EP Journal on Digital Signal Processing

Volume No. 09

Issue No. 1

January - April 2025

ENRICHED PUBLICATIONS PVT.LTD

JE - 18,Gupta Colony, Khirki Extn,
Malviya Nagar, New Delhi - 110017.
E- Mail: info@enrichedpublication.com
Phone :- +91-8877340707

EP Journal on Digital Signal Processing

Aims and Scope

EP Journal on Digital Signal Processings has become very important with the ever-increasing demands of the software development to serve the millions of applications across various disciplines. For large software projects, innovative software development approaches are of vital importance. In order to gain higher software standard and efficiency, software process adaptation must be derived from social behavior, planning, strategy, intelligent computing, etc.,

based on various factors. International Journal of Software Engineering address the state of the art of all aspects of software engineering, highlighting the all tools and techniques for the software development process.

EP Journal on Digital Signal Processing

EP Journal on Digital Signal Processing

(Volume No. 09, Issue No. 1, January - April 2025)

Contents

Study of Various Applications of Internet of Things

G. K. Sasithra
SNS College of Technology,
Coimbatore, Tamil Nadu

ABSTRACT

The Internet of Things is getting to be one of the accomplishments in the time of systems administration that will discard the eventual fate of data innovation. IoT benefit associations with clients on anyplace, anything and at any minute. IoT is an imaginative thought that adjusts this present reality objects into virtual items. IoT empowers clients to power over marked things like entryway locks, lights, microwave, television, coffeemaker, clothes washer, window bolts, etc. and stays up with the latest about the state. The depiction of an idea IoT speaks to different innovations that make the internet accessible to every certifiable substantial item. In this paper, we centre on the different uses of IoT like interoperability, keen urban areas, shrewd medication, workplaces, home, transportation, vegetable reconcilability framework in agribusiness, cyber security, eCommerce, etc. This paper additionally centres on the middleware which goes about as a product layer between the IT foundations and furthermore conceals the usage details of the software engineers. This paper additionally puts light on how temperature influences IoT.

Keywords: IoT, administration, innovations, imaginative, internet, temperature

INTRODUCTION

Modish structures on each side of the web have turned out to be tangled and broadened, confronting a quick change from remote frameworks to ubiquitous web-based things which are fit for creating information that can be broke down to produce helpful data. We are touching base in an ongoing age of figuring innovation named as the internet of things, step up business profitability, refine government mastery, develop every one's life, etc. Internet of things (IoT) is structured based on the web, comprises of new sort of difficulties. In view of the association of different correspondence stacks, old style security natives can't be straightly applied to IoT computerization.

IoT is a mentally associated framework like radio including Brainy machines conveying and cooperating with different machines or gadgets, items, condition and foundation lastly asset compelled gadgets like radio recurrence distinguishing proof (RFID's) and remote sensor systems. Subsequently, a movable foundation is should have been adjusted to accord with security and protection dangers in powerful conditions. Internet of Things has shown up as one of the most grounded correspondence models of the 21st century. The things that we utilized in our everyday life like a clothes washer, entryway lock, etc. Become some portion of the web because of their registering abilities, for example,

handsets, microcontrollers and reasonable convention stacks that grant them to interface with different items. IoT incorporates various types of modest sensors named as wearable, ecological and embedded in the social insurance area that enables matured individuals to appreciate medicinal services wherever and at any minute. RFID is one of the generous advances utilized in IoT on the purpose of putting away delicate information, follow/perceive questions naturally. Presently, RFID utilized elliptic bend cryptography-based RFID confirmation plans have connected. Contiki, mbed OS, Tiny os, RIOT, Brillo are a portion of the working frameworks for IoT which supports numerous gadgets and xively, kaa, IBM bluemix, carriols, nimbits, are a portion of the stages utilized by IoT which bolster administrations like application advancement, information the executives, and information related administrations. During 2008, the quantity of things associated with the web is more than the quantity of individuals on earth. By 2020, there will be 50 billion things associated with the web. IoT grants individuals and things to be associated with web whenever with anybody/anything and at wherever.

LITERATURE REVIEW

J. Darker et. Al dealt with how IoT correspondence is impacted by natural temperature. They additionally show that how high-temperature changes and stickiness impacts/influences the working of directing conventions and correspondence joins, remote inserted frameworks, clock float, battery limit, electronic materials, battery limit, and release and remote sensor frameworks. High temperature up to 70OC experienced by the framework especially in the event that it assimilates infrared beams which mounted that the ecological temperature of a framework can contrast outside by 35OC in one hour and 56OC in the entire day. In this paper, the creator gives a demo of two segments. In the previous part, they show how WSN and directing convention is influenced by temperature when then they will associate with Templab (a temperature-controlled experimental foundation) that is able to do precisely contrasting the locally available temperature of WSN. In the last part, the creator estimates the sign debasement by utilizing max for MTM-CM5000MSP WSN on which two will be mended by utilizing infrared lights to decide how locally available temperature impacts on correspondence. [1]

W Zeng et. Al presented optical fiber detecting IoT innovation and their specific application that is utilized in the mine security relies upon the optic fiber IoT. [2]

Y. Qu et. Al presents a framework which has the identifiable capacity in farming IoT and talks about its applications in the zones of coordination's, planting, natural observing, stockpiling, item handling, home, office, transportation, and human services. IoT can improve the nature of rural items from unique to completion by dissecting the development of items, variable of air and soil, adjusting the water system and preparation by means of the web and PC. Different advancements like Zigbee, GPRS and

RFID are utilized to distinguish the e-mark on the vegetables. This can bring social and monetary advantages for agribusiness. The trial area is partitioned into four connections given below. [3]

Table 1 Environmental Section

Planting Link	**This keeps tracks of the data with respect to seed treatment, water system, medicine preparation, generation date, reap bundling, and so forth**
Processing Link	**It follows the data of item name, evaluation, and quality-related data, handling date, bundling material, the time span of usability, and so forth.**
Logistics Link	**It Traces the data of continuous checking vehicles, etc**
Vegetable Consumption Link	**It follows the data of vegetables in the connection of preparing, planting, transportation, etc.**

V Avachat et. Al reads semantic middleware for IoT which is a product layer that extension the IoT application and IOT IT framework. The thought behind middleware is giving deliberation with the goal that the different utilizations of IoT can be created by software engineers. Middleware achieves a common standard among various dissimilar to/heterogeneous gadgets gives holding between different sorts of items, goes about as interface among gadgets and their administrations for correspondence and it is better justifiable by things and people. In this paper, creator characterizes a few qualities of middleware like adaptability, unconstrained association, zero foundation, assortment, interoperability, setting a location, gadget revelation, and the board, security and protection, reflection, overseeing enormous volume of information that is significant in building up middleware for IoT. To comprehend the design and to establish out which highlights they have, the creator talked about three arrangements of middleware in this paper named as triple divided based conveyed middleware, UBWARE, and SOA based middleware. The correspondence is finished utilizing shared space rather than message-based correspondence in triple space-based figuring where semantic information in asset portrayal system is communicated. In middleware, objects are executed in various condition and correspondence without knowing anything. There are two items named as specialist co-ops (offer administrations) and buyers (needs benefits) are characterized. To run the middleware, API is proposed by middleware. To carry out the responsibility of arrangement (coordination of the articles to create an ideal impact), programmed reconciliation, UBWARE based middleware is proposed which has the observation to create

independent self-guided parts. To design complex usefulness, find administration demands, to screen the condition of the articles for settling on choices and to find each other specialist innovation is utilized by middleware. Different issues are featured by the creator in this paper is triple space-based figuring is poor in adaptability, UBWARE is poor in security and protection and SOA is poor in setting identification. In this Paper Author Also Proposed middleware rely upon administration situated design SOA where every item gives administration as usefulness and its attributes are adaptability, zero frameworks, unconstrained connection, gadget revelation, security and protection, deliberation and interoperability. It doesn't bolster setting detection.[4]

S. Roy et. Al proposed DSS model structure for the checking driving principle infringement dependent on IoT in light of the fact that the vast majority of the mishaps occurred because of driver absence of consideration, because of the utilization of mobiles and due to ignoring of traffic rules. For taking care of this issue, the creator recommends a thought of three-layer various leveled haze-based traffic noncompliance observing DSS model structure for portability backing and better area mindfulness. [5]

Table 2 DSS Model Framework

Lower Layer	**LCS (Local Camera Sensor) and GCS (Global Camera Sensor) are required. LCS sensor which detects driver action and cautions them is conveyed inside the vehicle. GCS which perceive vehicle number is conveyed inside traffic flagging shaft**
Middle Layer	**It gets the vehicle personality and number from LCS and GCS resp. also, discover the vehicle who damage the transit regulations by utilizing the telephone during driving and send that data to the cloud server**
Upper Layer	**It gives results rely upon criminal traffic offence law book**

G. Li et. al planned an IoT portal for nursery observing framework by utilizing various access techniques like Wi-Fi, LAN, 3G, GPRS, etc. The STM32 is utilized by IoT Gateway as the installed OS, UC/OS-III, MCU. The application demonstrates the door is perfect, extendible and solid. Continuous identification, control of the nursery, improves the intensity of the computerization and the astuteness of

the nursery observing is cultivated by the nursery checking framework because of this passage. The passage relies upon modularized technique and its capacity is acknowledged information gathering, preparing remote client control information. The modularization technique meets the prerequisites of the confused rural condition and upgrades the similarity. It envisions the transmission among WSN and the web if remote conveys among portal and upper PC. On the off chance that the correspondence is lost in all systems, at that point, SD card will store the information and transmit it to the upper PC when an association is built up in system. The information is moved from upper PC to ZigBee organizer and afterward ZigBee facilitator to procurement and control framework (ACS). The ACS sends information to a microcontroller and afterward, microcontroller exemplifies the information and send back to ACS and afterward to ZigBee facilitator and after that to upper PC by means of GPRS or Ethernet. LabVIEW structured the product of PC created by NI organization, receives realistic language and its conduct is shown by realistic images and evacuate the perplexing principles of syntax to show the control and aftereffect of the framework. It is appropriate to take care of the issue of information procurement, gathering, dissect, record and waveform preparing and number-crunching tasks by LabVIEW. This application affirms that door run superb in the nursery checking framework by dependably and convenient exchanges nature information and control guidelines separately. Its applications are fine planting, remote shrewd checking, control nursery and cultivating logical planting crops. [6]

B.M Le et. al recommend a savvy administration model which gives powerful reaction to a person for medicinal services administration and distinguish the connection between shared illnesses and hazard elements named as hypertension, diabetes, and corpulence. They likewise propose intellectualized administration application calculation that will be worked in the individual wellbeing gadget. It made known the coordinated effort convention which movements hazard factors between IOT singular wellbeing gadgets. The analysis done in this paper demonstrated that exhaustive appraisal the board give progressively exact data contrasted with straightforward evaluation the executives about the condition of patients and it was demonstrated as a powerful model for patients to deal with a metabolic disorder. [7]

C.S Ryu proposed and structured a consolidated control framework and fire crisis reaction framework dependent on IoT utilizing sensors, for example, smoke alarms, heat identifiers, fire finders, ultrasonic sensors, vibration sensors, weight sensors, area control sensors and vicinity sensors and results the event of flame, noxious gas and the electrical sign in the structure and keenly guide individuals to crisis exit to decrease the death toll of people by crisis lights. It utilizes the WSN comprises sensors that measure the natural happenings like temperature, weight, seismic tremor and send the information to the control server and afterward server examine and process the information. To give correspondence, ZigBee is

utilized. The framework is planned comprises EM250 chipset, CDD controller, Sensor modules, a correspondence module, a CSD controller, a power module, ringers, and a LED presentation. [8]

C.M shah et.al proposed keen security arrangements dependent on the internet of things. Tm4CI23GXL improvement board is utilized. The information is transmitted by RFID peruser and biometric sensor to the microcontroller through information pins (D0, D1). Initial 26 bits are transmitted in which originally bit is even equality bit and the following 8 piece is office code and the following 16 bits are card number and the last piece is odd equality bit. On the off chance that two workers have the same card number, at that point office code are utilized to recognize it. The MCU transmits a sign to the Wi-Fi module; in the event that the legitimate unique mark or card number is gotten, at that point Wi-Fi trips the hand-off by accepting the sign. This is the working of how entryway opens. Savvy access control frameworks beat the issues looked by the business. Vitality proficiency can be accomplished by utilizing microcontrollers picked/chose. It executes AI and makes the framework shrewd that are utilized to look at timings and give get to. Assembled information can be utilized to oversee the effectiveness of laborers. A clicked photo transmitted on the server through Wi-Fi each time giving a second layer of security. It is additionally utilized in school and school study halls to gauge participation and make guardians state-of-the-art about their youngster participation records by transmitting it on the server. [9]

Y. sun put forward thought of disseminated railroad scaffold checking framework relies upon IOT to administer the security status of extension. In this creator did bounteous research on the sending of sensor hubs, updating of tactile arrangements and cautioning techniques for the WSN. For extension checking, the sound wave transmission strategy, low strain reflected wave technique, the centre technique and so forth are a portion of the customary strategies which has numerous disadvantages like the incomplete judgment of deformities, costly observing and so forth. Contrasted and the traditional strategies satellite situating observing technique came into power which has different attributes, for example, 3D exact estimation, short confinement, and synchronous solid constant estimation. The outfield and checking focus are the two sections required to structure the railroad observing framework. In the outfield focus, sensors are conveyed in the railroad lines and extensions to gather information, sensor arrangement technique are utilized to assemble information of different kinds of sensors, information transferring are utilized for crisis and day by day schedule information. The checking focus contains observing server which is utilized for constant checking and database which are utilized for putting away the sensor information. The correspondence is done in the middle of hubs of one kind and two hubs of the various sort in explicit organization strategy. The railroad observing system utilizes adhoc arrange. Media hubs are utilized to assemble picture data like break happens in extension and sensors are utilized to detect deck weight, the temperature of soil and data of wharfs removal. The

information is transmitted to the sink hub after information pressure, encryption and combination by means of multihop correspondence and after that moving to the observing host through web or train. The sensor hub conveyed on the extension and around railroad line works in two sections. The real work of the sensor hubs incorporates moistness sensors, weight sensors, misshapen sensors, media sensors, and temperature sensors sent on the scaffold is to direct the wellbeing status of the extension which gives staggered supervision of the scaffold. The significant work of the subsequent part is to move the information administered by the sensors on scaffold securely and quickly to the close-by screen focus with the goal that it can have constant control of the extension wellbeing. The following stage is data gathering in which the sensor hub gathers information and after that transmission happens. The information transmission happens in two kinds. The initial one is crisis information transmission which means a genuine cautioning the extension security along these lines, it sends by checking system sensor hubs to observing focus through the web which procedure crisis information and send the assembled information to the scaffold uprooting support. The second one is information transmission which is utilized to diminish the excess data transmission with the goal that sensor arrange hub and vitality utilization is spared. The subsequent stage is cautioning wellbeing information handling. In this paper, various sensors like removal sensors, temperature sensors, etc faculties different variables like one-sided disappointment, hamper, stun disappointment, float disappointment, and open circuit disappointment and gives a notice message. Be that as it may, at times because of vacillations in sensor arrange, WSN gives the wrong message. To evacuate this disadvantage more than once cautioning component is utilized. [10]

Mr. R Balasubramaniam et. al proposed elliptic curve cryptosystem (ECC) verified against all assaults since it gives encryption and unscrambling of information to anticipate unapproved get to. Its advantages are less control utilization, less memory, quick calculations, and data transfer capacity saver. It is utilized in web-based business, chip cards, compact gadgets, and savvy cards. Elgamal ECC has been proposed by the creator who gives encryption and unscrambling of any plaintext by utilizing the hexadecimal ASCII esteem for every letter set/Character and it is appropriate for human services condition. [11]

J. Jayakumar et al inspected IOT put together Smart Environment that depends with respect to RFID and distinguishes security and security issues and perceive the prerequisite for ensuring shopper protection. To proposed Data validation, Data uprightness and information Confidentiality, creator proposed "Execute Password" and "Access Password" Approach. [12]

L.Meng et. all proposed coal mineshaft groundwater observation framework dependent on IoT. Arranged Smart Sensors can be utilized as accumulation hubs on the detecting layer and to make novel sensors, late detecting techniques ought to be applied. To order remote correspondence and sensor systems administration, GSM and modern Ethernet have been implanted in the transmission layer. Distributed computing gives a modern answer for colossal informational collections stockpiling, investigation and handling on the application layer. For Coal mine hydrological issues, six sorts of topical data have been planned. [13]

In this paper, IoT gives a shrewd medicinal and physical wellbeing framework. By the utilization of IoT difficulties changes, that devours more labour, assets and time. Presently, the shrewd applications like keen home, brilliant rehabilitation become acclaimed contrasted with customary framework, the savvy rehabilitation is centring at giving a deliberate treatment, quick reconfiguration and satisfactory cooperation to utilizing the restorative assets. P. Elanthiraiyan et. al executes the human services administration in the earth and gives different attributes to actualize it.

