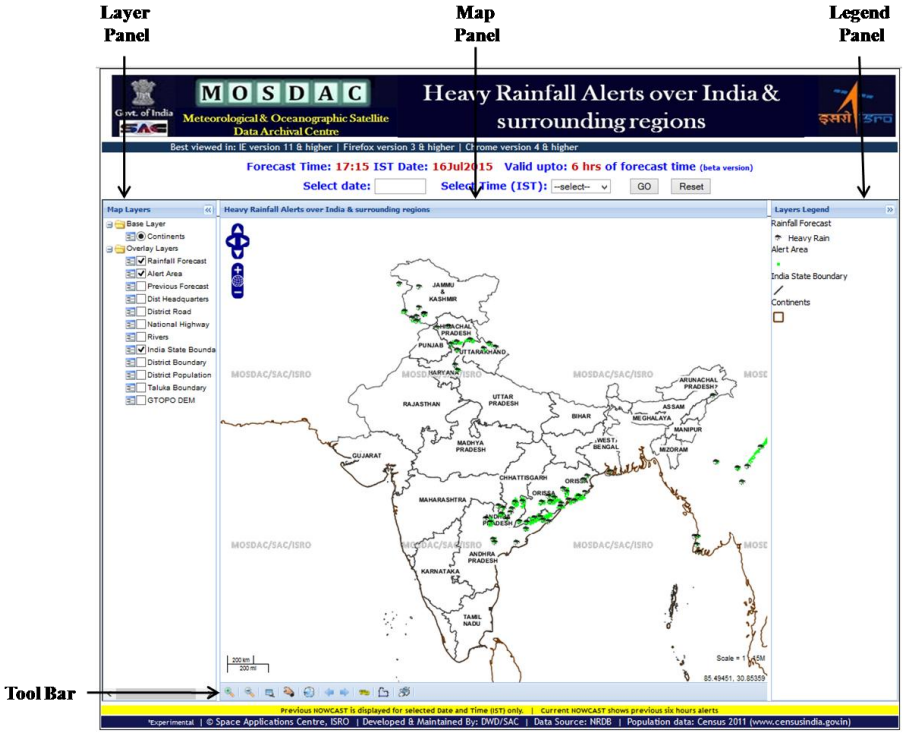

Figure 4: Showing User Interface depicting Heavy Rainfall alerts all over India and surroundings along with Layer Panel, Map Panel, Legend Panel and toolbar

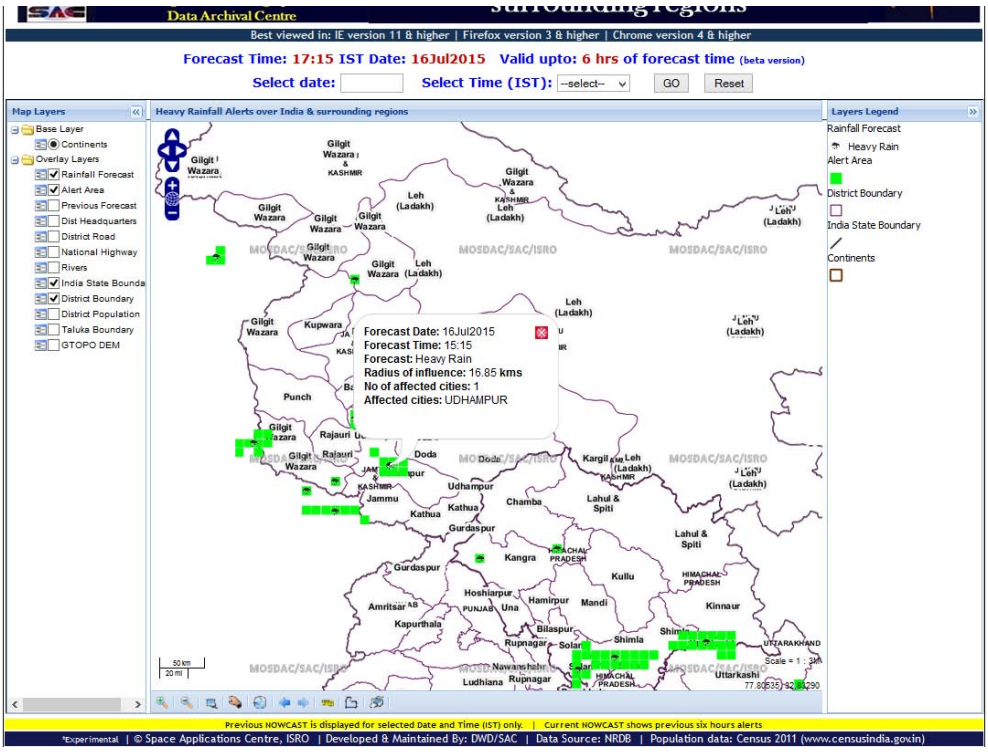

Figure 5: Predicted Heavy Rainfall alerts, alert area, overlay layers and popup with related information in parts of Jammu & Kashmir

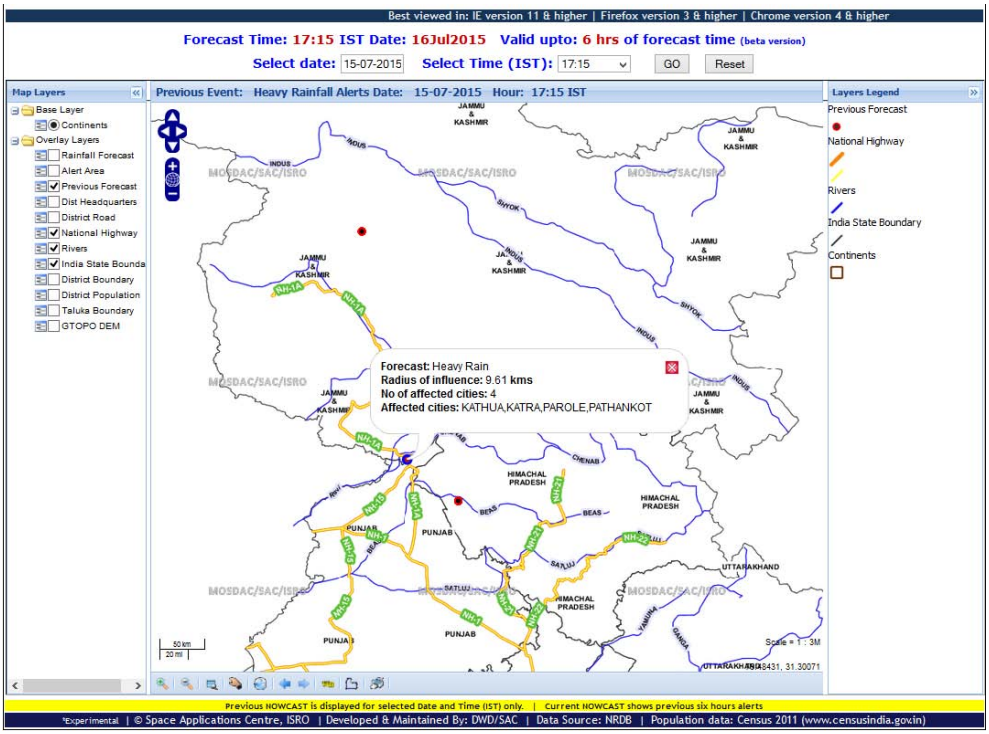

Figure 6: Showing Searched Previous date Heavy rainfall alerts events along with overlay layers

