

SIGNAL



Volume - 17 :: Issue No - 1 :: January-March, 2020

CHAIRMAN'S MESSAGE

Mr. P. S. Biswas

At the end of my tenure as the chairman of IETE, Kolkata centre, I am very happy to see the publication of Volume: 17 issues: 1 of SIGNAL, These are also the 5th and 6th issues after its revival. Because we received more material than what could be accommodated in one issue , and the earlier publication got delayed because of lockdown difficulties, we decided to publish two issues simultaneously.

The main topic of these publications is Sensor Network. We are all moving towards smarter and smarter environment. WSN is gradually going to be integral part of our lives and activities in future.

Your comments through our website are most welcome.

Partha S Biswas.

Chairman, IETE Kolkata Center

Members

- ⇒ Mr. P. S. Biswas, Hon. Chairman
- ⇒ Dr. Jyotsna Kumar Mandal, Secretary
- ⇒ Prof. P. R. Bandopadhyay, Treasurer
- ⇒ Mr. S. C. Rudra, Immediate Past Chairman, IETE Kolkata Centre
- ⇒ Mr. Anirban Guha, Vice Chairman
- ⇒ Sri Tapan Jyoti Sen, Committee Member
- ⇒ Mr. S. D Tiwary, Committee Member
- ⇒ Dr. A. K. Mukhopadhyay, Committee Member
- ⇒ Smt. Sangita Roy, Committee Member
- ⇒ Mr. Dibyandu Majumder, Committee Member
- ⇒ Prof. Dr. Sujit Biswas, Ex. Professor, Jadavpur University Co-opted Member
- ⇒ Mr. Soumya Roy, Ex. CGM Calcutta Telecom, Co-opted Member
- ⇒ Mr. Aniruddha Nag, Co-opted Member

EVENTS

UPCOMMING EVENTS

- ⇒ IETE Students' Forum, Haldia Institute of Technology will organize ByteFight coding competition during 25th April and 1st May 2020:
- ⇒ Webinar on "Industry Evolution, Fundamentals of Container/ Kubernetes & Associated Security" will be held on 03-06-2020 at the Adamas University.
- ⇒ Webinar on "What role will you play in the 5G enabled future world?" will be held on 09-06-2020 at the Adamas University:



Fight Against CORONA—Stay Home, Stay Safe

EDITOR'S COLUMN

Dr. Jyotsna Kumar Mandal

The Managing committee took charge during third week of July 2018. In the 7th EC meeting of IETE Kolkata Centre it was decided to revive the Quarterly Newsletter "SIGNAL" of IETE Kolkata Centre under the leadership of the Secretary, IETE as Editor. This last issue newsletter was published in December 2005. Fifteen years Long tradition was suspended due to some unknown reasons. MC, IETE has arranged to publish the IETE Newsletter which has been stopped since 2005. It was decided that the volume and issue numbers will be continuous, but the year of publication will start for 2019. The volume no 16 and the issue number 1, has been published as January-March 2019. The Secretary took initiative to redesign the newsletter and uploaded issues into to the web portal of IETE(www.ietekolkata.org) with circulation to all members of IETE. No printed version is there. Since January 2019 five issues are uploaded into the IETE web site. In this auspicious Annual General Meeting, we are publishing two issues due to receipt of good number of materials. Various activities of IETE Kolkata Center and different ISF Center have been reflected into these tow issues (Vol. 17 issue 1(January-March, 2020) and Vol 17 issue 2(April-June 2020)). Due to Lock Down, we could not host our International Conference IoTWR-2020. On 27th of June we have conducted this IoTWR-2020 in online mode. Glimpse about the event is also given in the vol. 17, issue 2.

On behalf of IETE Kolkata Center I would like to thanks to all esteem corporate members for their cooperation during entire period of my tenure. I would like to express my gratitude to OBs and EC members of IETE for their supports.

These two issues will be a valuable documents to the esteem members.

Best wishes

Jyotsna Kumar Mandal
Secretary, IETE Kolkata Centre
Editor, SIGNAL

"Take risk in your life. If you win, you can lead. If you loose"

— Swami Vivekananda

Trust Management System in Wireless Self-Organizing Networks

Prof. Subir Kumar Sarkar , Department of Electronics and Telecommunication Engineering,
Jadavpur University, Kolkata, India

Introduction:

Ad hoc networks are autonomous systems which comprise a collection of mobile nodes that use wireless transmission for communication. They are self-organized, self-configured, and self-controlled infrastructure-less networks. In the last few years , mobile ad hoc networks (MANET) and wireless sensor networks(WSN) have seen increased adaptation in a variety of disciplines because they can be deployed with simple infrastructures and virtually no central administration. This type of network can be set up or deployed anywhere and anytime because it poses very simple infrastructure setup and no or minimal central administration. In particular , the development of MANET and WSN provides tremendous opportunities in areas including disaster recovery , defense , health care, researchers , students, and industrial environments. A self-organizing network is a network that can automatically extend, change, configure and optimize its topology, coverage, capacity, cell size, and channel allocation, based on changes in location, traffic pattern, interference, and the situation or environment. Each node in these networks acts as trans-receiver and communicates via hops when some nodes are out of coverage area. Due to high mobility the topology of the networks changes dynamically, thus making routing very challenging. Only sender intends that receiver should "understand" message contents. But because of universal electronic connectivity electronic eavesdropping, viruses, hackers and electronic fraud can threaten thereby putting special importance on security. However because of proper attention on the area of network security there is significant development of practical , available applications to enforce network security. In MANETs and WSNs, nodes may exhibit various types of misbehavior. Node's misbehavior may be categorized into two broad types: Malicious behaviorà intention is to attack and damage the network, Selfish behaviorà intention is to save power, memory and CPU cycle. A malicious node delays packet forwarding to ensure that time-to-live (TTL) of the packets are expired so that the packets do not reach the destination. In order to prevent various attacks, which WSNs and MANET suffer, the possible solutions can be adapted. Trust tells the degree of reliability of other node in performing actions. It can be evaluated by maintaining a record of the transactions with other nodes directly as well as indirectly.