Table 3 Characteristics

Evaluation of ontology	Data like inspected quiet side effects and recognized sicknesses are put away in the database. The specialist initial step is to investigate the sickness when the patient enters the emergency clinic
Comparison of Global Ontology	In view of the learning bases, the consequence of assessed metaphysics is separated to the infections put away comprehensively.Maladies metaphysics comprises quiet essential data and asset philosophy comprises medicinal assets like specialists and so on are the two types of worldwide ontology
Similarity Calculations	Perform likeness coordinating of the side effects
Optimization of Design	The last advance is to plan the all-around requested information structure and to advance the plan after likeness calculations step

For keen medication and to comprehend side effects creator proposed metaphysics-based structure strategy utilizing IoT. Its will probably interface every one of the assets and give data right away. These demonstrated to be successful and proficient for data sharing. For gathering the patient basic data and side effects and overseeing restorative history, the recovery technique is connected with the proposed engineering of IoT based wellbeing framework by conjuring the RFID and gives arrangements quickly. Creator understood that IoT is the universal presence of articles and things that are converged to accomplish a shared objective, they convey among themselves and they are produced to work with one another. To make the framework unmistakable, two principle attributes specifically quick development of reclamation framework and the area information distribution has been proposed. [14]

X. Xu broke down the advancement of IoT applications in internet business. Along these lines after the portable and web association with the system, IoT is another accommodation in the data Technology. To check this present reality, brilliant gadgets and detecting components were supported by IoT. Data is part between things or in the middle of human and things. In this paper, the headway point of IoT usage has been evaluated in web-based business, the issues are talked about in web-based business. There are following three basic conditions in IOT activity: internet business stock, coordination's, and instalment. Internet business presents the propelled business-standard where the consistent does the web-based shopping, online execution among dealer and the online modernized pictures. There is the expansive arrangement of monetary and endeavour activities around the globe, at an open system status of the web. The development Progress of IoT tasks has been evaluated in this paper. The IoT computerization and the administration key business must be refined in a related gathering of internet business. Debasement in the merchandise cost is seen and thus the edge is diminished. [15]

J. Kadlec et. al demonstrated a strategy for improving the productivity of stock administration by utilizing RFID innovation. The point of their examination is to structural engineering for directing and distinguishing the movement of as of now observed articles and its need is to make a particular framework for utilizing in applications like emergency clinic clothing the executives dependent on the standards of IoT stage. This is all conceivable through RFID innovation by lessening establishment costs. [16]

P. Vlacheas et. al structured a psychological administration system for empowering brilliant urban communities through the Internet of Things (IoT). [17]

Applications

Table 4 Applications of IoT

Area	Applications
HealthCare/Medical Field	Patient Monitoring, Realtime Health Status, Triage
Emergency and Security Area	Global Personnel Monitoring (Location, Health), Resource Planning, Resource Management and Distribution, Detect Exposure and Hazardous Gases, Radiation Level Detection, Liquid Monitor In Data Centres
Traffic Management	Smart Transportation Via Real Time Traffic, Path Optimization
Infrastructure Supervision	Sensors Fit into Infrastructure to Supervise Structural Fatigue, Accident Supervision for Incident Management and Emergency Outcome Coordination
Water Services	Water Quality, Usage, Leakage and Waste Management
Building Management Services	Humility Control Management, Temperature, Activity Supervision, Ventilation, Energy Usage Management and Hair Conditioning
Environment	Noise Monitoring, Air Pollution, Industry Monitoring
Smart Cities	Parking Areas Monitoring, Vibrations, Bridges, Material Conditions and Historical Monuments Monitoring, Monitoring in Buildings, Android Devices, iPhone Detection, Energy Radiated Measurement, Traffic Monitoring Vehicle, Pedestrian Level Monitoring

Smart Agriculture	Soil Moisture Monitoring, Greenhouse Monitoring, Control Humidity and Temperature Levels and Study Weather Conditions
Domestic and Home Automation	Energy and Water Consumption Monitoring, Remote Control Appliances Monitoring, Intrusion Detection Systems, Monitoring Conditions Inside Museums and At Warehouses
Industrial and Control Area	Oxygen Levels and Toxic Gases Monitoring Inside Chemical Plants, Temperature Monitoring, Ozone Level Monitoring

The different utilizations of IoT are ongoing emergency clinic clothing the executives, transport transportation, transport transportation, agribusiness and nursery checking framework, homeroom access control, savvy home, brilliant city, middleware, farming, medicinal, railroads, vegetation recognizability framework, etc. Ongoing Monitoring can be accomplished by the IoT portal-based Greenhouse framework. A sensor system comprises of a huge number of tiny, affordable, self-fueled gadgets that can detect, interface and figure with other devices for the thought process of gathering neighborhood data to make widespread goals about a physical situation. [20]

CONCLUSION

IoT benefit associations with clients on anyplace, anything and at any minute. IoT is an imaginative thought that adjusts this present reality objects into virtual articles. IoT empowers clients to authority over marked things like entryway locks, lights, microwave, television, coffeemaker, clothes washer, window bolts, etc. and stays up with the latest about the state. The portrayal of an idea IoT speaks to different advances that make the web accessible to every certifiable substantial article. In this paper, we center around the different utilizations of IoT like interoperability, brilliant urban areas, keen medication, workplaces, home, transportation, vegetable detectability framework in farming, digital security, internet business, etc. This paper likewise centers around the middleware which goes about as a product layer between the IT frameworks and furthermore conceals the usage technicalities of the software engineers. This paper likewise puts light on how temperature influences IoT.

		tier architecture of IOT		
13	[14]	Ontology Based System Design methodology for smart medicine and physical health system based on IoT	Quick construction of rehabilitation system and easy sharing of domain knowledge make the system different and perform efficient.	**Health monitoring and emergency health care system, industrial systems.**
14	[15]	RFID, infrared sensors, global positioning systems, laser scanners, gas sensors and other information sensing device	Improved efficiency, reduced operating costs, improved customer experience/lack in business models, product quality is difficult to guarantee, logistics are not in place, online payment service still needs to be improved, no sufficient support on online payment, payment security with hidden danger, user action cumbersome, unreliable security, no sufficient support on online payment, lag rules and regulations on online payment and logistics and distribution system problems.	**It is applied in e-commerce such as logistics, inventory and payment.**
15	[16]	It uses RFID technology for the identification of monitored objects	Improved effectiveness and efficiency of inventory management.	**Real hospital laundry management**
16	[17]	**Cognitive management framework is proposed**	**Qualitative and quantitative results.**	**Support Sustainable Smart City development.**

REFERENCES

[1] *J.Brown, U. Roedig, C.A.Boano, K. Romer and N. Tsiftes," Demo Abstracts: How Temperature Affects IOT Communication".*

[2] *W. Zeng and H. Gao, " Optic Fiber Sensing IoT Technology and Application Research", Sensors and Transducers by IFSA Publishing, http://www.sensorsportal.com, vol. 180, issue 10, oct 2014, pp. 16-21.*

[3] *Y. Qu and B. Tao, "The Constitution of vegetable traceability system in agricultural IOT",ISSN-0975-7384, Journal of Chemical and Pharmaceutical research, vol. 6(7), 2014, pp. 2580-2583.*

[4] *V. Avachat, P. Gupta, "A Study of Semantic Middleware for Internet of Things", ISSN: 2277 128X, IJARCSSE, Vol 4, Issue 12, Dec 2014, pp.23-27.*

[5] *S. Roy, R.Bose and D. sarddar, "A Fog-Based DSS Model for Driving Rule Violation Monitoring Framework on the Internet of Things", International Journal of Advance Science and Technology, vol. 82,2015,pp.23-32.*

[6] *G.Li, W. Zhang and Y.Zhang, " A design of the IOT gateway for Agricultural Greenhouse", Sensors and Transducers, Vol 172, issue 6, June 2014, pp.75-80.*

[7] *B.M Lee, J. Quyang, "Intelligent Healthcare Service by using Collaborations between IoT Personal Health Devices", International Journal of Bio-Science and Bio-Technology, Vol.6, 2014, pp.155-164.*

[8] *C.S.Ryu, " IOT Based Intelligent for Fire Emergency Response Systems", International Journal of Smart Home, Vol. 9 , Issue 3, 2015, pp.161-168.*

[9] *C.M. Shah, V.B. Sangoi and R.M. Vishoria, " Smart Security Solutions Based on Internet of Things (IOT)", International Journal of Current Engineering and Technology, Vol 4, Issue 5, oct 2014, pp.3401-3404.*

[10] *Y.Sun, "Research on the Railroad Bridge Monitoring Platform Based on the Internet of Things", International Journal of Control and Automation, vol. 7, issue 1, 2014, pp.401- 408.*

[11] *Mr. R. Balasubramaniam, R.Sathya, S.Aschika and S.Senthilkumar, "An Analysis Of Rfid Authentication Schemes For Internet Of Things (Iot) In Healthcare Environment Using Elgamal Elliptic Curve Cryptosystem", ISSN: 2455-1457,International journal of recent trends in engineering and research, vol 2, issue 3, march 2016, pp.241-247.*

[12] *J.Jaykumar and A.Blessy, " Secure Smart Environment using IOT Based On RFID", ISSN: 0975-9646, International Journal of Computer Science and Information Technologies, vol 5,issue 2, 2014, pp.2493-2496.*

[13] *L. Meng, Q.Feng, P Liu and E.Ding, " Research on Key Technologies of Coal Mine Groundwater Perception Based on IOT", ISBN 978-7-5646-2437-8, An Interdisciplinary Response to Mine Water Challenges - Sui, Sun & Wang (eds) China University of Mining and Technology Press, Xuzhou, 2014, pp.437-440.*

[14] *P.Elanthiraiyan and Dr. S.Babu, "Smart Medicine and Physical Health System using IOT", ISSN:2320-088X, International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 3, March 2015, pp.333-338.*

Table 5 Summary of the Literature Review

No	Paper	Technology Used	Characteristics	Applications
1	[2]	Fibre Optical Sensor Technology and IOT Framework Technology.	Remote Transmission, multiparameter, multiplexing capability, ease of networking, real time online, interference, intrinsic safety	Mine Safety Based on Fibre Optical IOT, energy, healthcare, aerospace, chemicals, environment etc.
2	[3]	RFID, Zigbee, GPRS used to recognize e-mark on the vegetables.	Vegetable Traceability system/expensive equipment cost, more power consumption, require high technical requirements and poor security	Planting, environment monitoring, logistics, Product Processing, storage and distribution
3	[4]	Three Middleware Approach is used named as Triple Space Based Computing, UBIWARE and SOA Based Middleware	Interoperability, scalability, zero infrastructure, Spontaneous interaction, Multiplicity, context detection, security and privacy, device discovery and management, abstraction and managing large volumes of data	Logistics, Transportation, Healthcare, home and offices.
4	[5]	Fog Based Intelligent Decision Support System	Mobility Support, Location Awareness, Low Latency	Driving Rule Violation Monitoring
5	[6]	Multiple Access Methods like Wi-Fi, LAN, 3G, GPRS and So on, STM32 as the embedded OS	Compatible, Extendible and Reliable	Greenhouse monitoring system, fine planting, remote intelligent monitoring and farming scientific planting crops
6	[7]	Collaboration Protocol, Intellectualized Service Application Algorithm, WSN	Maintain mutually autonomous Collaboration systems, minimize human intervention, network access management, power management and security Management	Manage Metabolic Syndrome
7	[8]	Detection Sensors, WSN, Egress Capacity,	Compatible, Extendible and Reliable	Fire Emergency Response Systems in Buildings disasters
8	[9]	RFID Reader, TM4C123GXL-based on ARM Cortex-M4, Machine Learning Algorithms, Biometric Sensor, MCU, Wi-Fi Module, Relay Driven Electromagnetic locks,	Machine learning can be implemented by making system smarter, more security, used in college, energy efficiency /schools to take attendance/ difficult open the door in the absence of Wi-Fi connectivity	Door Opening, taking attendance, secure environment
9	[10]	Satellite Positioning, Information Collection Based WSN, Daily Transmission, Early Warning Data Processing	Large Range, Short Detention, Strong Real time and Synchronous Measurement.	Real Time Monitoring of Railroad bridge Safety
10	[11]	Elliptic Curve Cryptography, Elgamal Elliptic curve Cryptography, RFID	Efficient, accurate and economic in terms of performance and security.	Healthcare Area, smart city, smart grid, smart homes, intelligent transportation, portable devices, e-commerce, chip cards and smart energy management systems
11	[12]	RFID, middleware system, internet system, proposed Kill password and access password to provide data authentication, confidentiality and integrity.	Easy and Secure to use/ identify security and privacy threats	Healthcare construction, hospitality to transportation sector and so on.
12	[13]	Networked Smart Sensor, Distributed Monitoring network on surface and underground, data mining and thematic application system based on cloud computing, three	Decision making, quick response	Coal Mine Ground Water Perception

[15] X.Xu, "IOT Technology Research in E-commerce", ISSN: 1812-5638, Information Technology Journal, Volume 13, Issue 16, 2014, pp.2552-2559.
[16] J.Kadlec, R.Kuchta, R.Novotny and O.Cozik, "RFID Modular System for the Internet of Things(IOT)",ISSN: 2169-0316, Industrial Engineering and Management an open Access Journal, Vol 3, Issue 4, 2014,pp.1-7.
[17] P. Vlacheas, R.Giaffreda et. al, "Enabling Smart Cities through a Cognitive Management Framework for the Internet of Things", ISSN: 0163-6804, IEEE Communications Magazine, 2013, pp.102-111.
[18] J. Gubbi, R. Buyya,S.Marusic and M. Paliniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", www.buyya.com, pp.1-19.
[19] V.sharma and R.Tiwari, "A review paper on "IOT" &It¨s Smart Applications", ISSN: 2278-7798, International Journal of Science, engineering and Technology Research, Vol 5, issue 2, Feb 2016, pp.472-476.
[20] A.Bali and S.N Singh, " A Review on the Network Security Related to Wireless Sensor Network", ISSN: 2277 128X,IJARCSSE, Vol. 5, Issue 3, Mar 2015,pp.778-784.

Cluster Based Data Aggregation and Authentication Protocol for WSN

Ms. D. Vijayakumari*, Ms. Dhivya Kesavan*
* Assistant Professor, RMK College of Engineering and Technology,
RSM Nagar, Puduvoya - 601 206.