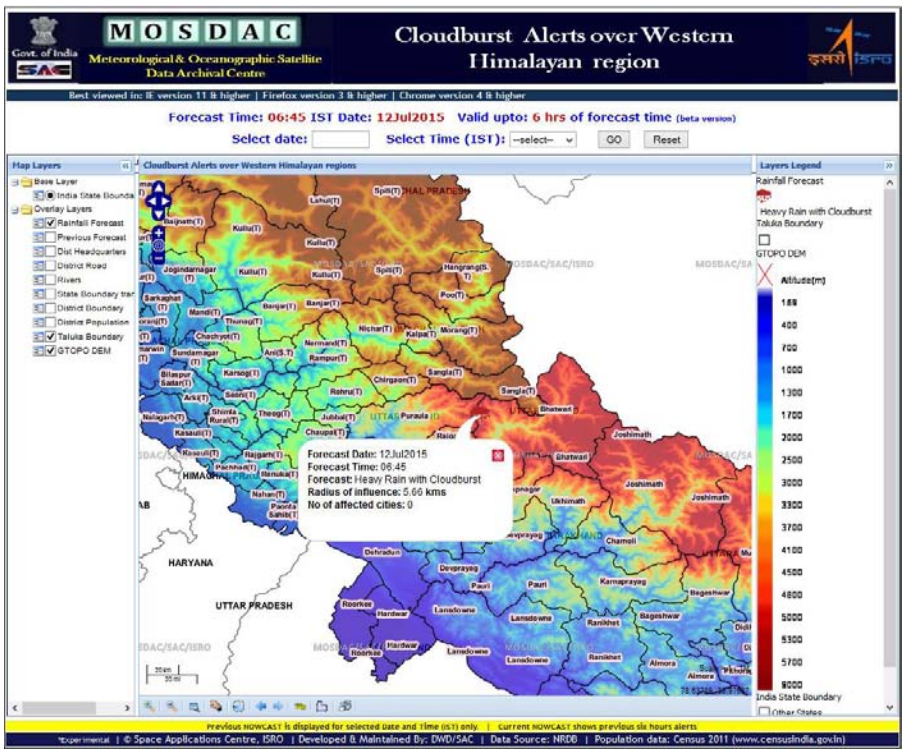

Figure 7: Showing WebGIS based Application depicting Cloudburst alert and along with alert related information on clicking alert icon and DEM as overlay layer

II. Conclusion and Future Work

The architecture of WebGIS based application developed during this study is a cost-effective, based on open standard and practical solution for GIS-based decision making exercise. One of the major goal behind development of WebGIS based DSS system is to provide forecast like heavy rainfall and Cloudburst in a timely fashion to mitigate casualties and economic losses. This WebGIS based decision support system can help government /Non government agencies, NGO's and others in planning to reduce economic and

material losses from disasters. This paper shows the process and methods of comprehensively using open source software like GeoServer, PostgreSQL, PostGIS, OpenLayers and others to publish geographic information, verifying the technical feasibility of the use of open source software to publish geographical information.

Similar technique has been adopted to provide information on heavy rain events using INSAT3D data; the same is available and updated at every half hour.

The current implementation of the GeoServer based depiction of heavy rain and or cloud burst events will be enhanced through implementation of probable impact assessment and depiction of the same.

III. Acknowledgements

The authors express their sincere gratitude to Mr. Tapan Mishra – Director SAC, Dr P.K. Pal -Deputy Director EPSA/SAC, Dr. B. S. Gohil - Group Director, ADVG/ EPSA and Mrs. Pushpalata B. Shah Head DWD/ADVG/EPSA for their support and encouragement. The authors would also like to acknowledge AOSG/EPSA for providing Heavy Rainfall and Cloudburst NOWCAST, Natural Resources Database (NRDB) team for providing GIS based thematic layers and Bhuvan for providing WMS layers.

References Références Referencias

1. Beaujardiere,J., 2004. OGC web map service interface [online], version 1.3.0, OGC 03-109r1. Available from: http://portal.opengeospatial.org/files /index.php?artifact_id=4756 & passcode= b9mnkb 6rr7uc1hs1t1ue [Accessed 6 September 2009].
2. Chaowei (Phil) Yang Corresponding author , David W. Wong , Ruixin Yang , Menas Kafatos & Qi Li (2005) Performance-improving techniques in web-based GIS, International Journal of Geographical Information Science, 19:3, 319-342, DOI: 10.1080/13658810412331280202
3. Daniel Caldeweyher, Jinglan Zhang & Binh Pham (2006), OpenCIS—Open Source GIS-based web community information system, International Journal of Geographical Information Science, 20:8, 885-898, DOI: 10.1080/13658810600711378
4. Erik Hazzard, (2011). OpenLayers 2.10 Beginner's Guide, First Edition. ISBN: 978-1-849514-12-5.
5. Harish Chandra Karnatak , Reedhi Shukla , Vinod Kumar Sharma , Y.V.S. Murthy & V. Bhanumurthy (2012) Spatial mashup technology and real time data integration in geo-web application using open source GIS – a case study for disaster management, Geocarto International, 27:6, 499-514, DOI: 10.1080/10106049.2011.650651
6. Herbert Schildt (2005). Java- A Beginners Guide. Third Edition. DOI: 10.1036/0071466509
7. James Goodwill, (2002). Apache Jakarta-Tomcat. ISBN: 1-893115-36-4
8. Peng, Z.-R. and Tsou, M.-H., 2003. Internet GIS: distributed geographic information services for the internet and wireless networks. Hoboken, NJ: Wiley.
9. Sharma, S. A. and Mishra, S. (2012), Web-GIS based monitoring of vegetationusing NDVI profiles, Journal of Geomatics, Vol.6 No.2 October 2012.
10. Shashi Shekhar and Sanjay Chawla, (2003). Spatial Databases: A Tour,ISBN: 0-13-017480-7
11. Shukla B.P, Kishtawal C.M. and Pal P.K. (2014), "Nowcasting of Extreme Orographic Rain (NETRA)", Space Applications Centre - Ahemdabad: Scientific Report. SAC/EPSA/AOSG/SR/12/2014.

Global Journals Inc. (US) Guidelines Handbook 2016

www.GlobalJournals.org

FELLOW OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (FARSC)

Global Journals Incorporate (USA) is accredited by Open Association of Research Society (OARS), U.S.A and in turn, awards "FARSC" title to individuals. The 'FARSC' title is accorded to a selected professional after the approval of the Editor-in-Chief/Editorial Board Members/Dean.

- The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

FARSC accrediting is an honor. It authenticates your research activities. After recognition as FARSC, you can add 'FARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, and Visiting Card etc.

The following benefits can be availed by you only for next three years from the date of certification:

FARSC designated members are entitled to avail a 40% discount while publishing their research papers (of a single author) with Global Journals Incorporation (USA), if the same is accepted by Editorial Board/Peer Reviewers. If you are a main author or co-author in case of multiple authors, you will be entitled to avail discount of 10%.

Once FARSC title is accorded, the Fellow is authorized to organize a symposium/seminar/conference on behalf of Global Journal Incorporation (USA).The Fellow can also participate in conference/seminar/symposium organized by another institution as representative of Global Journal. In both the cases, it is mandatory for him to discuss with us and obtain our consent.

You may join as member of the Editorial Board of Global Journals Incorporation (USA) after successful completion of three years as Fellow and as Peer Reviewer. In addition, it is also desirable that you should organize seminar/symposium/conference at least once.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The FARSC can go through standards of OARS. You can also play vital role if you have any suggestions so that proper amendment can take place to improve the same for the benefit of entire research community.

As FARSC, you will be given a renowned, secure and free professional email address with 100 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

The FARSC will be eligible for a free application of standardization of their researches. Standardization of research will be subject to acceptability within stipulated norms as the next step after publishing in a journal. We shall depute a team of specialized research professionals who will render their services for elevating your researches to next higher level, which is worldwide open standardization.