ABSTRACT

In wireless sensor network the information collected by sensor nodes should be aggregated and communicated without any false data. However Compromised sensor nodes are capable of injecting false data during both data aggregation and data forwarding. An Enhanced cluster based data aggregation and authentication protocol called DAA is proposed, to integrate false detection with data aggregation and confidentiality. In this protocol to perform data aggregation along with false data detection, the monitoring nodes of every data aggregator also conduct data aggregation and compute the corresponding small size message authentication codes for data verification at their pair mates. Cluster based approach is employed to select data aggregator. The data integrity on encrypted data rather than the plain data is verified to support confidential data transmission. Performance analysis shows that DAA detects any false data injected by up to T compromised nodes, and that the detected false data are not forwarded beyond the next data aggregator on the path. It is also considered that enabling every sensor node to be capable of both aggregating and forwarding data in order to improve network security and efficiency.

Keywords— Data aggregation, data integrity, network-level security, sensor networks, false detection.

I. INTRODUCTION

Wireless sensor networks (WSNs) open up new application areas such as tactical surveillance, intelligent environmental and structural monitoring and target tracking. In a WSN, large numbers of tiny nodes may be deployed in an ad hoc manner. These nodes automatically configure a topology by communicating and coordinating with each other. Nodes assume the roles of both sensing device and router. Messages are relayed to other nodes or to a hub in a multi hop fashion. Multi-hop routing in an energy-constrained WSN has been shown to give rise to significant gains in network performance. With more nodes, the area being monitored can be increased or with the same area, the increase in node density gives more precise and timely data and also provides a degree of operational reliability. In wireless sensor networks it is important to save energy so that the batteries of the sensor nodes last for a long time. This means that computations and communications should be kept at a minimum so that the nodes can sleep as often as possible. On the other hand there is a demand for security which increases the number of clock cycles used for computations and the number of bits sent over communication channels.

II. RELATED WORK

False data injections, data authentication schemes that employ multiple MACs are proposed based on the observations of data integrity. The statistical en-route detection scheme, called SEF, enables relaying nodes and base station to detect false data with a certain probability. In 10 hops, SEF is able to drop 80%–90% of the injected false reports. In the interleaved hop-by- hop authentication scheme, any packet containing false data injected by compromised sensor nodes is detected by those sensor nodes that collaborate to verify data integrity. In the interleaved hop-by-hop authentication scheme, sensor nodes are not allowed to perform data aggregation during data forwarding. The Commutative Cipher based En-route Filtering scheme (CCEF) drops false data en-route without symmetric key sharing[5][6]. Secure data aggregation problem is studied extensively. In [1] the security mechanism detects node misbehaviors such as dropping or forging messages and transmitting false data. Random sampling mechanisms and interactive proofs are used to check the correctness of the aggregated data at base station[2][3]. Several key establishment protocols are developed for sensor networks, whichoffer ―direct key establishment‖ for neighboring nodes and ―path key establishment‖[4] for sensor nodes that are multiple hops away from each other. In path key establishment method, to establish a pairwise key with node, a sensor node needs to find a path between itself and node such that any two adjacent nodes in that path can establish a pair wise key directly.

III. PROBLEM DEFINITION

Power-controlled networks have nodes with variable RF power transceivers that provide greater routing performance at the expense of higher power consumption and costs Fixed-power networks have cheaper motes with fixed-power RF transceivers but may be more prone to communication disruptions. Several routing protocols in fixed-power, multi hop WSNs use shortest-path routing. Since operation is often over long unattended periods, the protocol must be energy efficient. As such, routing protocols must ensure that the WSN can reconfigure, be energy efficient and resilient to failures. These non-trivial requirements pose conflicting demands on protocol design.

A. False Detection and Authentication

Data confidentiality prefers data to be encrypted at the source node and decrypted at the destination. However, data aggregation techniques usually require any encrypted sensor data to be decrypted at data aggregators for aggregation. The existing false data detection algorithms address neither data aggregation nor confidentiality. Although they could be modified easily to support data confidentiality, it is a challenge for them to support the data aggregation that alters data. For instance, the basic idea behind the false data detection algorithm in is to form pairs of sensor nodes such that one pairmate computes a message authentication code (MAC) of forwarded data and the other pairmate later verifies the data using the MAC, as illustrated in Fig. 1.

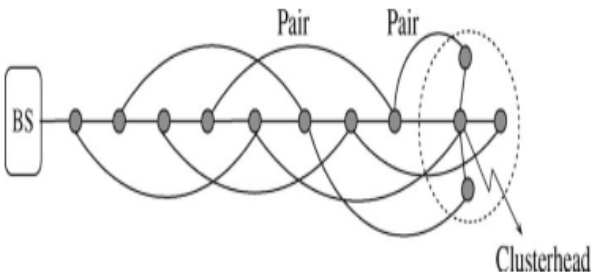


Fig. 1. An example of forming sensor pairs to authenticate data for the false data detection scheme in [3], where data aggregation is not allowed if it requires any change in the data. In this scheme, any data change between two pairmates is considered as false data injection, and therefore, data aggregation is not allowed if it requires alterations in the data. Hence, the false data detection algorithm cannot be implemented when a data aggregator between two pair mates changes the data.

IV. DATA AGGREGATION AND AUTHENTICATION PROTOCOL

This section presents the protocol DAA and its algorithms, namely MNS and SDFC, provides secure data aggregation, data confidentiality, and false data detection by performing data aggregation at data aggregators and their neighbouring nodes and verifying the aggregated data during data forwarding between two consecutive data aggregators. DAA has three steps that are explained in the following subsections.

Input: A Wireless sensor network with densely deployed sensor nodes, some of which are designated as data aggregators. For given valve of T, data aggregators are already selected in such a way that there exists at least T nodes between any two data aggregators.

Output: Even though the network can have up to T compromised nodes, data are aggregated in data aggregators.

Step-1: T neighbouring nodes of each data aggregator are randomly selected as monitoring nodes to perform the additional data aggregation and to compute sub MAC s of the aggregated.

Step-2: The following 2T+1 pair of nodes are formed by enabling the nodes of every pair to share a distinct symmetric key: (1) one pair is formed by the current and forward data aggregators, (2) T pairs are formed by the monitoring and forwarding nodes of the current data aggregator.

Srep-3: Each data aggregator and its selected T monitoring nodes aggregate data and then compute sub MACs. The aggregated data are encrypted by the current data aggregator. The data aggregator and its

monitoring nodes compute two sub MACs: one sub MAC for the encrypted aggregated data and another sub MAC for the plain aggregated data. The current data aggregator constructs two FMACs to forwarding nodes. The integrity of the encrypted data is verified by forwarding pair mates of the selected monitoring nodes of the current data aggregator. The integrity of the plain data is verified by some neighbouring nodes of the forward data aggregator. If the integrity verification of the encrypted or plain data fails at any sensor node, the data are dropped immediately.

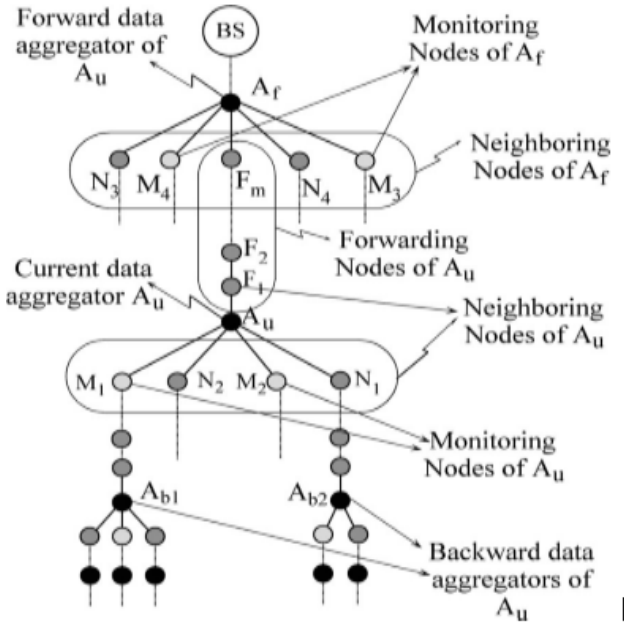


Fig. 2. The system architecture of sensor nodes used by DAA.

To support false data detection, secure data aggregation, and confidentiality against up to T compromised sensor nodes, DAA forms 2T+1 pairs of sensor nodes by the neighbouring and forwarding nodes of Au and Af.

A. Data aggregation

Data aggregation results in better bandwidth and battery utilization, which enhances the network lifetime because communication constitutes 70% of the total energy consumption of the network. This paper introduces a data aggregation and authentication protocol (DAA) to provide false data detection and secure data aggregation against up to T compromised sensor nodes, for T>1. The value of T depends on security requirements, node density, packet size, and the amount of tolerable overhead. We assume that some sensor nodes are selected dynamically as data aggregators, and the nodes between two consecutive data aggregators are called forwarding nodes simply because they forward data. To detect false data injected by a data aggregator while performing data aggregation, some neighbouring nodes of the data aggregator also perform data aggregation and compute MACs for the aggregated data to enable their pair mates to verify the data later. DAA also provides data confidentiality as data are forwarded

between data aggregators. To provide data confidentiality during data forwarding between every two consecutive data aggregators, the aggregated data are encrypted at data aggregators, and false data detection is performed over the encrypted data rather than the plain data. Whenever the verification of encrypted data fails at a forwarding node, the data are dropped immediately to minimize the waste of resources such as bandwidth and battery power due to false data injection.

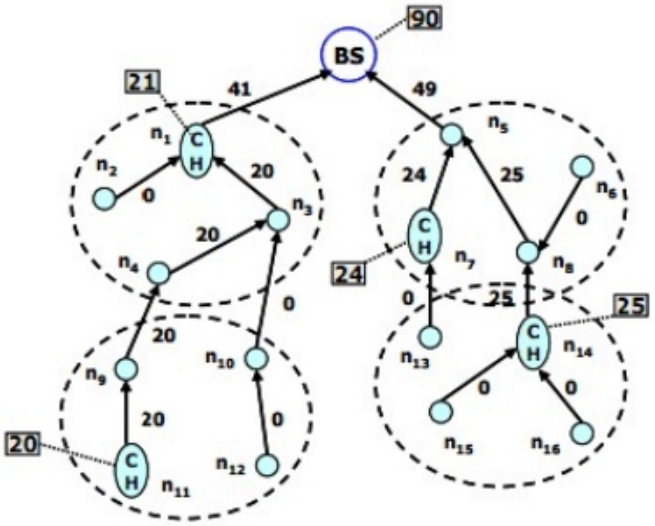


Fig.3 Aggregation of four cluster aggregates

B. Cluster based Approach for Data Aggregators

In cluster-based approach, whole network is divided in to several clusters. Each cluster has a cluster-head which is selected among cluster members. Cluster-heads do the role of aggregator which aggregate data received from cluster members locally and then transmit the result to sink. The advantages and disadvantages of the cluster-based approaches are very much similar to tree-based approaches form a direct link with cluster-head. Phase I of this scheme is similar to various scheme used for clustering but differ in one way that the cluster-head rotation is localized and is done based on the remaining energy level of the sensor nodes which minimize time variance of sensors and this lead to energy saving from unnecessary cluster-head rotation. In phase II, each node within the cluster searches for a neighbour closer than cluster-head which is called data relay point and setup up a data relay link. Now the sensor nodes within a cluster either use direct link or data relay link to send their data to cluster head which is an energy efficient scheme. The data relay point aggregates data at forwarding time to another data relay point or cluster-head.

V. MONITORING NODE SELECTION

Aggregator Au requests it's every neighbouring node to send two random numbers along with its node ID number. Each neighbouring node of Au generates two random numbers(Ra and Rb) using its key that it shares with Au. Ra, Rb and MAC(Ra|Rb) are sent to Au. When Au finishes receiving random numbers

and node IDs from nits neighbouring nodes, it labels them Ni in the receiving order of their random numbers. Then Au sorts all random numbers in ascending order and computes MAC using Kgroup. All such information are broadcasted by Au. Each Ni verifies the broadcast numbers by checking whether two random numbers that it sent earlier to Au match two of the random numbers that Au has broadcasted. If the verification is successful Ni encrypts the MAC Kgroup using the key it shares with Au and sends it to Au. Else Ni informs its neighbouring nodes and Au about it, along with a request of re-starting the monitoring node selection. To determine the indices of the T monitoring nodes, each Ni runs the following modulus function Ik. Any Ni whose index I happens to be equal to an Ik is selected as a monitoring node. If there is a duplicate Ik value, modulus function is run by increasing the K value by 1.

$$I_k = \left[\left(\sum_{j=k}^{n-1+k} R_j + K^u_{group} \right) mod(n) \right] + 1$$

SECURE DATA AGGREGATION AND FALSE DETECTION-INTEGRATION.

To provide data confidentiality, transmitted data are always encrypted and forwarding nodes perform the data verification over the encrypted data. Prior to this step of DAA, monitoring nodes of every data aggregator are selected, and 2T+1 pairs are formed. To verify data integrity and detect false data injections, one pair mate computes a sub MAC, and the other pair mate verifies the sub MAC. Sub Macs are computed for both plain and encrypted data. Sub Macs of plain data are used to detect false data injections during data aggregation, whereas subMACs of encrypted data are used to detect false data injections during data forwarding. To detect any false data that the current data aggregator can inject during data aggregation, the monitoring nodes of also aggregate the incoming data of and compute subMACs for the plain aggregated data, so that the forward data aggregator and its neighboring nodes verify the subMACs. Similarly, to detect those false data that can be injected during data forwarding, the monitoring nodes of compute subMACs for the encrypted aggregated data and then their pairmates of forwarding nodes verify the subMACs. Main steps of SDFC are: 1) whenever some data are received by a data aggregator, the authenticity of data is verified by the data aggregator and its neighboring nodes; 2) the data aggregator and its monitoring nodes aggregate the data independently of each other; 3) each monitoring node computes one subMAC for the encrypted data and the other subMAC for the plain data; 4) the data aggregator collects these subMACs from its monitoring nodes to form the FMACs of the encrypted and plain data, appends the FMACs to the encrypted data, and transmits them; 5) the forwarding nodes verify the data integrity of the encrypted data; and finally 6) the neighboring nodes of the next aggregator verify the integrity of the plain data. In Algorithm SDFC, each data aggregator forms two FMACs: one FMAC for the encrypted data, and the other FMAC for the plain data. Each FMAC consists of T+1 subMACs computed by the data aggregator and its T monitoring nodes. The FMACs of encrypted and plain data are forwarded along with the encrypted data. In the formation of FMACs, data aggregator determines the order of subMACs in anyway and informs each forwarding node about its subMAC location individually.

VI. PERFORMANCE EVALUATION

Integration of False detection and data aggregation providing confidentiality results in improvising network security. The quality of the data obtained is better vivid through the performance analysis iv various parameters such as packet delivery ratio, End-End latency, Energy Consumption, Throughput.

Packet delivery ratio (PDR): It measures the percentage of data packets generated by nodes that are successfully delivered, expressed as

$$\frac{\text{TOTAL NUMBER OF PACKETS SUCCESFULLY DELIVERED}}{\text{TOTAL NUMBER OF PACKETS SENT}} X100\%$$

End-End latency: It measures the average time it takes to route a data packet from the source node to the hub it is expressed as

$$\frac{\sum \text{INDIVIDUAL DATA PACKET LATENCY}}{\text{TOTAL NUMBER OF PACKETS DELIVERED}}$$

Energy consumption: It measures the energy expended per delivered data packet. It is expressed as

$$\frac{\sum ENERGY\ EXPENDED\ BY\ EACH\ NODE}{TOTAL\ NUMBER\ OF\ PACKETS\ DELIVERED}$$

Throughput: It is defined as the number of packed at destination side at a particular time.

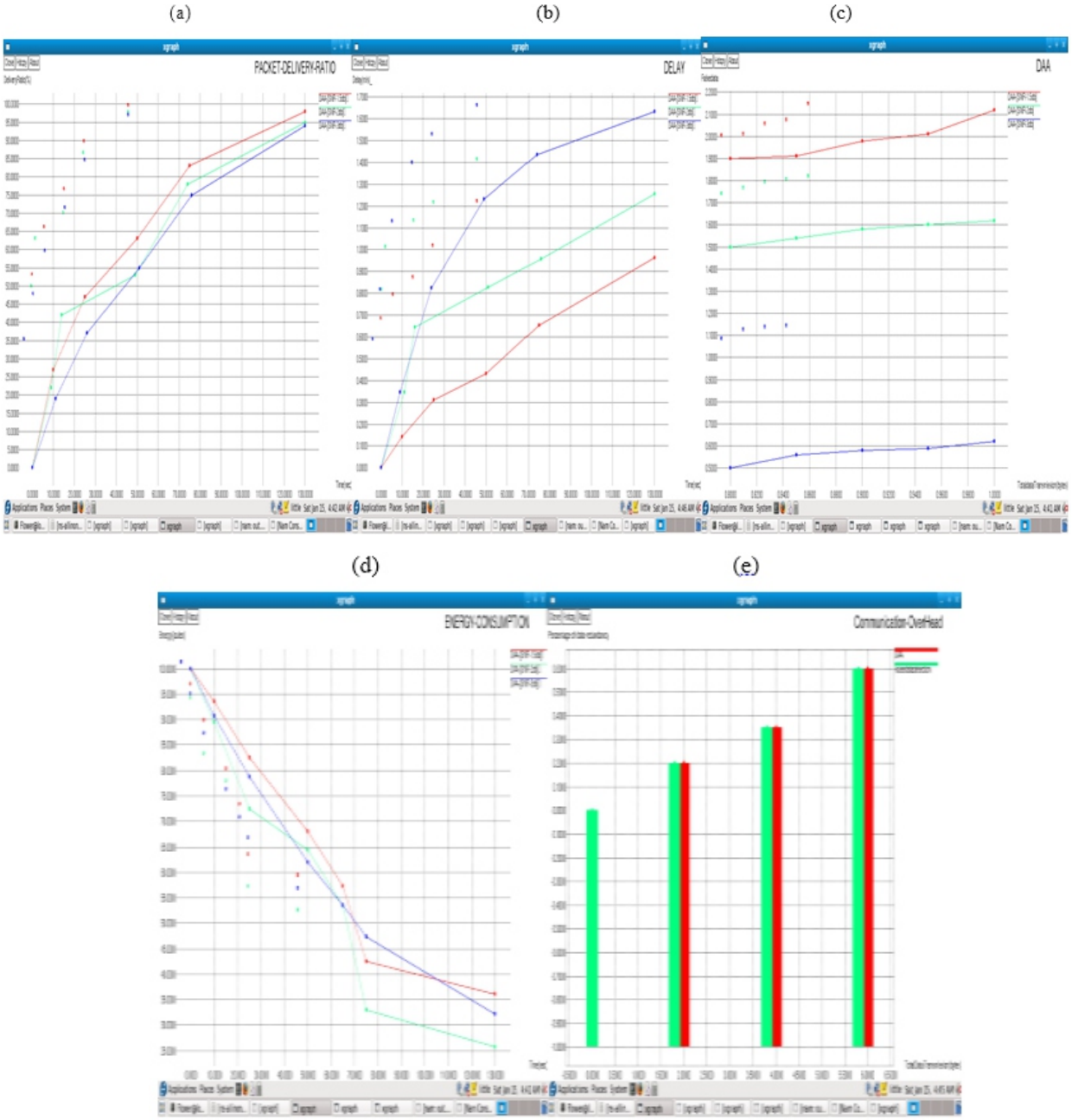
$$\frac{NUMBER\ OF\ PACKET\ RECEIVED}{TIME\ (Sec)}$$

VII. CONCLUSION

Data integrity distorted by compromised sensor nodes is prevented through the security protocol which detects false data during both data forwarding and in data aggregation, improving the network security and quality of received data. Significant Bandwidth utilization, Energy consumption, and improved data accuracy is achieved. Cluster based approach employed in selection of data aggregators adds with reducing end to end delivery. As for the future research, we consider of enabling every sensor node to be capable of both aggregating and forwarding data simultaneously in order to improve network security and efficiency.

Fig.4 Performance Analysis

(a) Packet delivery ratio, (b) Delay, (c) DAA compared with different S/N ratio, (d) Energy Consumption, (e) Communication overhead-Data aggregation Vs transmitted bytes



REFERENCES

[1] K. Wu, D. Dreef, B. Sun, and Y. Xiao, —Secure data aggregation without persistent cryptographic operations in wireless sensor networks,‖ Ad Hoc Netw., vol. 5, 2007, pp. 100–111.

[2] R. Rajagopalan and P. K. Varshney, —Data aggregation techniques in sensor networks: A survey,‖ IEEE Commun. Surveys Tutorials, vol. 8, no. 4, 4th Quarter 2006.

[3] H.Çam, S.Ozdemir, P.D.Muthuavinashiappan, and H. O. Sanli, —Energy-efficient and secure pattern based data aggregation for wireless sensor networks,‖ Comput. Commun., vol. 29, no. 4, pp. 446– 455, Feb. 2006.

[4] D. Liu, P. Ning, and R. Li, —Establishing pairwise keys in distributed sensor networks,‖ ACM Trans. Inf. Syst. Security, vol. 8, no. 1, pp. 41–77, Feb. 2005.

[5] S. Xu, —On the security of group communication schemes based on Symmetric key cryptosystems,‖ in Proc. ACM Workshop Security Ad hoc Sensor Netw., 2005, pp. 22–31.

[6] P. Gauravaram, W. Millan, J. G. Nieto, and E. Dawson, —3C—A provably Secure pseudorandom function and message authentication code: A new mode of operation for cryptographic hash functions,‖ Cryptology ePrint archive, Rep., 2005.

[7] C. Karlof, N. Sastry, and D. Wagner, —TinySec: A link layer security architecture for wireless sensor networks,‖ in Proc. 2nd ACM Conf. Embedded Netw. Sensor Syst., 2004, pp. 162–175,

[8] D. Seetharam and S. Rhee, —An efficient pseudo random number generator for low-power sensor networks,‖ in Proc. 29th Annu. IEEE Int.Conf. Local Comput. Netw., 2004, pp. 560–562.

[9] F. Ye, H. Luo, S. Lu, and L. Zhang, —Statistical en-route detection and filtering of injected false data in sensor networks,‖ in Proc. IEEE INFOCOM, 2004, vol. 4, pp. 2446–2457.

[10] H. Yang and S. Lu, —Commutative cipher based en- route filtering In wireless sensor networks,‖ in Proc. IEEE VTC, 2004, vol. 2, pp. 1223–1227.

[11] W. Du, J. Deng, Y. S. Han, and P. K.Varshney, —A witness-based approach for data fusion assurance in wireless sensor networks,‖ in Proc. IEEE GLOBECOM, 2003, pp. 1435–1439.

[12] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, —A pairwise key predistribution scheme for wireless sensor networks,‖ in Proc. 10th ACM CCS, 2003, pp. 42–51.

[13] L. Hu and D.Evans, —Secure aggregation for wireless networks,‖ in Proc. Workshop Security Assurance Ad hoc Netw., Orlando, FL, Jan. 28, 2003, pp. 384–394.

A Survey of Routing Protocol in VANET with its Pros and Cons

Patel Pragnesh V*
* Student Master in Information Technology,
PIET, Waghodia, Baroda

ABSTRACT

VANET are a special form of wireless networks made by vehicles communicating among themselves on roads. VANET has opened door to develop several new applications like, traffic engineering, traffic management, dissemination of emergency information to avoid hazardous situations and other user applications. VANETs are direct offshoot of Mobile Ad hoc Networks (MANETs) but with distinguishing characteristics like, movement at high speeds, in-sufficient storage and processing power, unpredictable node density and short link lifetime. The conventional routing protocols proposed for mobile ad hoc networks (MANETs) work poorly in VANETs. As communication links break more frequently in VANETs than in MANETs, the routing reliability of such highly dynamic networks needs to be paid special attention.

1. INTRODUCTION

Vehicular Ad Hoc Network (VANET) is a new challenging network environment that pursues the concept of ubiquitous computing for future. They are a special form of mobile ad hoc networks (MANETs) that provide vehicle-to vehicle communications. It can be thought as each vehicle is equipped with a wireless communication facility to provide ad hoc network connectivity. VANETs tend to operate without an infrastructure; each vehicle in the network can send, receive, and relay messages to other vehicles in the network. This way, vehicles can exchange real-time information, and drivers can be informed about road traffic conditions and other travel-related information. VANETs have unique and fascinating features, different from other types of MANETs, such as normally higher computational capability, higher transmission power, and some kind of predictable mobility, with comparison with general MANETs. VANETs bring lots of possibilities for new range of applications which will not only make the travel safer but faster as well. Reaching to a destination or getting help would be much easier. The concept of VANETs is quite simple by incorporating the wireless communication and data sharing capabilities, the vehicles can be turned into a network providing similar services like the ones with which we are used to in our offices or homes. For the wide spread and ubiquitous use of VANETs, a number of technical challenges exist. Besides, VANETs are also similar to MANETs in many ways. For example, both networks are multi-hop mobile networks having dynamic topology. Both VANET and MANET are rapidly deployable, without intense of an infrastructure. Although, MANET and VANET, both are mobile networks, however, the mobility pattern of VANET nodes is such that they move on specific paths (roads) and hence not in random direction. This gives VANETs some advantage over

MANETs as the mobility pattern of VANET nodes is predictable. MANETs are often characterized by limited storage capacity and low battery and processing power. VANETs, on the other hand, do not have such limitations.

2. CHARACTERISTICS & APPLICATION OF VANET

VANETs comprise of radio-enabled vehicles which act as mobile nodes as well as routers for other nodes. In addition to the similarities to ad hoc networks, such as short radio transmission range, self-organization and self management, and low bandwidth, VANETs can be distinguished from other kinds of ad hoc networks as follows:

[i] Highly Dynamic Topology:

Due to high speed of movement between vehicles, the topology of VANETs is always changing. For example, assume that the wireless transmission range of each vehicle is 100 m, if the distance between them is less than 200 m, there can be a link between two cars. In the worst case, if two cars with the speed of 60 mph (25 m/sec) are driving in opposite directions, the link will last only for at most 10 sec.

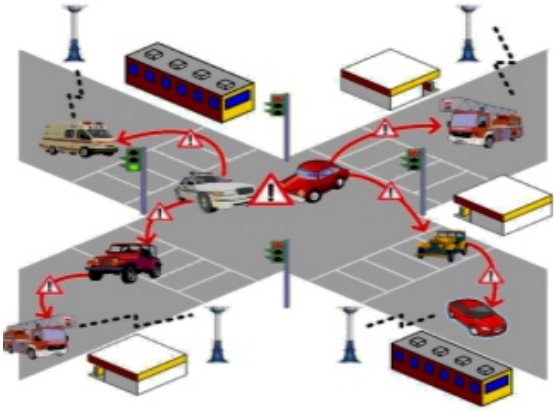


Figure 2.1 Example of a VANET

[i] Frequently Disconnected Network:

Due to the some reason, the connectivity of the VANETs could also be changed frequently. Especially when the vehicle density is low, it has higher probability that the network is disconnected. In some applications, such as ubiquitous Internet access, the problem needs to be solved. However, one possible solution is to pre-deploy several relay nodes or access points along the road to keep the connectivity.

[ii] Sufficient Energy and Storage:

A common characteristic of nodes in VANETs is that nodes have ample energy and computing power (including both storage and processing), since nodes are cars instead of small handheld devices.

[iii] Geographical Type of Communication:

Compared to other networks that use unicast or multicast where the communication end points are defined by ID or group ID, the VANETs often have a new type of communication whichaddresses geographical areas where packets need to be forwarded (e.g., in safety driving applications).

[iv] Mobility Modelling and Predication:

Due to highly mobile node movement and dynamic topology, mobility model and predication play an important role in network protocol design for VANETs. Moreover, vehicular nodes are usually constrained by prebuilt highways, roads and streets, so given the speed and the street map, the future position of the vehicle can be predicated.

[v] Various Communications Environments:

VANETs are usually operated in two typical communications environments. In highway traffic scenarios, the environment is relatively simple and straightforward (e.g., constrained one- dimensional movement); while in city conditions it becomes much more complex. The streets in a city are often separated by buildings, trees and other obstacles. Therefore, there isn't always a direct line of communications in the direction of intended data communication.

[vi] Hard Delay Constraints:

In some VANETs applications, the network does not require high data rates but has hard delay constraints. For example, in an automatic highway system, when brake event happens, the message should be transferred and arrived in a certain time to avoid car crash. In this kind of applications, instead of average delay, the maximum delay will be crucial.

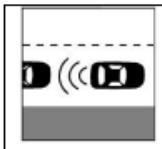
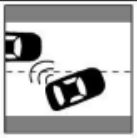
[vii] Interaction with On-Board Sensors:

It is assumed that the nodes are equipped with on-board sensors to provide information which can be used to form communication links and for routing purposes. For example, GPS receivers are increasingly becoming common in cars which help to provide location information for routing purposes. It is assumed that the nodes are equipped with on-board sensors to provide information which can be used to form communication links and for routing purposes.

Applications of VANET

The characteristics of Vehicular networks advance the development of striking and challenging services and applications as under.

- Vehicle collision & Lane change warning
- Intersection collision warning
- Approaching Emergency vehicle
- Rollover & Work zone warning
- Electronic Toll collection
- Inter Vehicle Communication

		
Co-operative Collision Warning	Intersection Collision Warning	Lane Change Warning
		
Approaching Emergency vehicle	Work Zone Warning	Rollover Warning
		
Coupling/De coupling	Inter-Vehicle Communication	Electronic Toll Collection

3. ROUTING PROTOCOLS

Routing Protocol can be classified into 2 classes

- TRANSMISSION STRATEGIES
- ROUTING INFORMATION

TRANSMISSION STRATEGIES

Delivery of information from a source to a destination can be classified into four types:

- UNICAST
- BROADCAST
- MULTICAST
- GEOCAST

However the multicast and geocast can be merged in one class because geocast usually is a special type of multicast transmission.

ROUTING INFORMATION

This class has been divided into two subclasses:

- Topology-Based
- Position-Based Routing Protocols.

In topology-based routing, each node should be aware of the network layout, also should able to forward packets using information about available nodes and links in the network. In contrast, position-based routing should be aware of the nodes locations in the packet forwarding.

Topology-Based Routing Protocol

Topology-based routing protocol usually a traditional MANET routing protocol, it uses link's information which stored in the routing table as a basis to forward packets from source node to destination; it commonly categorized into three categories (base on underlying architecture)

- PROACTIVE (PERIODIC)
- REACTIVE (ON-DEMAND)
- HYBRID

Proactive Routing Protocols

Proactive protocols allow access to a network node to use the routing table in order to store routes information for all other nodes, where each entry in the table contains the next hop node used in the path from source to the destination, without considering whether the route is actually useful or not. The table must be updated frequently to reflect the network topology changes, and should be broadcast periodically to the neighbours. This scheme may cause more overhead especially in the high mobility network. However, routes to destinations will always be available when needed. Proactive protocols usually depend on shortest path algorithms to determine which route will be chosen; they generally use two routing strategies: Link state strategy and distance vector strategy.

Pros

- No Route Discovery is required.
- Latency for real time applications is low.

Cons

- Unused paths occupy a significant part of the available bandwidth. never updated.