The FARSC member can apply for grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A. Once you are designated as FARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria. After certification of all your credentials by OARS, they will be published on your Fellow Profile link on website https://associationofresearch.org which will be helpful to upgrade the dignity.

The FARSC members can avail the benefits of free research podcasting in Global Research Radio with their research documents. After publishing the work, (including published elsewhere worldwide with proper authorization) you can upload your research paper with your recorded voice or you can utilize chargeable services of our professional RJs to record your paper in their voice on request.

The FARSC member also entitled to get the benefits of free research podcasting of their research documents through video clips. We can also streamline your conference videos and display your slides/ online slides and online research video clips at reasonable charges, on request.

The FARSC is eligible to earn from sales proceeds of his/her researches/reference/review Books or literature, while publishing with Global Journals. The FARSC can decide whether he/she would like to publish his/her research in a closed manner. In this case, whenever readers purchase that individual research paper for reading, maximum 60% of its profit earned as royalty by Global Journals, will be credited to his/her bank account. The entire entitled amount will be credited to his/her bank account exceeding limit of minimum fixed balance. There is no minimum time limit for collection. The FARSC member can decide its price and we can help in making the right decision.

The FARSC member is eligible to join as a paid peer reviewer at Global Journals Incorporation (USA) and can get remuneration of 15% of author fees, taken from the author of a respective paper. After reviewing 5 or more papers you can request to transfer the amount to your bank account.

MEMBER OF ASSOCIATION OF RESEARCH SOCIETY IN COMPUTING (MARSC)

The ' MARSC ' title is accorded to a selected professional after the approval of the Editor-in-Chief / Editorial Board Members/Dean.
The “MARSC” is a dignified ornament which is accorded to a person’s name viz. Dr. John E. Hall, Ph.D., MARSC or William Walldroff, M.S., MARSC.

MARSC accrediting is an honor. It authenticates your research activities. After becoming MARSC, you can add 'MARSC' title with your name as you use this recognition as additional suffix to your status. This will definitely enhance and add more value and repute to your name. You may use it on your professional Counseling Materials such as CV, Resume, Visiting Card and Name Plate etc.

The following benefitscan be availed by you only for next three years from the date of certification.

MARSC designated members are entitled to avail a 25% discount while publishing their research papers (of a single author) in Global Journals Inc., if the same is accepted by our Editorial Board and Peer Reviewers. If you are a main author or co-author of a group of authors, you will get discount of 10%.

As MARSC, you will be given a renowned, secure and free professional email address with 30 GB of space e.g. johnhall@globaljournals.org. This will include Webmail, Spam Assassin, Email Forwarders, Auto-Responders, Email Delivery Route tracing, etc.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

The MARSC member can apply for approval, grading and certification of standards of their educational and Institutional Degrees to Open Association of Research, Society U.S.A.

Once you are designated as MARSC, you may send us a scanned copy of all of your credentials. OARS will verify, grade and certify them. This will be based on your academic records, quality of research papers published by you, and some more criteria.

It is mandatory to read all terms and conditions carefully.

AUXILIARY MEMBERSHIPS

Institutional Fellow of Open Association of Research Society (USA)-OARS (USA)

Global Journals Incorporation (USA) is accredited by Open Association of Research Society, U.S.A (OARS) and in turn, affiliates research institutions as "Institutional Fellow of Open Association of Research Society" (IFOARS).

The "FARSC" is a dignified title which is accorded to a person's name viz. Dr. John E. Hall, Ph.D., FARSC or William Walldroff, M.S., FARSC.

The IFOARS institution is entitled to form a Board comprised of one Chairperson and three to five board members preferably from different streams. The Board will be recognized as "Institutional Board of Open Association of Research Society"-(IBOARS).

The Institute will be entitled to following benefits:

The IBOARS can initially review research papers of their institute and recommend them to publish with respective journal of Global Journals. It can also review the papers of other institutions after obtaining our consent. The second review will be done by peer reviewer of Global Journals Incorporation (USA) The Board is at liberty to appoint a peer reviewer with the approval of chairperson after consulting us.

The author fees of such paper may be waived off up to 40%.

The Global Journals Incorporation (USA) at its discretion can also refer double blind peer reviewed paper at their end to the board for the verification and to get recommendation for final stage of acceptance of publication.

The IBOARS can organize symposium/seminar/conference in their country on behalf of Global Journals Incorporation (USA)-OARS (USA). The terms and conditions can be discussed separately.

The Board can also play vital role by exploring and giving valuable suggestions regarding the Standards of "Open Association of Research Society, U.S.A (OARS)" so that proper amendment can take place for the benefit of entire research community. We shall provide details of particular standard only on receipt of request from the Board.

The board members can also join us as Individual Fellow with 40% discount on total fees applicable to Individual Fellow. They will be entitled to avail all the benefits as declared. Please visit Individual Fellow-sub menu of GlobalJournals.org to have more relevant details.

We shall provide you intimation regarding launching of e-version of journal of your stream time to time. This may be utilized in your library for the enrichment of knowledge of your students as well as it can also be helpful for the concerned faculty members.

After nomination of your institution as "Institutional Fellow" and constantly functioning successfully for one year, we can consider giving recognition to your institute to function as Regional/Zonal office on our behalf.
The board can also take up the additional allied activities for betterment after our consultation.

The following entitlements are applicable to individual Fellows:

Open Association of Research Society, U.S.A (OARS) By-laws states that an individual Fellow may use the designations as applicable, or the corresponding initials. The Credentials of individual Fellow and Associate designations signify that the individual has gained knowledge of the fundamental concepts. One is magnanimous and proficient in an expertise course covering the professional code of conduct, and follows recognized standards of practice.

Open Association of Research Society (US)/ Global Journals Incorporation (USA), as described in Corporate Statements, are educational, research publishing and professional membership organizations. Achieving our individual Fellow or Associate status is based mainly on meeting stated educational research requirements.

Disbursement of 40% Royalty earned through Global Journals : Researcher = 50%, Peer Reviewer = 37.50%, Institution = 12.50% E.g. Out of 40%, the 20% benefit should be passed on to researcher, 15 % benefit towards remuneration should be given to a reviewer and remaining 5% is to be retained by the institution.

We shall provide print version of 12 issues of any three journals [as per your requirement] out of our 38 journals worth $ 2376 USD.

Other:

The individual Fellow and Associate designations accredited by Open Association of Research Society (US) credentials signify guarantees following achievements:

- The professional accredited with Fellow honor, is entitled to various benefits viz. name, fame, honor, regular flow of income, secured bright future, social status etc.

- In addition to above, if one is single author, then entitled to 40% discount on publishing research paper and can get 10%discount if one is co-author or main author among group of authors.
- The Fellow can organize symposium/seminar/conference on behalf of Global Journals Incorporation (USA) and he/she can also attend the same organized by other institutes on behalf of Global Journals.
- The Fellow can become member of Editorial Board Member after completing 3yrs.
- The Fellow can earn 60% of sales proceeds from the sale of reference/review books/literature/publishing of research paper.
- Fellow can also join as paid peer reviewer and earn 15% remuneration of author charges and can also get an opportunity to join as member of the Editorial Board of Global Journals Incorporation (USA)
- • This individual has learned the basic methods of applying those concepts and techniques to common challenging situations. This individual has further demonstrated an in–depth understanding of the application of suitable techniques to a particular area of research practice.