Reactive Routing Protocols

Reactive routing protocols (also called on-demand) reduce the network overhead; by maintaining routes only when needed, that the source node starts a route discovery process, if it needs a non existing route to a destination, it does this process by flooding the network by a route request message. When the message reaches the destination node (or to node which has a route to destination), this node will send a route reply message back to the source node using unicast communication method. Reactive routing protocols are applicable to the large size of the mobile ad hoc networks which are highly mobility and frequent topology changes. Many reactive routing protocols have been developed, the following sections will illustrate characteristic of some reactive protocols, as well as illustrates the existing enhancement protocols. Reactive routing protocols also suffer from the initial latency incurred in the route discovery process, which potentially makes them unsuitable for safety applications. AODV, DSR are the examples of reactive routing protocols whereas OLSR, TBRPF and FSR are the examples of proactive routing protocols.

Pros

-To update routing table not require periodic flooding the network. Flooding requires when it is demanded.

-Beaconless so it saves the bandwidth.

Cons

- For route finding latency is high.
- Excessive flooding of the network causes disruption of nodes communication.

4. PROACTIVE (TABLE-DRIVEN)

Proactive routing protocols are mostly based on shortest path algorithms. They keep information of all connected nodes in form of tables because these protocols are table based. Furthermore, these tables are also shared with their neighbours. Whenever any change occurs in network topology, every node updates its routing table.

Pros

- No Route Discovery is required.
- Low Latency for real time applications.

Cons

- Unused paths occupy a significant part of the available bandwidth.

4.1 Fisheye State Routing

FSR [8] is a proactive or table driven routing protocol where the information of every node collects from the neighbouring nodes. Then calculate the routing table. It is based on the link state routing & an improvement of Global State Routing.

Pros

- FSR reduces significantly the consumed bandwidth as it exchanges partial routing update information with neighbours only.
- Reduce routing overhead.
- Changing in the routing table will not occur even if there is any link failure because it doesn't trigger any control message for link failure.

Cons

-Very poor performance in small ad hoc networks.

-Less knowledge about distant nodes.

-The increase in network size the storage complexity and the processing overhead of routing table also increase.

- Insufficient information for route establishing.

4.2 Reactive (On Demand)

Reactive routing protocol is called on demand routing because it starts route discovery when a node needs to communicate with another node thus it reduces network traffic.

Pros

-To update routing table not require periodic flooding the network. Flooding requires when it is demanded.

-Beaconless so it saves the bandwidth.

Cons

- For route finding latency is high.
- Excessive flooding of the network causes disruption of nodes communication.

4.2.1 AODV

Ad Hoc on Demand Distance Vector routing protocol [9] is a reactive routing protocol which establish a route when a node requires sending data packets. It has the ability of unicast & multicast routing. It uses a destination sequence number

(DestSeqNum) which makes it different from other on demand routing protocols.

Pros

- An up-to-date path to the destination because of using destination sequence number.
- It reduces excessive memory requirements and the route redundancy.
- AODV responses to the link failure in the network.
- It can be applied to large scale adhoc network.

Cons

-More time is needed for connection setup & initial communication to establish a route compared to other approaches.

-If intermediate nodes contain old entries it can lead inconsistency in the route.

-For a single route reply packet if there has multiple route reply packets this will lead to heavy control overhead.

- Because of periodic beaconing it consume extra bandwidth.

4.2.2 Dynamic Source Routing

The Dynamic Source Routing (DSR) protocol represented in [10] which utilize source routing & maintain active routes. It has two phases route discovery & route maintenance.

Pros

-Beacon less.

-To obtain route between nodes, it has small overload on the network. It uses caching which reduce load on the network for future route discovery.

-No periodical update is required in DSR.

Cons

-If there are too many nodes in the network the route information within the header will lead to byte overhead.

-Unnecessary flooding burden the network.

-In high mobility pattern it performs worse.

-Unable to repair broken links locally.

4.2.3 Temporally Ordered Routing Protocol (TORA)

Temporally Ordered Routing Protocol [11] is based on the link reversal algorithm that creates a direct acyclic graph towards the destination where source node acts as a root of the tree. In TORA packet is broadcasted by sending node, by receiving the packet neighbour nodes rebroadcast the packet based on the DAG if it is the sending node's downward link.

Pros

-It creates DAG (Direct acyclic graph) when necessary.

-Reduce network overhead because all intermediate nodes don't need to rebroadcast the message.

-Perform well in dense network.

Cons

-It is not used because DSR & AODV perform well than TORA.

-It is not scalable.

5. PROS & CONS OF GEOGRAPHIC ROUTING PROTOCOLS

Geographic routing is a routing that each node knows it's own & neighbour node geographic position by position determining services like GPS. It doesn't maintain any routing table or exchange any link state information with neighbor nodes.

Information from GPS device is used for routing decision.

Pros

- Route discovery & management is not required.

-Scalability.

-Suitable for high node mobility pattern.

Cons

-It requires position determining services.

-GPS device doesn't work in tunnel because satellite signal is absent there.

5.1 DTN

Delay Tolerant Network (DTN) uses carry & forward strategy to overcome frequent is connection of nodes in the network. In carry & forward strategy when a node can't contact with other nodes it stores the packet & forwarding is done based on some metric of nodes neighbours.

5.2 BEACON

Beacon means transmitting short hello message periodically. It exposes presence and position of a node. An entry will be removed from neighbour table of a receiving node if it fails to receive a beacon after a certain period of time from the corresponding node.

5.3 OVERLAY

Overlay is a network that every node is connected by virtual or logical links which is built on top of an existing network.

5.3.1 VADD (Vehicle-Assisted Data Delivery)

Vehicle-Assisted Data Delivery [12] is based on the idea of carry & forward approach by using predicable vehicle mobility. Among proposed VAAD protocols H-VAAD shows better performance.

Pros

-Comparing with GPSR (with buffer), epidemic routing and DSR, VADD performs high delivery ratio.
-It is suitable for multi-hop data delivery.

Cons

- Due to change of topology & traffic density it causes large delay.

5.3.2 Geographical Opportunistic Routing (GeOpps)

Geographical Opportunistic Routing (GeOpps) [13] protocol utilizes the navigation system suggested routes of vehicles for selecting the forwarding node which is closer to the destination. During this process if there is any node which has minimum arrival time the packet will be forwarded to that node.

Pros

-By comparing with the Location-Based Greedy routing and MoVe routing algorithm GeOpps has high delivery ratio.
-To find a vehicle which is driving towards near the destination GeOpps need few encounters.
- The delivery ratio of GeOpps rely on the mobility patterns & the road topology but not dependent on high density of vehicles.

Cons

-Privacy is an issue because navigation information is disclosed to the network.

5.3.3 Greedy Perimeter Stateless Routing (GPSR)

Greedy Perimeter Stateless Routing [14] selects a node which is closest to the final destination by using beacon. It uses greedy forwarding algorithm if it fails it uses perimeter forwarding for selecting a node through which a packet will travel.

Pros

-To forward the packet a node needs to remember only one hop neighbour location.

-Forwarding packet decisions are made dynamically.

Cons

-For high mobility characteristics of node, stale information of neighbour's position is often contained in the sending nodes neighbour table.

-Though the destination node is moving its information in the packet header of intermediate node is never updated.

5.3.4 Greedy Perimeter Coordinator Routing (GPCR)

Greedy Perimeter Coordinator Routing [17] is a position-based routing protocol uses greedy algorithms to forward packet based on a pre-selected path which has been designed to deal with the challenges of city scenarios. No global or external information like static map does not require in GPCR.

Pros

- Does not require any global or external information.

-For representing the planar graph it uses the underlying roads though it is based on the GPSR.

-It has no as usual a planarization problem like unidirectional links, planar sub-graphs & so on.

Cons

- Depends on junction nodes.

-There has a problem in the Junction detection approach in which first approach fails on curve road & second approach fails on a sparse road.

5.4 CAR (Connectivity-Aware Routing)

For city and/or highway environment Connectivity-Aware Routing (CAR) [19] is designed which uses AODV for path discovery and uses PGB for data dissemination mode. It uses guard concept to maintain the path.

Pros

-No digital map is required.

-It has no local maximum problem.

- CAR ensures to find the shortest connected path because CAR has higher packet delivery ratio than GPSR and GPSR+AGF.

Cons

-Unnecessary nodes can be selected as an anchor.

-It cannot adjust with different sub-path when traffic environment changes.

5.5 Greedy Traffic Aware Routing protocol (GyTAR)

Greedy Traffic Aware Routing protocol [23] gives a new concept of intersection-based routing protocol which aims to reduce the control message overhead & end-to-end delay with low packet loss.

Pros

- For high mobility topology changes rapidly and often occurring network fragmentation which is efficiently handle by GyTAR.

-Performance shows that throughput, delay and routing overhead are better than GSR.

Cons

- GyTAR depends on roadside units because it assumes that the number of cars in the road will be given from road side units.

-GyTAR cannot avoid void.

6. Conclusion

In this paper, we have investigated the pros and cons of different routing protocols for inter- vehicle communication in VANET. By studying different routing protocol in VANET we have seen that further performance evaluation is required to verify performance of a routing protocol with other routing protocols based on various traffic scenarios. Comparison can be done among the routing protocols in the Overlay and so on.

7. REFERENCES

[1] "Survey of Routing Protocols in Vehicular Ad Hoc Networks," Kevin C. Lee, Uichin Lee, Mario Gerla, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, IGI Global, Oct, 2009.

[2] Ericson, "Communication and Mobility by Cellular Advanced Radio", ComCar project, www.comcar.de, 2002.

[3] Prabhakar Rajan & Kamalkant Ahirwar, "Comparative Study Of Manet And Vanet Routing Protocols", Amity University, Noida (2011).
[4] W. Franz, H. Hartenstein, and M. Mauve, Eds., Inter- Vehicle-Communications Based on Ad Hoc Networking Principles-The Fleet Net Project. Karlshue, Germany: Universitatverlag Karlsuhe,November 2005.
[5] A. Festag, et. al., "NoW-Network on Wheels: Project Objectives,Technology and Achievements", Proceedings of 6th InternationalWorkshop on Intelligent Transportations (WIT), Hamburg, Germany,March 2008.
[6] Reichardt D., Miglietta M., Moretti L., Morsink P., and Schulz W.,"CarTALK 2000 – safe and comfortable driving based upon inter-vehicle-communication," in Proc. IEEE IV'02.
[7] Morris R., Jannotti J., Kaashoek F., Li J., Decouto D., "CarNet: A scalable ad hoc wireless network system," 9th ACM SIGOPS European Workshop, Kolding, Denmark, Sept. 2000.
[8] Pei, G., Gerla, M., and Chen, T.-W. (2000), "Fisheye State Routing: A Routing Scheme for Ad Hoc Wireless Networks," Proc. ICC 2000, New Orleans, LA, June 2000.
[9] Perkins, C.; Belding-Royer, E.; Das, S. (July 2003)"Ad hoc On-Demand Distance Vector (AODV) Routing".
[10] Johnson, D. B. and Maltz, D. A. (1996), "Dynamic Source Routing in Ad Hoc Wireless Networks," Mobile Computing, T. Imielinski and H. Korth, Eds., Ch. 5, Kluwer, 1996, pp. 153– 81.
[11] Park, V.D., Corson, M.S. (1997), "A highly adaptive distributed routing algorithm for mobile wireless networks," INFOCOM '97. Sixteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE , vol.3, no., pp.1405-1413 vol.3, 7- 12 Apr 1997.
[12] Zhao, J.; Cao, G. (2006), "VADD: Vehicle-Assisted Data Delivery in Vehicular Ad Hoc Networks," INFOCOM 2006. 25th IEEE International Confrence on Computer Communications. Proceedings , vol., no., pp.1- 12, April 2006.
[13] Leontiadis, I., Mascolo, C. (2007), "GeOpps: Geographical Opportunistic Routing for Vehicular Networks," World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a , vol., no., pp.1-6, 18-21 June 2007.
[14] Karp, B. and Kung, H. T (2000), "GPSR: greedy perimeter stateless routing for wireless networks." In Mobile Computing and Networking, pages 243-254, 2000.
[15] Naumov, V., Baumann, R., Gross, T. (2006), "An evaluation of Inter-Vehicle Ad Hoc Networks Based on Realistic Vehicular Traces," Proc. ACM MobiHoc'06 Conf., May, 2006.
[16] Schnaufer, S., Effelsberg, W. (2008), "Position-based unicast routing for city scenarios," World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a , vol., no., pp.1-8, 23-26 June 2008.
[17] Lochert, C., Mauve, M., F¨ussler, H., and Hartenstein, H., "Geographic routing in city scenarios," SIGMOBILE Mob. Comput. Commun. Rev., vol. 9, no. 1, pp. 69–72, 2005.
[18] Lee, K. C., Haerri, J., Lee, U., and Gerla, M. (2007), "Enhanced perimeter routing for geographic forwarding protocols in urban vehicular scenarios," Globecom Workshops, 2007 IEEE, pp. 1–10, 26-30 Nov. 2007.
[19] Naumov, V., Gross, T.R. (2007), "Connectivity-Aware Routing (CAR) in Vehicular Ad-hoc Networks," INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE , vol., no., pp.1919- 1927, 6-12 May, 2007.
[20] Jerbi, M., Senouci, S.-M., Meraihi, R., and Ghamri- Doudane, Y. (2007), "An improved vehicular ad hoc routing protocol for city environments," Communications, 2007. ICC '07. IEEE International Conference, pp. 3972–3979, 24-28 June 2007.
[21] Lochert, C., Hartenstein, H., Tian, J., Fussler, H., Hermann, D., Mauve, M. (2003), "A routing strategy for vehicular ad hoc networks in city environments," Intelligent Vehicles Symposium, 2003. Proceedings. IEEE , vol., no., pp. 156-161, 9-11 June 2003.
[22] Seet, B.-C., Liu, G., Lee, B.-S., Foh, C. H., Wong, K. J., Lee, .-K. (2004), "A-STAR: A Mobile Ad Hoc Routing Strategy for Metropolis Vehicular Communications." NETWORKING 2004, 989-999.
[23] Forderer, D (2005). "Street-Topology Based Routing." Master's thesis, University of Mannheim, May 2005.
[24] Lee, K., Le, M., Haerri J., and Gerla, M. (2008), "Louvre: Landmark overlays for urban vehicular routing environments," Proceedings of IEEE WiVeC, 2008.
[25] F¨ußler, H., Hannes, H., J¨org, W., Martin, M., Wolfgang, E. (2004), "Contention-Based Forwarding for Street Scenarios," Proceedings of the 1st InternationalWorkshop in Intelligent Transportation (WIT 2004), pages 155–160, Hamburg, Germany, March 2004.
[26] Lee, K.C.; Lee, U.; Gerla, M. (2009), "TO-GO: TOpology-assist geo-opportunistic routing in urban vehicular grids," Wireless On-Demand Network Systems and Services, 2009. WONS 2009. Sixth International Conference on , vol., no., pp.11-18, 2-4 Feb. 2009.

[27] Cheng, P.-C., Weng, J.-T., Tung, L.-C., Lee, K. C., Gerla M., and Härri J. (2008), "GeoDTN+NAV: A Hybrid Geographic and DTN Routing with Navigation Assistance in Urban Vehicular Networks," Proceedings of the 1st International Symposium on Vehicular Computing Systems (ISVCS'08), Dublin, Irland, July.