Note :

"

- In future, if the board feels the necessity to change any board member, the same can be done with the consent of the chairperson along with anyone board member without our approval.
- In case, the chairperson needs to be replaced then consent of 2/3rd board members are required and they are also required to jointly pass the resolution copy of which should be sent to us. In such case, it will be compulsory to obtain our approval before replacement.
- In case of "Difference of Opinion [if any]" among the Board members, our decision will be final and binding to everyone.

"

Process of submission of Research Paper

The Area or field of specialization may or may not be of any category as mentioned in 'Scope of Journal' menu of the GlobalJournals.org website. There are 37 Research Journal categorized with Six parental Journals GJCST, GJMR, GJRE, GJMBR, GJSFR, GJHSS. For Authors should prefer the mentioned categories. There are three widely used systems UDC, DDC and LCC. The details are available as 'Knowledge Abstract' at Home page. The major advantage of this coding is that, the research work will be exposed to and shared with all over the world as we are being abstracted and indexed worldwide.

The paper should be in proper format. The format can be downloaded from first page of 'Author Guideline' Menu. The Author is expected to follow the general rules as mentioned in this menu. The paper should be written in MS-Word Format (*.DOC,*.DOCX).

The Author can submit the paper either online or offline. The authors should prefer online submission.Online Submission: There are three ways to submit your paper:

(A) (I) First, register yourself using top right corner of Home page then Login. If you are already registered, then login using your username and password.

(II) Choose corresponding Journal.

(III) Click 'Submit Manuscript'. Fill required information and Upload the paper.

(B) If you are using Internet Explorer, then Direct Submission through Homepage is also available.

(C) If these two are not convenient, and then email the paper directly to dean@globaljournals.org.

Offline Submission: Author can send the typed form of paper by Post. However, online submission should be preferred.

Preferred Author Guidelines

MANUSCRIPT STYLE INSTRUCTION (Must be strictly followed)

Page Size: 8.27" X 11'"

- Left Margin: 0.65
- Right Margin: 0.65
- Top Margin: 0.75
- Bottom Margin: 0.75
- Font type of all text should be Swis 721 Lt BT.
- Paper Title should be of Font Size 24 with one Column section.
- Author Name in Font Size of 11 with one column as of Title.
- Abstract Font size of 9 Bold, "Abstract" word in Italic Bold.
- Main Text: Font size 10 with justified two columns section
- Two Column with Equal Column with of 3.38 and Gaping of .2
- First Character must be three lines Drop capped.
- Paragraph before Spacing of 1 pt and After of 0 pt.
- Line Spacing of 1 pt
- Large Images must be in One Column
- Numbering of First Main Headings (Heading 1) must be in Roman Letters, Capital Letter, and Font Size of 10.
- Numbering of Second Main Headings (Heading 2) must be in Alphabets, Italic, and Font Size of 10.

You can use your own standard format also.
Author Guidelines:

1. General,

2. Ethical Guidelines,

3. Submission of Manuscripts,

4. Manuscript's Category,

5. Structure and Format of Manuscript,

6. After Acceptance.

1. GENERAL

Before submitting your research paper, one is advised to go through the details as mentioned in following heads. It will be beneficial, while peer reviewer justify your paper for publication.

Scope

The Global Journals Inc. (US) welcome the submission of original paper, review paper, survey article relevant to the all the streams of Philosophy and knowledge. The Global Journals Inc. (US) is parental platform for Global Journal of Computer Science and Technology, Researches in Engineering, Medical Research, Science Frontier Research, Human Social Science, Management, and Business organization. The choice of specific field can be done otherwise as following in Abstracting and Indexing Page on this Website. As the all Global

Journals Inc. (US) are being abstracted and indexed (in process) by most of the reputed organizations. Topics of only narrow interest will not be accepted unless they have wider potential or consequences.

2. ETHICAL GUIDELINES

Authors should follow the ethical guidelines as mentioned below for publication of research paper and research activities.

Papers are accepted on strict understanding that the material in whole or in part has not been, nor is being, considered for publication elsewhere. If the paper once accepted by Global Journals Inc. (US) and Editorial Board, will become the copyright of the Global Journals Inc. (US).

Authorship: The authors and coauthors should have active contribution to conception design, analysis and interpretation of findings. They should critically review the contents and drafting of the paper. All should approve the final version of the paper before submission

The Global Journals Inc. (US) follows the definition of authorship set up by the Global Academy of Research and Development. According to the Global Academy of R&D authorship, criteria must be based on:

1) Substantial contributions to conception and acquisition of data, analysis and interpretation of the findings.

2) Drafting the paper and revising it critically regarding important academic content.

3) Final approval of the version of the paper to be published.

All authors should have been credited according to their appropriate contribution in research activity and preparing paper. Contributors who do not match the criteria as authors may be mentioned under Acknowledgement.

Acknowledgements: Contributors to the research other than authors credited should be mentioned under acknowledgement. The specifications of the source of funding for the research if appropriate can be included. Suppliers of resources may be mentioned along with address.

Appeal of Decision: The Editorial Board's decision on publication of the paper is final and cannot be appealed elsewhere.

Permissions: It is the author's responsibility to have prior permission if all or parts of earlier published illustrations are used in this paper.

Please mention proper reference and appropriate acknowledgements wherever expected.

If all or parts of previously published illustrations are used, permission must be taken from the copyright holder concerned. It is the author's responsibility to take these in writing.

Approval for reproduction/modification of any information (including figures and tables) published elsewhere must be obtained by the authors/copyright holders before submission of the manuscript. Contributors (Authors) are responsible for any copyright fee involved.

3. SUBMISSION OF MANUSCRIPTS

Manuscripts should be uploaded via this online submission page. The online submission is most efficient method for submission of papers, as it enables rapid distribution of manuscripts and consequently speeds up the review procedure. It also enables authors to know the status of their own manuscripts by emailing us. Complete instructions for submitting a paper is available below.

Manuscript submission is a systematic procedure and little preparation is required beyond having all parts of your manuscript in a given format and a computer with an Internet connection and a Web browser. Full help and instructions are provided on-screen. As an author, you will be prompted for login and manuscript details as Field of Paper and then to upload your manuscript file(s) according to the instructions.

To avoid postal delays, all transaction is preferred by e-mail. A finished manuscript submission is confirmed by e-mail immediately and your paper enters the editorial process with no postal delays. When a conclusion is made about the publication of your paper by our Editorial Board, revisions can be submitted online with the same procedure, with an occasion to view and respond to all comments.

Complete support for both authors and co-author is provided.

4. MANUSCRIPT'S CATEGORY

Based on potential and nature, the manuscript can be categorized under the following heads:

Original research paper: Such papers are reports of high-level significant original research work.

Review papers: These are concise, significant but helpful and decisive topics for young researchers.

Research articles: These are handled with small investigation and applications.

Research letters: The letters are small and concise comments on previously published matters.

5. STRUCTURE AND FORMAT OF MANUSCRIPT

The recommended size of original research paper is less than seven thousand words, review papers fewer than seven thousands words also.Preparation of research paper or how to write research paper, are major hurdle, while writing manuscript. The research articles and research letters should be fewer than three thousand words, the structure original research paper; sometime review paper should be as follows:

Papers: These are reports of significant research (typically less than 7000 words equivalent, including tables, figures, references), and comprise:

(a)Title should be relevant and commensurate with the theme of the paper.

(b) A brief Summary, "Abstract" (less than 150 words) containing the major results and conclusions.

(c) Up to ten keywords, that precisely identifies the paper's subject, purpose, and focus.

(d) An Introduction, giving necessary background excluding subheadings; objectives must be clearly declared.