[26] Mahmoud Hashem Eiza and Qiang Ni, Senior Member, IEEE "An Evolving Graph-Based Reliable Routing Scheme for VANETs" May 2013

[27] Ehsan Mostajerani, Rafidah Md Noor2 and Hassan Keshavarz3 "A Novel Improved Neighbor Discovery Method for an Intelligent-AODV in Mobile Ad hoc Networks" International Conference of Information and Communication Technology (lCoICl) 2013

[28] S. Mohapatra, P. Kanungo "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator" International Conference on Communication Technology and System Design 2011

[29] Christos Liaskos, Graduate Student Member, IEEE, Andreas Xeros, Georgios I. Papadimitriou, Senior Member, IEEE, Marioslestas, Member, IEEE And Andreas Pitsillides, Senior Member, "Balancing Wireless Data Broadcasting And Information Hovering For Efficient Information Dissemination " IEEE (March 2012).

Wireless Model for Monitoring and Controlling Water Networks and Stations in Khartoum

Ibrahim Khider*, Mohamed Abdalla*, Khalid Hamid**
* Sudan university of science and technology
** University of science and technology

A B S T R A C T

In this study, monitor and control of tow pumps and ground tank in station and pipe line in network using Atmega16 microcontroller is activated Visual basic programming language (BASCOM AVR), at main point Mobile. At remote points Atmega 16, another external modem is required for asynchronous communication. Both sides can call each other to sent status information. With this system monitor and control of water pumping stations and motorize valve can be activated. The system name Monitoring and Controlling Unit (MCU).

Key Words: ULN2003, Atmega16, GSM Modem, MAX232, Relay, SMS, Pressure sensor, LCD, Pump.

I. INTRODUCTION

Monitor and control the water networks and stations for better water utilization in Khartoum State Water Corporation (KSWC) by design an electronic circuit in order to measure pressure, quantity and level water in stations and pressure water in networks using sensors, send the pressure information to the operation engineer through GSM, and control the water pumps and water motorized valves depending on water pressure information.

II. MONITOR AND CONTROL SYSTEM

Remotely the system allows the user to effectively monitor and control the appliances and equipments via the mobile phone set by sending commands in the form of SMS messages and receiving the appliances status. The main concept behind the project is receiving the sent SMS and processing it further as required to perform several operations. The type of the operation to be performed depends on the nature of the SMS sent. The principle in which the project is based is fairly simple. First, the sent SMS is stored and polled from the receiver mobile station and then the required control signal is generated and sent to the intermediate hardware that execution according to the command received in form of the sent message.

The application of this technique has more efficient, comfortable and reliable apply in Khartoum State Water Corporation (KSWC). The comfort of being able to take control and monitor of pumps in (Stations, Wells) and valves in networks one location for saves a lot of time, cost and effort.

III. WORKING PRINCIPLES OF SYSTEM

The main task of the system is data flow control between Mobile side (Operation Engineer) and microcontroller sides (Station - Well - Network) to arrived to best operation in KSWC (efficiency - quality - cost) and provide data sharing shown in Figure 1.

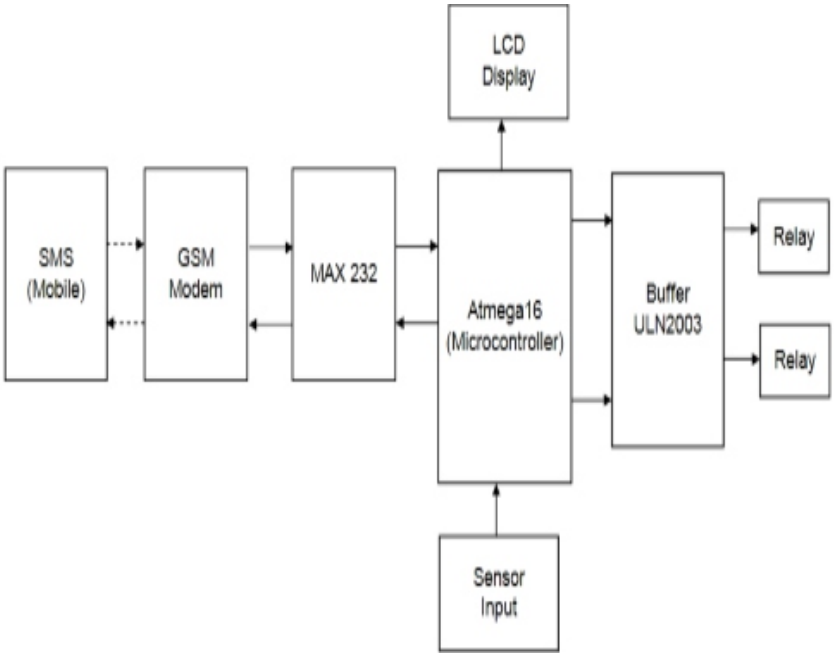


Figure 1: Block Diagram for system

The MCU in station read the (Pressure - Level) water by sensor (Pumps - Ground tank) then control in the operation pumps depending on the amount of values and send SMS to a central device every 1 minute (Pressure – Quantity – Level) water and display on LCD also. The MCU had two mode operation Auto mode and Manual mode, In Auto mode the MCU control pump automatic depend on value pressure outlet main pipe from station and level water in ground tank. In manual mode the operation engineer have control pump by send SMS for MCU (Open – Close) pump shown in Figure 2.

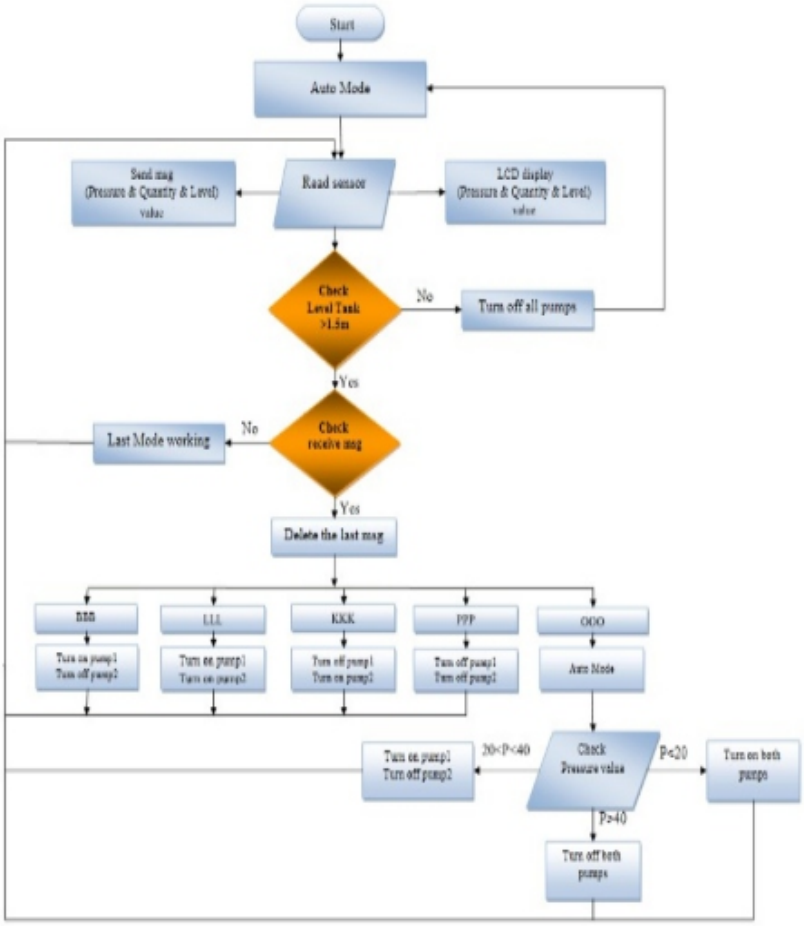


Figure 2 Flowchart system operation (station)

The MCU in network read the pressure water only by sensor then send SMS to a central device every 1 minute (or any time slot determine by operation engineer) contain pressure water and display on LCD also. The MCU had one mode controlling by operation engineer, can control motorize valve by send SMS for MCU (Open – Close) motorize valve shown in Figure 3.

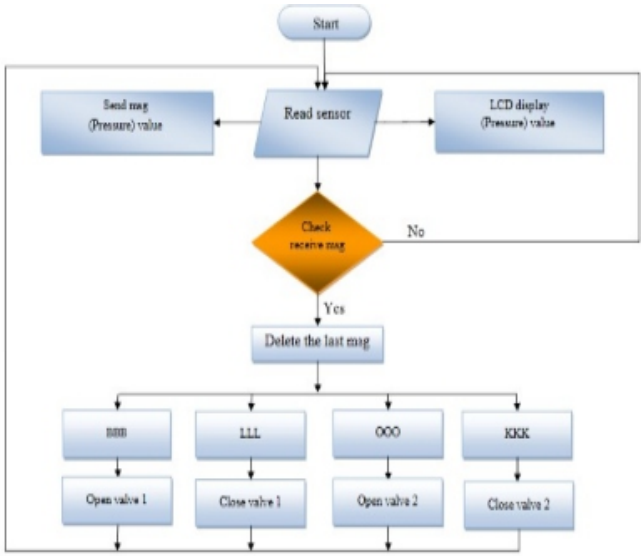


Figure 3 Flowchart system operation (Network)

III. TESTING AND RESULS

Started many test before assembly electronic circuit (MCU). First: known actual water pressure in networks and stations in Khartoum State Water Corporation (KSWC), Second: testing electronic circuit in simulation (Protues). Selected location testing devices (Logger) in the stations and network after knowing the areas of weakness and strength of the water by maintenance engineers in the State Water Corporation Khartoum, shown in Figure 4. Started the pressure tests period from April 2012 to September 2012, we had obtained the following location and results for Stations and Networks shown in Figure 5.

Figure 4 Testing devices (Logger)

Figure 5: Map showing the location and results in Khartoum area

Found some difference between MCU in station and Network (Design-function-contain SMS)

Station:

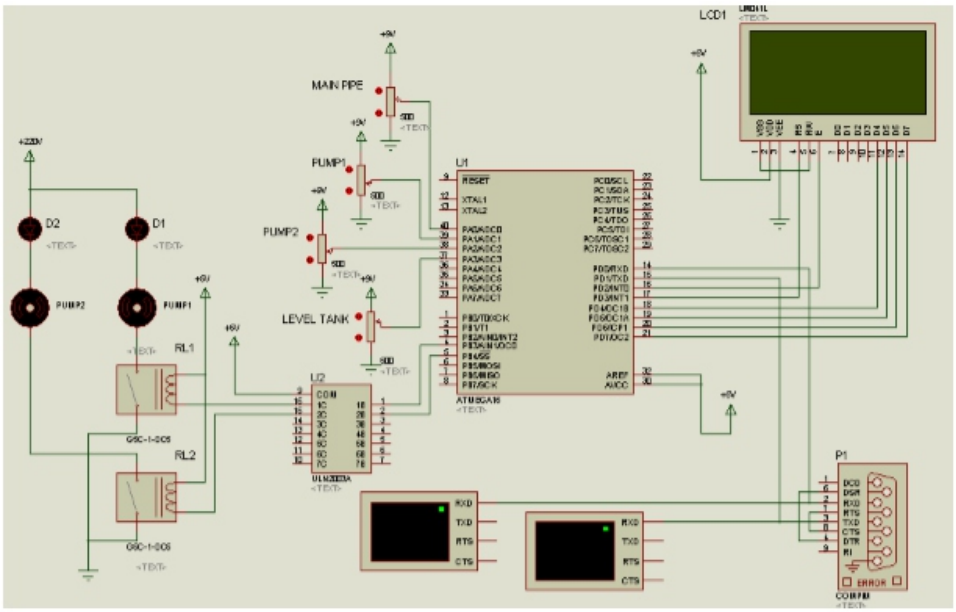


Figure 5 Circuit Diagram (Station)

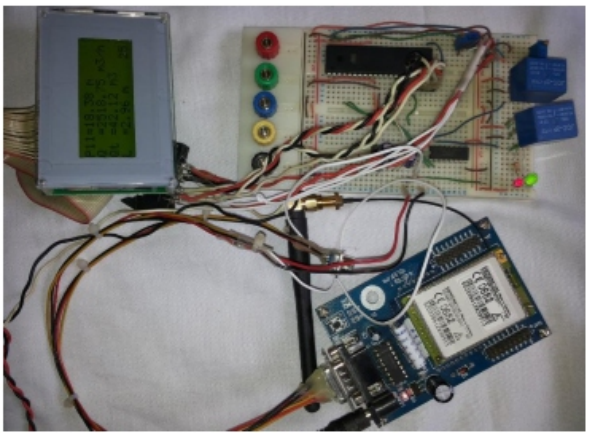


Figure 6 Electronic Circuit (Station)

Network:

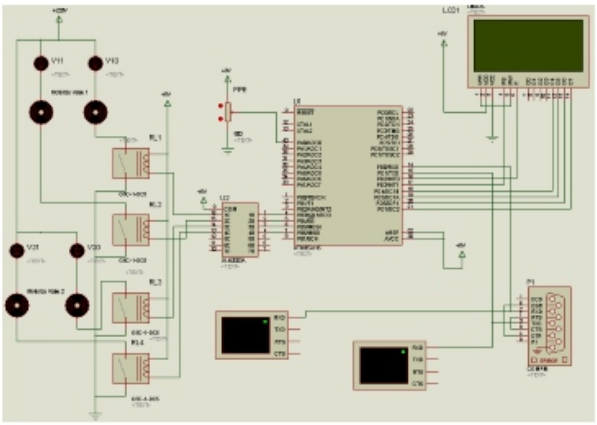


Figure 7 Circuit Diagram (Network)

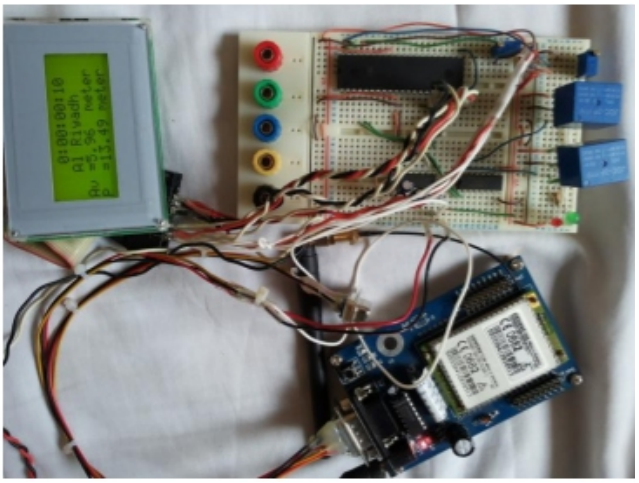


Figure 8 Electronic Circuit (Network)

Figure 9 Massage in Mobile

V. CONCULUSION

An attempt is made to integrate the two most widely used technologies namely Microcontroller and GSM for developing monitoring and controlling system. It is found that, it is possible to integrate microcontroller with GSM modem for reliable pressure and quantity water information and to ascertain the coverage area in Khartoum State Water Corporation (KSWC) for improve level service by low cost compare to wireless radio, PLC and SCADA.

REFERENCES

1. *Sensing and monitoring, Australian Communications and Media Authority © Commonwealth of Australia 2011.*
2. *Taylor & Francis Group, LLC, Wireless Sensors and Instruments © 2006.*
3. *Wireless framework for monitoring and controlling agricultural actions Editor International Journal of Machine Intelligence © 2, 2011*
4. *Wireless sensor network - Wikipedia, the free encyclopaedia, this page was last modified on 16 June 2012 at 02:32.*
5. *Modem - Wikipedia, the free encyclopaedia, this page was last modified on 16 June 2012.*
6. *GSM Based Control System © 5/3/2011.*
7. *GPRS Controlled System for Monitoring and Control of Well Sites 10th International Conference on DEVELOPMENT AND APPLICATION SYSTEMS, Suceava, Romania, © May 27-29, 2010*
8. *Development of real time digital controller for a liquid level system using Atmega32 microcontroller department of electrical engineering national institute of technology Rourkela © May 2011.*

The Dual Reciprocity Boundary Element Method and Numerical Solutions of One- Dimensional Transient Heat Transfer Problem

Walter Arthur Nondi*, Thomas Onyango,S. N. Muthiga*, N. B. Okelo*****

* Catholic University of Eastern Africa, Kenya.