(e) Resources and techniques with sufficient complete experimental details (wherever possible by reference) to permit repetition; sources of information must be given and numerical methods must be specified by reference, unless non-standard.

(f) Results should be presented concisely, by well-designed tables and/or figures; the same data may not be used in both; suitable statistical data should be given. All data must be obtained with attention to numerical detail in the planning stage. As reproduced design has been recognized to be important to experiments for a considerable time, the Editor has decided that any paper that appears not to have adequate numerical treatments of the data will be returned un-refereed;

(g) Discussion should cover the implications and consequences, not just recapitulating the results; conclusions should be summarizing.

(h) Brief Acknowledgements.

(i) References in the proper form.

Authors should very cautiously consider the preparation of papers to ensure that they communicate efficiently. Papers are much more likely to be accepted, if they are cautiously designed and laid out, contain few or no errors, are summarizing, and be conventional to the approach and instructions. They will in addition, be published with much less delays than those that require much technical and editorial correction.

The Editorial Board reserves the right to make literary corrections and to make suggestions to improve briefness.

It is vital, that authors take care in submitting a manuscript that is written in simple language and adheres to published guidelines.

Format

Language: The language of publication is UK English. Authors, for whom English is a second language, must have their manuscript efficiently edited by an English-speaking person before submission to make sure that, the English is of high excellence. It is preferable, that manuscripts should be professionally edited.

Standard Usage, Abbreviations, and Units: Spelling and hyphenation should be conventional to The Concise Oxford English Dictionary. Statistics and measurements should at all times be given in figures, e.g. 16 min, except for when the number begins a sentence. When the number does not refer to a unit of measurement it should be spelt in full unless, it is 160 or greater.

Abbreviations supposed to be used carefully. The abbreviated name or expression is supposed to be cited in full at first usage, followed by the conventional abbreviation in parentheses.

Metric SI units are supposed to generally be used excluding where they conflict with current practice or are confusing. For illustration, 1.4 l rather than 1.4 × 10-3 m3, or 4 mm somewhat than 4 × 10-3 m. Chemical formula and solutions must identify the form used, e.g. anhydrous or hydrated, and the concentration must be in clearly defined units. Common species names should be followed by underlines at the first mention. For following use the generic name should be constricted to a single letter, if it is clear.

Structure

All manuscripts submitted to Global Journals Inc. (US), ought to include:

Title: The title page must carry an instructive title that reflects the content, a running title (less than 45 characters together with spaces), names of the authors and co-authors, and the place(s) wherever the work was carried out. The full postal address in addition with the e-mail address of related author must be given. Up to eleven keywords or very brief phrases have to be given to help data retrieval, mining and indexing.

Abstract, used in Original Papers and Reviews:

Optimizing Abstract for Search Engines

Many researchers searching for information online will use search engines such as Google, Yahoo or similar. By optimizing your paper for search engines, you will amplify the chance of someone finding it. This in turn will make it more likely to be viewed and/or cited in a further work. Global Journals Inc. (US) have compiled these guidelines to facilitate you to maximize the web-friendliness of the most public part of your paper.

Key Words

A major linchpin in research work for the writing research paper is the keyword search, which one will employ to find both library and Internet resources.

One must be persistent and creative in using keywords. An effective keyword search requires a strategy and planning a list of possible keywords and phrases to try.

Search engines for most searches, use Boolean searching, which is somewhat different from Internet searches. The Boolean search uses "operators," words (and, or, not, and near) that enable you to expand or narrow your affords. Tips for research paper while preparing research paper are very helpful guideline of research paper.

Choice of key words is first tool of tips to write research paper. Research paper writing is an art.A few tips for deciding as strategically as possible about keyword search:

- One should start brainstorming lists of possible keywords before even begin searching. Think about the most important concepts related to research work. Ask, "What words would a source have to include to be truly valuable in research paper?" Then consider synonyms for the important words.
- It may take the discovery of only one relevant paper to let steer in the right keyword direction because in most databases, the keywords under which a research paper is abstracted are listed with the paper.
- One should avoid outdated words.

Keywords are the key that opens a door to research work sources. Keyword searching is an art in which researcher's skills are bound to improve with experience and time.

Numerical Methods: Numerical methods used should be clear and, where appropriate, supported by references.

Acknowledgements: Please make these as concise as possible.

References

References follow the Harvard scheme of referencing. References in the text should cite the authors' names followed by the time of their publication, unless there are three or more authors when simply the first author's name is quoted followed by et al. unpublished work has to only be cited where necessary, and only in the text. Copies of references in press in other journals have to be supplied with submitted typescripts. It is necessary that all citations and references be carefully checked before submission, as mistakes or omissions will cause delays.

References to information on the World Wide Web can be given, but only if the information is available without charge to readers on an official site. Wikipedia and Similar websites are not allowed where anyone can change the information. Authors will be asked to make available electronic copies of the cited information for inclusion on the Global Journals Inc. (US) homepage at the judgment of the Editorial Board.

The Editorial Board and Global Journals Inc. (US) recommend that, citation of online-published papers and other material should be done via a DOI (digital object identifier). If an author cites anything, which does not have a DOI, they run the risk of the cited material not being noticeable.

The Editorial Board and Global Journals Inc. (US) recommend the use of a tool such as Reference Manager for reference management and formatting.

Tables, Figures and Figure Legends

Tables: Tables should be few in number, cautiously designed, uncrowned, and include only essential data. Each must have an Arabic number, e.g. Table 4, a self-explanatory caption and be on a separate sheet. Vertical lines should not be used.

Figures: Figures are supposed to be submitted as separate files. Always take in a citation in the text for each figure using Arabic numbers, e.g. Fig. 4. Artwork must be submitted online in electronic form by e-mailing them.

Preparation of Electronic Figures for Publication

Even though low quality images are sufficient for review purposes, print publication requires high quality images to prevent the final product being blurred or fuzzy. Submit (or e-mail) EPS (line art) or TIFF (halftone/photographs) files only. MS PowerPoint and Word Graphics are unsuitable for printed pictures. Do not use pixel-oriented software. Scans (TIFF only) should have a resolution of at least 350 dpi (halftone) or 700 to 1100 dpi (line drawings) in relation to the imitation size. Please give the data for figures in black and white or submit a Color Work Agreement Form. EPS files must be saved with fonts embedded (and with a TIFF preview, if possible).

For scanned images, the scanning resolution (at final image size) ought to be as follows to ensure good reproduction: line art: >650 dpi; halftones (including gel photographs) : >350 dpi; figures containing both halftone and line images: >650 dpi.

Color Charges: It is the rule of the Global Journals Inc. (US) for authors to pay the full cost for the reproduction of their color artwork. Hence, please note that, if there is color artwork in your manuscript when it is accepted for publication, we would require you to complete and return a color work agreement form before your paper can be published.

Figure Legends: Self-explanatory legends of all figures should be incorporated separately under the heading 'Legends to Figures'. In the full-text online edition of the journal, figure legends may possibly be truncated in abbreviated links to the full screen version. Therefore, the first 100 characters of any legend should notify the reader, about the key aspects of the figure.

6. AFTER ACCEPTANCE

Upon approval of a paper for publication, the manuscript will be forwarded to the dean, who is responsible for the publication of the Global Journals Inc. (US).

6.1 Proof Corrections

The corresponding author will receive an e-mail alert containing a link to a website or will be attached. A working e-mail address must therefore be provided for the related author.

Acrobat Reader will be required in order to read this file. This software can be downloaded

(Free of charge) from the following website:

www.adobe.com/products/acrobat/readstep2.html. This will facilitate the file to be opened, read on screen, and printed out in order for any corrections to be added. Further instructions will be sent with the proof.

Proofs must be returned to the dean at dean@globaljournals.org within three days of receipt.

As changes to proofs are costly, we inquire that you only correct typesetting errors. All illustrations are retained by the publisher. Please note that the authors are responsible for all statements made in their work, including changes made by the copy editor.

6.2 Early View of Global Journals Inc. (US) (Publication Prior to Print)

The Global Journals Inc. (US) are enclosed by our publishing's Early View service. Early View articles are complete full-text articles sent in advance of their publication. Early View articles are absolute and final. They have been completely reviewed, revised and edited for publication, and the authors' final corrections have been incorporated. Because they are in final form, no changes can be made after sending them. The nature of Early View articles means that they do not yet have volume, issue or page numbers, so Early View articles cannot be cited in the conventional way.

6.3 Author Services

Online production tracking is available for your article through Author Services. Author Services enables authors to track their article - once it has been accepted - through the production process to publication online and in print. Authors can check the status of their articles online and choose to receive automated e-mails at key stages of production. The authors will receive an e-mail with a unique link that enables them to register and have their article automatically added to the system. Please ensure that a complete e-mail address is provided when submitting the manuscript.

6.4 Author Material Archive Policy

Please note that if not specifically requested, publisher will dispose off hardcopy & electronic information submitted, after the two months of publication. If you require the return of any information submitted, please inform the Editorial Board or dean as soon as possible.

6.5 Offprint and Extra Copies

A PDF offprint of the online-published article will be provided free of charge to the related author, and may be distributed according to the Publisher's terms and conditions. Additional paper offprint may be ordered by emailing us at: editor@globaljournals.org .

You must strictly follow above Author Guidelines before submitting your paper or else we will not at all be responsible for any corrections in future in any of the way.

Before start writing a good quality Computer Science Research Paper, let us first understand what is Computer Science Research Paper? So, Computer Science Research Paper is the paper which is written by professionals or scientists who are associated to Computer Science and Information Technology, or doing research study in these areas. If you are novel to this field then you can consult about this field from your supervisor or guide.

TECHNIQUES FOR WRITING A GOOD QUALITY RESEARCH PAPER:

1. Choosing the topic: In most cases, the topic is searched by the interest of author but it can be also suggested by the guides. You can have several topics and then you can judge that in which topic or subject you are finding yourself most comfortable. This can be done by asking several questions to yourself, like Will I be able to carry our search in this area? Will I find all necessary recourses to accomplish the search? Will I be able to find all information in this field area? If the answer of these types of questions will be "Yes" then you can choose that topic. In most of the cases, you may have to conduct the surveys and have to visit several places because this field is related to Computer Science and Information Technology. Also, you may have to do a lot of work to find all rise and falls regarding the various data of that subject. Sometimes, detailed information plays a vital role, instead of short information.

2. Evaluators are human: First thing to remember that evaluators are also human being. They are not only meant for rejecting a paper. They are here to evaluate your paper. So, present your Best.

3. Think Like Evaluators: If you are in a confusion or getting demotivated that your paper will be accepted by evaluators or not, then think and try to evaluate your paper like an Evaluator. Try to understand that what an evaluator wants in your research paper and automatically you will have your answer.

4. Make blueprints of paper: The outline is the plan or framework that will help you to arrange your thoughts. It will make your paper logical. But remember that all points of your outline must be related to the topic you have chosen.

5. Ask your Guides: If you are having any difficulty in your research, then do not hesitate to share your difficulty to your guide (if you have any). They will surely help you out and resolve your doubts. If you can't clarify what exactly you require for your work then ask the supervisor to help you with the alternative. He might also provide you the list of essential readings.

6. Use of computer is recommended: As you are doing research in the field of Computer Science, then this point is quite obvious.

7. Use right software: Always use good quality software packages. If you are not capable to judge good software then you can lose quality of your paper unknowingly. There are various software programs available to help you, which you can get through Internet.

8. Use the Internet for help: An excellent start for your paper can be by using the Google. It is an excellent search engine, where you can have your doubts resolved. You may also read some answers for the frequent question how to write my research paper or find model research paper. From the internet library you can download books. If you have all required books make important reading selecting and analyzing the specified information. Then put together research paper sketch out.

9. Use and get big pictures: Always use encyclopedias, Wikipedia to get pictures so that you can go into the depth.

10. Bookmarks are useful: When you read any book or magazine, you generally use bookmarks, right! It is a good habit, which helps to not to lose your continuity. You should always use bookmarks while searching on Internet also, which will make your search easier.

11. Revise what you wrote: When you write anything, always read it, summarize it and then finalize it.

12. Make all efforts: Make all efforts to mention what you are going to write in your paper. That means always have a good start. Try to mention everything in introduction, that what is the need of a particular research paper. Polish your work by good skill of writing and always give an evaluator, what he wants.

13. Have backups: When you are going to do any important thing like making research paper, you should always have backup copies of it either in your computer or in paper. This will help you to not to lose any of your important.

14. Produce good diagrams of your own: Always try to include good charts or diagrams in your paper to improve quality. Using several and unnecessary diagrams will degrade the quality of your paper by creating "hotchpotch." So always, try to make and include those diagrams, which are made by your own to improve readability and understandability of your paper.

15. Use of direct quotes: When you do research relevant to literature, history or current affairs then use of quotes become essential but if study is relevant to science then use of quotes is not preferable.

16. Use proper verb tense: Use proper verb tenses in your paper. Use past tense, to present those events that happened. Use present tense to indicate events that are going on. Use future tense to indicate future happening events. Use of improper and wrong tenses will confuse the evaluator. Avoid the sentences that are incomplete.

17. Never use online paper: If you are getting any paper on Internet, then never use it as your research paper because it might be possible that evaluator has already seen it or maybe it is outdated version.

18. Pick a good study spot: To do your research studies always try to pick a spot, which is quiet. Every spot is not for studies. Spot that suits you choose it and proceed further.

19. Know what you know: Always try to know, what you know by making objectives. Else, you will be confused and cannot achieve your target.

20. Use good quality grammar: Always use a good quality grammar and use words that will throw positive impact on evaluator. Use of good quality grammar does not mean to use tough words, that for each word the evaluator has to go through dictionary. Do not start sentence with a conjunction. Do not fragment sentences. Eliminate one-word sentences. Ignore passive voice. Do not ever use a big word when a diminutive one would suffice. Verbs have to be in agreement with their subjects. Prepositions are not expressions to finish sentences with. It is incorrect to ever divide an infinitive. Avoid clichés like the disease. Also, always shun irritating alliteration. Use language that is simple and straight forward. put together a neat summary.

21. Arrangement of information: Each section of the main body should start with an opening sentence and there should be a changeover at the end of the section. Give only valid and powerful arguments to your topic. You may also maintain your arguments with records.

22. Never start in last minute: Always start at right time and give enough time to research work. Leaving everything to the last minute will degrade your paper and spoil your work.

23. Multitasking in research is not good: Doing several things at the same time proves bad habit in case of research activity. Research is an area, where everything has a particular time slot. Divide your research work in parts and do particular part in particular time slot.

24. Never copy others' work: Never copy others' work and give it your name because if evaluator has seen it anywhere you will be in trouble.

25. Take proper rest and food: No matter how many hours you spend for your research activity, if you are not taking care of your health then all your efforts will be in vain. For a quality research, study is must, and this can be done by taking proper rest and food.

26. Go for seminars: Attend seminars if the topic is relevant to your research area. Utilize all your resources.

27. Refresh your mind after intervals: Try to give rest to your mind by listening to soft music or by sleeping in intervals. This will also improve your memory.