** Technical University of Kenya, Kenya.

*** School of mathematics and actuarial science, Jaramogi Oginga Odinga University of Science and Technology

ABSTRACT

The dual-reciprocity boundary element method for the solution of a one-dimensional transient heat equation with a source term is considered. We give a numerical solution to this kind of heat equation. Discretization of heat equation using BEM and the solution of boundary integral equation is further discussed and results presented in graphs.

INTRODUCTION

We consider a one-dimensional heat conduction equation which models an unsteady temperature distribution in a solid (domain Ω). This problem is governed by the differential equation

$$k\nabla^2 T(x,t) + Q(x,t) = \rho c \frac{\partial T(x,t)}{\partial t} \quad \text{.....(3.46)}$$

where $Q(x,t)$ is the source term.

with the Neumann boundary conditions;

$$q(x,t) = \bar{q}(x,t) \qquad x \in \Gamma_q \quad \text{.....(3.47)}$$

And the initial condition

$$T(x,0) = T_0 \qquad T \epsilon \Omega \quad \text{.....(3.48)}$$

TIME-STEPPING SCHEME

This scheme is used to handle the time-variable of heat conduction process and then the system is replaced by a set of inhomogeneous modified Helmholtz equations. There are different approaches to handle time variable, two of which are; (1) Laplace transform; (2) Finite differencing in time. Since numerical inversion of the Laplace transform is often ill-poised, here we apply the finite difference scheme to handle the time variable. For a typical time interval $[t^n, t^{n+1}] \in [0,T]$, $T(x,t)$, rative with respect to time variable t and $Q(x,t)$ oximated as

$$T(x,t) = \theta T^{n+1} + (1-\theta)T^n(x) \quad \text{.....(3.49)}$$

$$\frac{\partial T(x,t)}{\partial t} = \frac{T^{n+1}(x) - T^n(x)}{\tau} \quad \text{.....(3.50)}$$

$$Q(x,t) = \theta Q^{n+1}(x) + (1-\theta)Q^n(x) \quad \text{.....(3.51)}$$

where the superscripts n and $n+1$ refer to subsequent $\tau = t^{n+1} - t^n$ and is θ $(0 \leq \theta \leq 1)$ is a real parameter that determines if the n$(\theta = 0)$, explicit $(\theta = 1)$licit

or a linear combination of both. It is easily verified that the conditions which prevent oscillations in explicit case are exactly the same as the commonly cited sufficient conditions which ensure that it is stable. Furthermore, even though a Crank Nicolson approach is unconditionally stable, it permits the development of spurious oscillations unless the step size is no more than twice that required for an explicit method to be stable. Although an explicit scheme is only first-order accur$\theta = 1$ne, it is proved that the PDE can be solved accurately using the implicit scheme. Hence, we use in our analysis. Substituting equation (3.50) into equation (3.51) and rearrt^{n+1} it yields the following $T^{n+1}(x)$;

$$\nabla^2 T^{n+1}(x) - \frac{\rho c}{k\tau} T^{n+1}(x) = -\frac{\rho c}{k\tau} T^n(x) - \frac{1}{k} Q^n(x) \quad \text{.....(3.52)}$$

Note that the right-hand side of equation (3.52) is well defined in terms of approximate solution T^n calculated on the previous time step $t = t^n$. To start the procedure we take $T(x,0) = T_0$, the initial condition of the transient problem. For simplicity, the single step formula of equation (3.52) can be written as;

$$(\nabla^2 - \lambda^2) T(x) = f(x) \quad \text{.....(3.53)}$$

where

$$\lambda = \sqrt{\frac{\rho c}{\tau k}}$$

$$f(x) = -\frac{\rho c}{\tau k} T^n(x) - \frac{Q^n(x)}{k} \quad \text{.....(3.54)}$$

Equation (3.54) is a sequence of inhomogeneous modified Helmholtz equation

Dual Reciprocity Boundary Element Method (DRBEM) for particular Solution

The DRBEM employs a fundamental solution corresponding to a simpler equation, and treats the remaining terms as well as other non-homogeneous terms in the original equation, through a procedure which involves a series expansion using global approximating functions and the applications of the reciprocity principle (Partridge et.al, 1992).The method is called dual reciprocity method because it utilizes twice times of basic reciprocal theorem. It is essentially a method of constructing particular solutions that can be used to solve non-linear and time- dependent problems as well as to represent any internal source distribution. The main idea of the DRBEM is to divide the solution into two parts; a known particular solution of the inhomogeneous plus a complementary solution of its inhomogeneous counterpart. Since particular solutions to complex problems are very difficult or sometimes even

impossible to obtain, the in homogeneity is approximated by a series of simpler radial basis functions (RBFs) for which particular solutions can be easily determined. In particular, the DRBEM, which transforms domain integrals to boundary integrals by combining radial basis functions and conventional BEM, has wide applications in practical engineering. Due to linear property of equation (3.53), its solution can be expressed as a summation of a particular solution T_p and a homogeneous solution T_h

$$T = T_p + T_h$$

where T_p satisfies the inhomogeneous equation

$$(\nabla^2 - \lambda^2)T_p(x) = f(x) x \epsilon \Omega \ldots\ldots(3.55)$$

but does not necessarily satisfy the boundary condition.

T_h satisfies,

$$(\nabla^2 - \lambda^2)T_h(x) = 0, \quad x \in \Omega \ldots\ldots(3.56)$$

The particular solution T_p can be obtained by DRBEM. To do this the right-hand side term of equation (3.55) is approximated by RBF, yielding

$$f(x) = \sum_{i=1}^{N} \alpha_i \varphi_i(x) x \epsilon \Omega \ldots\ldots \quad (3.57)$$

where N is the number of interpolation points in the domain under consideration. Here,

$\varphi_i(x) = \varphi(r) = \varphi(|x - x_i|)$ denotes radial basis functions with the reference point x_i and α_i are interpolating coefficients to be determined.

Simultaneously, the particular solution T_p is similarly expressed as

$$T_p(x) = \sum_{i=1}^{N} \alpha_i \psi_i(x) \ldots\ldots(3.58)$$

where ψ_i represents corresponding approximated particular solutions which satisfy the following differential equations.

$$(\nabla^2 - \lambda^2)\psi_i = \psi_i \ldots\ldots(3.59)$$

noting the relation between the particular solution T_p and the function *f(x)* in equation (3.57).

By enforcing equation (3.59) to satisfy equation (3.58) at all nodes, we can obtain a set of simultaneous equations to uniquely determine the unknown coefficients *ai.*

These coefficients can be evaluated numerically.

Numerical Solutions

In this section, two numerical examples of heat conduction problems, to which analytical solutions are available, are used to test the accuracy and efficiency of DRBEM.

Example 1

Consider heat equation

$U_t = U_{xx} + 2 \qquad 0 < x < 1, \;\; 1 < t < 2$.....(4.1.0)

The boundary conditions are;

$U_x(o,t) = 0 \qquad 1 < t < 2$.....(4.2.0)

$U(1,t) = 1 + 4t1 < t < 2$..... (4.3.0)

The initial condition is;

$U(x,0) = x^2 0 < x < 1$..... (4.4.0)

We solve the equation using the DRBEM and compare the results with the analytic solution.

The exact solution to the above heat equation is

$U(x,t) = x^2 + 4t$ ..... (4.5.0)

Figure 2: Temperature distribution against x, when N=5

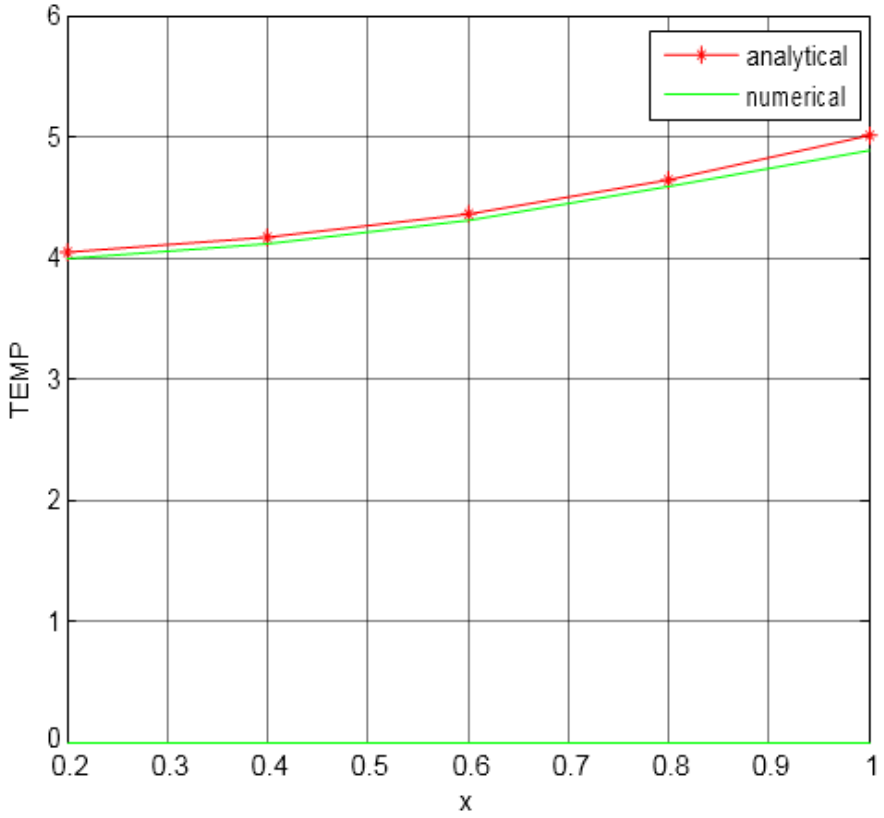
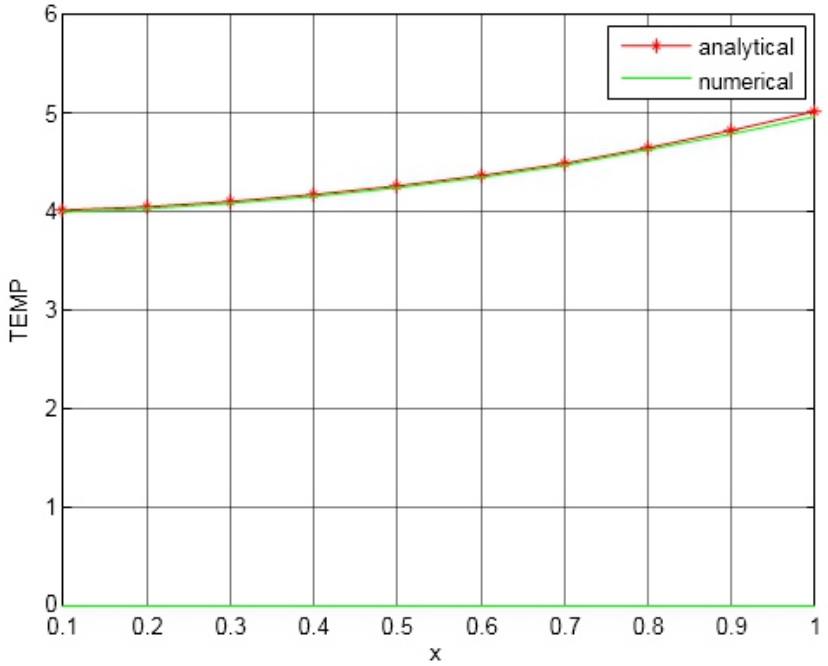


Figure 3; Temperature distribution against x, when N=10



Example 2

Consider the heat conduction problem

$$U_t(x,t) = U_{xx}(x,t) + f(x) \quad ;0 < x < 1, 1 < t < 2, \ldots\ldots\ldots\ldots\ldots(4.2.0)$$

The boundary conditions are;

$$U(0,t) = 2 \qquad 1 < t < 2 \qquad (4.2.1)$$

$$U(1,t) = 3 \qquad 1 < t < 2 \qquad (4.2.2)$$

The initial condition is;

$$U(x,0) = x^2 + \sin(2\pi x); \quad 0 \leq x \leq 1 (4.2.1)$$

The problem has a dirichlet homogeneous boundary surface at one end. The exact solution of this problem is

$$U(x,t) = x^2 + 2t + \sin(2\pi x); \quad 0 \leq x \leq 1, 1 \leq t \leq 2 \ldots\ldots\ldots(4.2.2)$$

$$f(x) = 4\pi^2 \sin(2\pi x) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4.2.)$$

Figure 4; Temperature distribution against x, when the time step is 1, time interval is 0.04, with N=50.

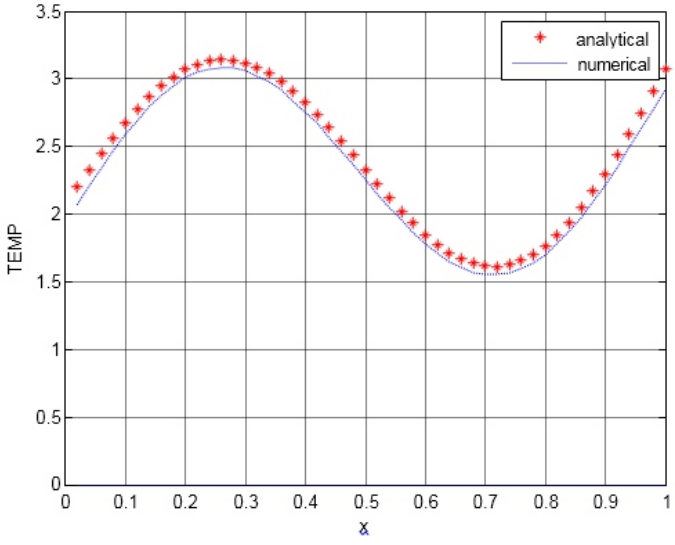


Figure 5; Temperature distribution when the time step is 1, time interval is 0.02, with N=50