28. Make colleagues: Always try to make colleagues. No matter how sharper or intelligent you are, if you make colleagues you can have several ideas, which will be helpful for your research.

29. Think technically: Always think technically. If anything happens, then search its reasons, its benefits, and demerits.

30. Think and then print: When you will go to print your paper, notice that tables are not be split, headings are not detached from their descriptions, and page sequence is maintained.

31. Adding unnecessary information: Do not add unnecessary information, like, I have used MS Excel to draw graph. Do not add irrelevant and inappropriate material. These all will create superfluous. Foreign terminology and phrases are not apropos. One should NEVER take a broad view. Analogy in script is like feathers on a snake. Not at all use a large word when a very small one would be sufficient. Use words properly, regardless of how others use them. Remove quotations. Puns are for kids, not grunt readers. Amplification is a billion times of inferior quality than sarcasm.

32. Never oversimplify everything: To add material in your research paper, never go for oversimplification. This will definitely irritate the evaluator. Be more or less specific. Also too, by no means, ever use rhythmic redundancies. Contractions aren't essential and shouldn't be there used. Comparisons are as terrible as clichés. Give up ampersands and abbreviations, and so on. Remove commas, that are, not necessary. Parenthetical words however should be together with this in commas. Understatement is all the time the complete best way to put onward earth-shaking thoughts. Give a detailed literary review.

33. Report concluded results: Use concluded results. From raw data, filter the results and then conclude your studies based on measurements and observations taken. Significant figures and appropriate number of decimal places should be used. Parenthetical remarks are prohibitive. Proofread carefully at final stage. In the end give outline to your arguments. Spot out perspectives of further study of this subject. Justify your conclusion by at the bottom of them with sufficient justifications and examples.

34. After conclusion: Once you have concluded your research, the next most important step is to present your findings. Presentation is extremely important as it is the definite medium though which your research is going to be in print to the rest of the crowd. Care should be taken to categorize your thoughts well and present them in a logical and neat manner. A good quality research paper format is essential because it serves to highlight your research paper and bring to light all necessary aspects in your research.

Informal Guidelines of Research Paper Writing

Key points to remember:

- Submit all work in its final form.
- Write your paper in the form, which is presented in the guidelines using the template.
- Please note the criterion for grading the final paper by peer-reviewers.

Final Points:

A purpose of organizing a research paper is to let people to interpret your effort selectively. The journal requires the following sections, submitted in the order listed, each section to start on a new page.

The introduction will be compiled from reference matter and will reflect the design processes or outline of basis that direct you to make study. As you will carry out the process of study, the method and process section will be constructed as like that. The result segment will show related statistics in nearly sequential order and will direct the reviewers next to the similar intellectual paths throughout the data that you took to carry out your study. The discussion section will provide understanding of the data and projections as to the implication of the results. The use of good quality references all through the paper will give the effort trustworthiness by representing an alertness of prior workings.

Writing a research paper is not an easy job no matter how trouble-free the actual research or concept. Practice, excellent preparation, and controlled record keeping are the only means to make straightforward the progression.

General style:

Specific editorial column necessities for compliance of a manuscript will always take over from directions in these general guidelines.

To make a paper clear

· Adhere to recommended page limits

Mistakes to evade

- Insertion a title at the foot of a page with the subsequent text on the next page
- Separating a table/chart or figure - impound each figure/table to a single page
- Submitting a manuscript with pages out of sequence

In every sections of your document

· Use standard writing style including articles ("a", "the," etc.)

· Keep on paying attention on the research topic of the paper

· Use paragraphs to split each significant point (excluding for the abstract)

· Align the primary line of each section

· Present your points in sound order

· Use present tense to report well accepted

· Use past tense to describe specific results

· Shun familiar wording, don't address the reviewer directly, and don't use slang, slang language, or superlatives

· Shun use of extra pictures - include only those figures essential to presenting results

Title Page:

Choose a revealing title. It should be short. It should not have non-standard acronyms or abbreviations. It should not exceed two printed lines. It should include the name(s) and address (es) of all authors.

Abstract:

The summary should be two hundred words or less. It should briefly and clearly explain the key findings reported in the manuscript--must have precise statistics. It should not have abnormal acronyms or abbreviations. It should be logical in itself. Shun citing references at this point.

An abstract is a brief distinct paragraph summary of finished work or work in development. In a minute or less a reviewer can be taught the foundation behind the study, common approach to the problem, relevant results, and significant conclusions or new questions.

Write your summary when your paper is completed because how can you write the summary of anything which is not yet written? Wealth of terminology is very essential in abstract. Yet, use comprehensive sentences and do not let go readability for briefness. You can maintain it succinct by phrasing sentences so that they provide more than lone rationale. The author can at this moment go straight to shortening the outcome. Sum up the study, with the subsequent elements in any summary. Try to maintain the initial two items to no more than one ruling each.

- Reason of the study - theory, overall issue, purpose
- Fundamental goal
- To the point depiction of the research
- Consequences, including definite statistics - if the consequences are quantitative in nature, account quantitative data; results of any numerical analysis should be reported
- Significant conclusions or questions that track from the research(es)

Approach:

- Single section, and succinct
- As a outline of job done, it is always written in past tense
- A conceptual should situate on its own, and not submit to any other part of the paper such as a form or table
- Center on shortening results - bound background information to a verdict or two, if completely necessary
- What you account in an conceptual must be regular with what you reported in the manuscript
- Exact spelling, clearness of sentences and phrases, and appropriate reporting of quantities (proper units, important statistics) are just as significant in an abstract as they are anywhere else

Introduction:

The **Introduction** should "introduce" the manuscript. The reviewer should be presented with sufficient background information to be capable to comprehend and calculate the purpose of your study without having to submit to other works. The basis for the study should be offered. Give most important references but shun difficult to make a comprehensive appraisal of the topic. In the introduction, describe the problem visibly. If the problem is not acknowledged in a logical, reasonable way, the reviewer will have no attention in your result. Speak in common terms about techniques used to explain the problem, if needed, but do not present any particulars about the protocols here. Following approach can create a valuable beginning:

- Explain the value (significance) of the study
- Shield the model - why did you employ this particular system or method? What is its compensation? You strength remark on its appropriateness from a abstract point of vision as well as point out sensible reasons for using it.
- Present a justification. Status your particular theory (es) or aim(s), and describe the logic that led you to choose them.
- Very for a short time explain the tentative propose and how it skilled the declared objectives.

Approach:

- Use past tense except for when referring to recognized facts. After all, the manuscript will be submitted after the entire job is done.
- Sort out your thoughts; manufacture one key point with every section. If you make the four points listed above, you will need a least of four paragraphs.

- Present surroundings information only as desirable in order hold up a situation. The reviewer does not desire to read the whole thing you know about a topic.
- Shape the theory/purpose specifically - do not take a broad view.
- As always, give awareness to spelling, simplicity and correctness of sentences and phrases.

Procedures (Methods and Materials):

This part is supposed to be the easiest to carve if you have good skills. A sound written Procedures segment allows a capable scientist to replacement your results. Present precise information about your supplies. The suppliers and clarity of reagents can be helpful bits of information. Present methods in sequential order but linked methodologies can be grouped as a segment. Be concise when relating the protocols. Attempt for the least amount of information that would permit another capable scientist to spare your outcome but be cautious that vital information is integrated. The use of subheadings is suggested and ought to be synchronized with the results section. When a technique is used that has been well described in another object, mention the specific item describing a way but draw the basic principle while stating the situation. The purpose is to text all particular resources and broad procedures, so that another person may use some or all of the methods in one more study or referee the scientific value of your work. It is not to be a step by step report of the whole thing you did, nor is a methods section a set of orders.

Materials:

- Explain materials individually only if the study is so complex that it saves liberty this way.
- Embrace particular materials, and any tools or provisions that are not frequently found in laboratories.
- Do not take in frequently found.
- If use of a definite type of tools.
- Materials may be reported in a part section or else they may be recognized along with your measures.

Methods:

- Report the method (not particulars of each process that engaged the same methodology)
- Describe the method entirely
- To be succinct, present methods under headings dedicated to specific dealings or groups of measures
- Simplify - details how procedures were completed not how they were exclusively performed on a particular day.
- If well known procedures were used, account the procedure by name, possibly with reference, and that's all.

Approach:

- It is embarrassed or not possible to use vigorous voice when documenting methods with no using first person, which would focus the reviewer's interest on the researcher rather than the job. As a result when script up the methods most authors use third person passive voice.
- Use standard style in this and in every other part of the paper - avoid familiar lists, and use full sentences.

What to keep away from

- Resources and methods are not a set of information.
- Skip all descriptive information and surroundings - save it for the argument.
- Leave out information that is immaterial to a third party.

Results:

The principle of a results segment is to present and demonstrate your conclusion. Create this part a entirely objective details of the outcome, and save all understanding for the discussion.

The page length of this segment is set by the sum and types of data to be reported. Carry on to be to the point, by means of statistics and tables, if suitable, to present consequences most efficiently.You must obviously differentiate material that would usually be incorporated in a study editorial from any unprocessed data or additional appendix matter that would not be available. In fact, such matter should not be submitted at all except requested by the instructor.

Content

- Sum up your conclusion in text and demonstrate them, if suitable, with figures and tables.
- In manuscript, explain each of your consequences, point the reader to remarks that are most appropriate.
- Present a background, such as by describing the question that was addressed by creation an exacting study.
- Explain results of control experiments and comprise remarks that are not accessible in a prescribed figure or table, if appropriate.
- Examine your data, then prepare the analyzed (transformed) data in the form of a figure (graph), table, or in manuscript form.

What to stay away from

- Do not discuss or infer your outcome, report surroundings information, or try to explain anything.
- Not at all, take in raw data or intermediate calculations in a research manuscript.
- Do not present the similar data more than once.
- Manuscript should complement any figures or tables, not duplicate the identical information.
- Never confuse figures with tables - there is a difference.

Approach

- As forever, use past tense when you submit to your results, and put the whole thing in a reasonable order.
- Put figures and tables, appropriately numbered, in order at the end of the report
- If you desire, you may place your figures and tables properly within the text of your results part.

Figures and tables

- If you put figures and tables at the end of the details, make certain that they are visibly distinguished from any attach appendix materials, such as raw facts
- Despite of position, each figure must be numbered one after the other and complete with subtitle
- In spite of position, each table must be titled, numbered one after the other and complete with heading
- All figure and table must be adequately complete that it could situate on its own, divide from text

Discussion:

The Discussion is expected the trickiest segment to write and describe. A lot of papers submitted for journal are discarded based on problems with the Discussion. There is no head of state for how long a argument should be. Position your understanding of the outcome visibly to lead the reviewer through your conclusions, and then finish the paper with a summing up of the implication of the study. The purpose here is to offer an understanding of your results and hold up for all of your conclusions, using facts from your research and generally accepted information, if suitable. The implication of result should be visibly described. Infer your data in the conversation in suitable depth. This means that when you clarify an observable fact you must explain mechanisms that may account for the observation. If your results vary from your prospect, make clear why that may have happened. If your results agree, then explain the theory that the proof supported. It is never suitable to just state that the data approved with prospect, and let it drop at that.

- Make a decision if each premise is supported, discarded, or if you cannot make a conclusion with assurance. Do not just dismiss a study or part of a study as "uncertain."
- Research papers are not acknowledged if the work is imperfect. Draw what conclusions you can based upon the results that you have, and take care of the study as a finished work
- You may propose future guidelines, such as how the experiment might be personalized to accomplish a new idea.
- Give details all of your remarks as much as possible, focus on mechanisms.
- Make a decision if the tentative design sufficiently addressed the theory, and whether or not it was correctly restricted.
- Try to present substitute explanations if sensible alternatives be present.
- One research will not counter an overall question, so maintain the large picture in mind, where do you go next? The best studies unlock new avenues of study. What questions remain?
- Recommendations for detailed papers will offer supplementary suggestions.

Approach:

- When you refer to information, differentiate data generated by your own studies from available information
- Submit to work done by specific persons (including you) in past tense.
- Submit to generally acknowledged facts and main beliefs in present tense.

Please carefully note down following rules and regulation before submitting your Research Paper to Global Journals Inc. (US):

Segment Draft and Final Research Paper: You have to strictly follow the template of research paper. If it is not done your paper may get rejected.

- The **major constraint** is that you must independently make all content, tables, graphs, and facts that are offered in the paper. You must write each part of the paper wholly on your own. The Peer-reviewers need to identify your own perceptive of the concepts in your own terms. NEVER extract straight from any foundation, and never rephrase someone else's analysis.

- Do not give permission to anyone else to "PROOFREAD" your manuscript.

- Methods to avoid Plagiarism is applied by us on every paper, if found guilty, you will be blacklisted by all of our collaborated research groups, your institution will be informed for this and strict legal actions will be taken immediately.)
- To guard yourself and others from possible illegal use please do not permit anyone right to use to your paper and files.

Criterion for Grading a Research Paper (Compilation) by Global Journals Inc. (US)

Please note that following table is only a Grading of "Paper Compilation" and not on "Performed/Stated Research" whose grading solely depends on Individual Assigned Peer Reviewer and Editorial Board Member. These can be available only on request and after decision of Paper. This report will be the property of Global Journals Inc. (US).

Topics	Grades		
	A-B	**C-D**	**E-F**
Abstract	Clear and concise with appropriate content, Correct format. 200 words or below	Unclear summary and no specific data, Incorrect form Above 200 words	No specific data with ambiguous information Above 250 words
Introduction	Containing all background details with clear goal and appropriate details, flow specification, no grammar and spelling mistake, well organized sentence and paragraph, reference cited	Unclear and confusing data, appropriate format, grammar and spelling errors with unorganized matter	Out of place depth and content, hazy format
Methods and Procedures	Clear and to the point with well arranged paragraph, precision and accuracy of facts and figures, well organized subheads	Difficult to comprehend with embarrassed text, too much explanation but completed	Incorrect and unorganized structure with hazy meaning
Result	Well organized, Clear and specific, Correct units with precision, correct data, well structuring of paragraph, no grammar and spelling mistake	Complete and embarrassed text, difficult to comprehend	Irregular format with wrong facts and figures
Discussion	Well organized, meaningful specification, sound conclusion, logical and concise explanation, highly structured paragraph reference cited	Wordy, unclear conclusion, spurious	Conclusion is not cited, unorganized, difficult to comprehend
References	Complete and correct format, well organized	Beside the point, Incomplete	Wrong format and structuring

Index

A

Asynchronous · 11, 14, 15, 16, 17, 21

C

Caldeweyher · 61, 69
Concatenating · 57

H

Holesalgorithm · 49

M

Mockjax · 19, 21
Movassaghi · 27, 32

N

Nomenclature · 22, 23

P

Postgresql · 61, 64, 69
Pseudonymity · 5

U

Ubiquitous · 1, 5, 24, 31
Underutilized · 45

save our planet

Global Journal of Computer Science and Technology

Visit us on the Web at www.GlobalJournals.org | www.ComputerResearch.org
or email us at helpdesk@globaljournals.org

ISSN 9754350