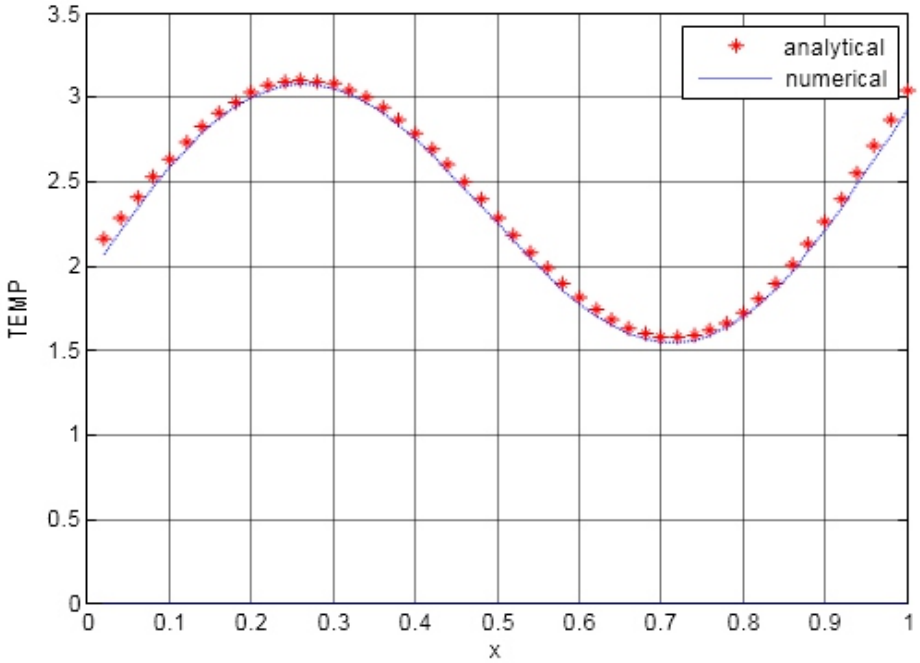
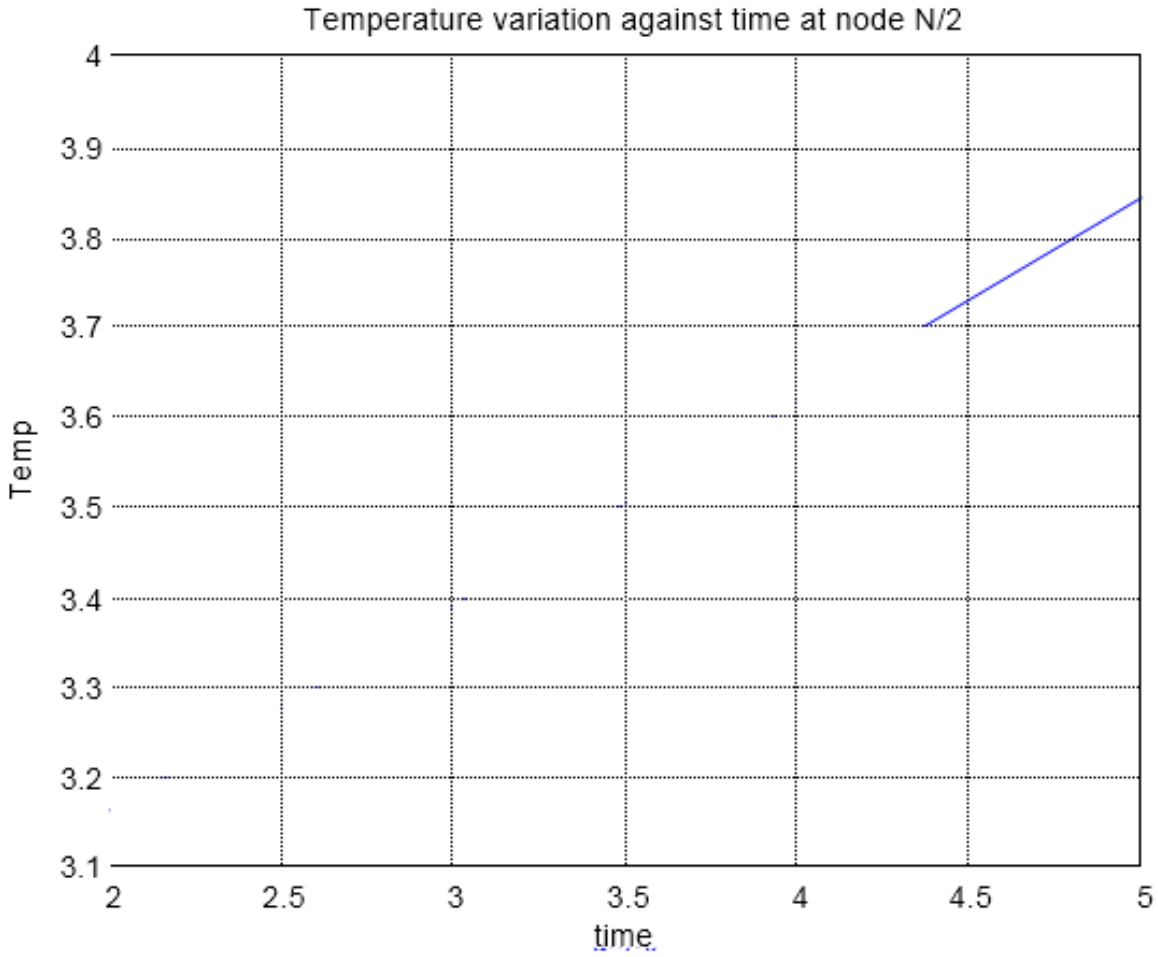


Figure 6; Temperature variation against time at the center node



DISCUSSION OF GRAPHS

Figure 2, shows the temperature distribution against space variable x when the nodes are five. The source term in the heat equation is two. At temperature , heat increases within the bar because of the source term. As more nodes are increased the flow becomes smooth. The temperature distribution along the bar increases. The analytic solution and the numerical solution coincide as the discretization nodes are increased.

Figure 4 and figure 5 show the temperature distribution against spacial variable x along the rod. This is a sinusoidal graph that stabilizes as the number of time step is reduced. It clearly shows when the time interval at time step size of one is reduced the analytical and numerical solutions converge. Thus, justifying the DRBEM as a numerical solution that converges as the discretization nodes are increased.
Figure 6, shows the temperature variation against time in the center node. Temperature increases linearly with time, an indication that within the bar there is an internal heat generating term, which is the source term.

These graphical results shows the importance of source term in the design of materials used in heat generating regions. The DRBEM can be developed as an efficient method to model and analyze the heat and cooling systems which are governed by the heat equations. For example, the combustion chamber and nozzle walls have to withstand relatively high temperature, high gas velocity, chemical erosion and high stress. The choice of materials used should be such that the wall material must be capable of enduring high heat transfer rates (which means good thermal conductivity) yet, at the same time, have adequate strength to withstand the chamber combustion pressure. All these considerations are as a result of the presence of the source term. Material requirements are critical only in those parts which come into direct contact with propellant gases.

CONCLUSION

The main objective of the study was to solve a one-dimensional transient heat conduction problem using DRBEM. With the help of the governing equations in chapter three fundamental solutions for heat equation was discretized over the time and space. A thin finite slab geometry (0,1) was used with specified boundary conditions to model the problem. The mathematical software MATLAB was used to compute results and graphs were drawn at various nodes of discretization. Two test problems, parabolic and sinusoidal functions were used. It is clear that the comparison of the analytical and numerical results presented by the DRBEM leads to a rapid convergence to the exact solutions with small discretization of time parameter. The results obtained from both problems were very close to the analytical solution confirming the efficiency of DRBEM. The effect of increasing the number of discretization of the

boundary resulted high convergence. It is clearly shown that the presence of internal heat generation or source term leads to an increase in temperature distribution within the material. However, this increase depends on the function of the source term. These findings can help in the design of thermal insulators in high heat generating materials and also in choosing the type of materials to use in making conductors and insulators.

RECOMMENDATION

For future work, we may extend the DRBEM formulation to transient problems governed by convection-diffusion equations with a constant or variable velocity field. In addition, we may try to investigate the feasibility of applying the DRBEM to non-linear scalar wave propagation problems or hyperbolic heat conduction problems. From the mathematical point of view, more theoretical studies are required in order to support numerical studies related to convergence of the solution of a linearized system to the true solution of the original nonlinear differential system. However, this could be quite involving but well rewarding.

REFERENCES

[1] A. J. Nowak and C. A. Brebbia, "Solving Helmholtz equation by Multiple reciprocity method" in computer and experiments in fluids flow (eds G.M Carlomagno and C.A.
Brebbia), (comput.,southampton, 1989) 265-270
[2] A.C.Neves and C.A. Brebbia, "The multiple reciprocity element method inelasticity: A new approach for transforming domain integrals to boundary", Int. J. Numer. Methods Eng.31 (1991) 709-729.
[3] Bialecki R. A, Jurga's P. , (2002), Dual reciprocity Boundary Element Method without matrix inversion for transient heat conduction, Engineering Analysis with Boundary Elements, 26, 227-236.
[4] M.Itagaki and C.A.Brebbia, "Generation of higher order fundamental solutions to thetwo- dimensional modified Helmholtz equation", Eng. Anal. Boundary Elements11 (1993) 87- 90
[5] C.A.Brebbia, J. C. F.Tells and L.C. Wrobel (ads.), Boundary element techniques (Springer, Berlin, 1984)
[6] D. Nardini and C. A. Brebbia, "A new approach to free vibration analysis using boundary elements".(comput.Mech. ,Southampton, and Springer, Berlin, 1982).
[7] P.W. Partridge and C. A.Brebbia, "Computer implementation of the BEM dualreciprocitymethod for the solution of Poisson-type equations", Software Engrg.workstation5 (1989) 199-206
[8] Edmond Ghandour (1974). Initial Value Problem for Boundary Values of a Green's Function. Journal of Applied Mathematics.Vol.27, pg 650-652.
[9] L. Wrobel (2002), The Boundary Element Method; Applications Thermo- Fluidsand Acoustics. Vol.1.pg 20-35.
[10] Paris F. (1997).Boundary Element Method; Fundamentals and Applications, Oxford University Press.
[11] Iso Y. (1991) Convergence of Boundary Element solutions for Heat Equation. Journal of Computational and Applied Mathematics, vol. 38,pg 201-209.
[12] P.W.Partridge and L.C.Wrobel, "The dual reciprocity method for spontaneous Ignition".Int. J.Numer.methods Eng.30 (1990) 953-963
[13] S. P. Zhu and Y.L. Zhang, "Improvement on dual reciprocity boundary element for equations with convective terms", Comm. Numer. methods Eng. 10 (1994) 361-371.
[14] Y. L. Zhang and S. P Zhu , "On the choice of interpolation functions used in the dual- reciprocity boundary element method", Eng.Anal. Boundary Elements13 (1994)387-396
[15] S. P Zhu, H. W. Liu and X. P. Lu , "A combinationof the LTDRM and ATPs in solving linear diffusion problems", Eng. Anal. Boundary Elements 21 (1998) 285- 289.
[16] I. L. Bruton and A. J. Pullan, "A semi-analytic boundary element for parabolic problem", Eng. Anal. Boundary Elements,18, (1996) 253-264.

[17] Onyango T.T.M, Ingham D.B and D.Lensic, (2008) Restoring Boundary ConditionsIn Heat Transfer, Journal of engineering mathematics, vol. 62.No1 pg85-101.Universty of Leeds, U.K.

[18] Mushtag, Shak and Muhammed, (2010) Comparison of direct and indirect boundary element methods for the flow past a sphere. Journal of American Science 2010, 61, pg166-17

[19] MohammadiaM ,Hematiyan M.R, Marin L. (2010), Boundary element analysis of nonlinear transient heat conduction problems involving non-homogeneous and nonlinear heat sources using time-dependent fundamental solutions, Engineering Analysis with Boundary Elements,34,655-665

[20] Ochiai Y., Kitayama Y. (2009), Three-dimensional unsteady heat conduction analysis of triple-reciprocity boundary element method, Engineering Analysis withBoundary Elements, 33, 789-795.

[21] Yang K., Gao X. W. (2010), Radial integration of Boundary Element Method for transient heat conduction problems, Engineering Analysis with Boundary Elements, 34, 557-563.

[22] Sutradhar A. ,Paulino G.H. (2004), The simple boundary element method for transient heat conduction in functionally graded materials, Computer methods in Applied Mechanics and Engineering, 193, 4511-4539.

Instructions for Authors

Essentials for Publishing in this Journal

1 Submitted articles should not have been previously published or be currently under consideration for publication elsewhere.

2 Conference papers may only be submitted if the paper has been completely re-written (taken to mean more than 50%) and the author has cleared any necessary permission with the copyright owner if it has been previously copyrighted.

3 All our articles are refereed through a double-blind process.

4 All authors must declare they have read and agreed to the content of the submitted article and must sign a declaration correspond to the originality of the article.

Submission Process

All articles for this journal must be submitted using our online submissions system. http://enrichedpub.com/ . Please use the Submit Your Article link in the Author Service area.

Manuscript Guidelines

The instructions to authors about the article preparation for publication in the Manuscripts are submitted online, through the e-Ur (Electronic editing) system, developed by **Enriched Publications Pvt. Ltd**. The article should contain the abstract with keywords, introduction, body, conclusion, references and the summary in English language (without heading and subheading enumeration). The article length should not exceed 16 pages of A4 paper format.

Title

The title should be informative. It is in both Journal's and author's best interest to use terms suitable. For indexing and word search. If there are no such terms in the title, the author is strongly advised to add a subtitle. The title should be given in English as well. The titles precede the abstract and the summary in an appropriate language.

Letterhead Title

The letterhead title is given at a top of each page for easier identification of article copies in an Electronic form in particular. It contains the author's surname and first name initial .article title, journal title and collation (year, volume, and issue, first and last page). The journal and article titles can be given in a shortened form.

Author's Name

Full name(s) of author(s) should be used. It is advisable to give the middle initial. Names are given in their original form.

Contact Details

The postal address or the e-mail address of the author (usually of the first one if there are more Authors) is given in the footnote at the bottom of the first page.

Type of Articles

Classification of articles is a duty of the editorial staff and is of special importance. Referees and the members of the editorial staff, or section editors, can propose a category, but the editor-in-chief has the sole responsibility for their classification. Journal articles are classified as follows:

Scientific articles:

1. Original scientific paper (giving the previously unpublished results of the author's own research based on management methods).

2. Survey paper (giving an original, detailed and critical view of a research problem or an area to which the author has made a contribution visible through his self-citation);

3. Short or preliminary communication (original management paper of full format but of a smaller extent or of a preliminary character);

4. Scientific critique or forum (discussion on a particular scientific topic, based exclusively on management argumentation) and commentaries. Exceptionally, in particular areas, a scientific paper in the Journal can be in a form of a monograph or a critical edition of scientific data (historical, archival, lexicographic, bibliographic, data survey, etc.) which were unknown or hardly accessible for scientific research.

Professional articles:

1. Professional paper (contribution offering experience useful for improvement of professional practice but not necessarily based on scientific methods);
2. Informative contribution (editorial, commentary, etc.);
3. Review (of a book, software, case study, scientific event, etc.)

Language

The article should be in English. The grammar and style of the article should be of good quality. The systematized text should be without abbreviations (except standard ones). All measurements must be in SI units. The sequence of formulae is denoted in Arabic numerals in parentheses on the right-hand side.

Abstract and Summary

An abstract is a concise informative presentation of the article content for fast and accurate Evaluation of its relevance. It is both in the Editorial Office's and the author's best interest for an abstract to contain terms often used for indexing and article search. The abstract describes the purpose of the study and the methods, outlines the findings and state the conclusions. A 100- to 250-Word abstract should be placed between the title and the keywords with the body text to follow. Besides an abstract are advised to have a summary in English, at the end of the article, after the Reference list. The summary should be structured and long up to 1/10 of the article length (it is more extensive than the abstract).

Keywords

Keywords are terms or phrases showing adequately the article content for indexing and search purposes. They should be allocated heaving in mind widely accepted international sources (index, dictionary or thesaurus), such as the Web of Science keyword list for science in general. The higher their usage frequency is the better. Up to 10 keywords immediately follow the abstract and the summary, in respective languages.

Acknowledgements

The name and the number of the project or programmed within which the article was realized is given in a separate note at the bottom of the first page together with the name of the institution which financially supported the project or programmed.

Tables and Illustrations

All the captions should be in the original language as well as in English, together with the texts in illustrations if possible. Tables are typed in the same style as the text and are denoted by numerals at the top. Photographs and drawings, placed appropriately in the text, should be clear, precise and suitable for reproduction. Drawings should be created in Word or Corel.

Citation in the Text

Citation in the text must be uniform. When citing references in the text, use the reference number set in square brackets from the Reference list at the end of the article.

Footnotes

Footnotes are given at the bottom of the page with the text they refer to. They can contain less relevant details, additional explanations or used sources (e.g. scientific material, manuals). They cannot replace the cited literature.
The article should be accompanied with a cover letter with the information about the author(s): surname, middle initial, first name, and citizen personal number, rank, title, e-mail address, and affiliation address, home address including municipality, phone number in the office and at home (or a mobile phone number). The cover letter should state the type of the article and tell which illustrations are original and which are not.

Note