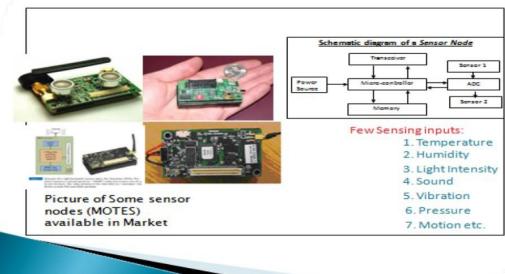
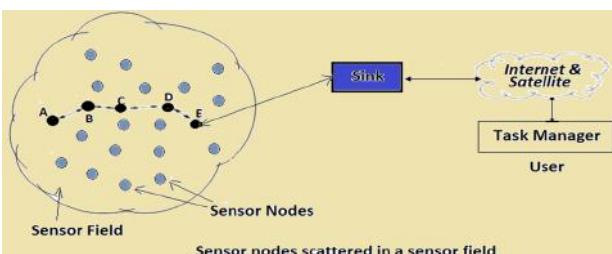
Wireless Self-Organizing Networks (Ad-hoc Network):

A self-organizing network is a network that can automatically extend, change, configure and optimize its topology, coverage, capacity, cell size, and channel allocation, based on changes in location, traffic pattern, interference, and the situation or environment. Wireless ad hoc networks is a special class self-organizing network, where capabilities or existence of links, capabilities or availabilities of nodes or network services are considered as a random function of time. Examples: MANETs and WSN. A Mobile Ad hoc NETwork (MANET) is a collection of mobile nodes that can has no fixed or predetermined topology, with mobile nodes and dynamic membership changes. A Wireless Sensor Network (WSN) is a highly distributed network consisting of a large number of tiny, low cost, light-weight wireless nodes deployed to monitor an environment or system.

Wireless Sensor Network:

A Wireless Sensor Network (WSN) consists of spatially distributed autonomous wireless sensors (also called nodes or motes) to cooperatively monitor physical or environmental conditions, such as temperature, humidity, light intensity, sound, vibration, pressure, motion etc. Each node will be having its small sensing area of few meters and radio range

approximately 10 to 15 meters. Each node or Mote can sense, compute and communicate each other. They can either receive message or transmit message and can transmit messages to the sink (or Base Station) via self-configuration and multi-hop routing. The sink can use many ways to communicate with remote network, such as Internet, satellite and mobile communication network. Finally, the Task Manager (User) collects this transmitted data.



Sensor Node limitations:

- Limited Hardware
 - Limited Processing
 - Limited Storage
 - Limited Communication Capability
 - Limited Energy Supply
 - Limited Bandwidth
 - Limited Support for Networking
- N/W is peer-to-peer with mesh topology and dynamic, mobile and unreliable connectivity
There are no universal routing protocols or central registry services
Each node acts both as a router and as an application host.

Application Domain of WSN:

- Military fields.
- Medical monitoring and Health care.
- Industrial Control.
- Homeland security.
- Ocean and wildlife monitoring.
- Building safety.
- Earthquake Early Warning and Monitoring.
- Environmental applications.
- Intelligent green aircrafts.
- Smart Roads.

Contd..

Limitations of WSN:

Deployment environment is *Hazardous*.

Unattended, hostile and dangerous.

Susceptible to variety of *Attacks*.

nodes can be physically tampered and mis-configured by an external or an insider attacker, adversary force overtaking.

Nodes are High-volume.

Nodes must be economic.

Hence, limitations on node's capabilities.

Due to resource constraint, there is an incentive for a node to act in a selfish manner without cooperating with other nodes.

....To be continued in next issue

GLIMPSES OF EVENTS

During January–March, 2020

Webinar on "Security and Authentication through Imperceptible Communication" on April 22,2020

A Webinar Program on "Security and Authentication through Imperceptible Communication" were organised by , under the IETE student forum, ECE dept. NIT. Prof. J K Mandal was the speaker. The lecture covered cryptography, security, authentication and its application in signal processing covering communication, image, text processing. Different state-of-the art algorithms were also explained with their applications in the related issues. The session was informative, lucid .Intuitive question answer session was followed after the lecture. Students and participants asked different hacking, security threats problems that we are facing. Prof. Mandal answered all the.



Expert talk on "Zero Trust: A model for more effective security to stop data breaches in Wireless Self-Organizing Networks"

Dr. Subir Kumar Sarkar, Professor & Former Head, Senior Member IEEE & IEEE Distinguished Lecturer of Electron Device Society, Coordinator IC Design and Fabrication Centre, Coordinator of Evening course M. Tech in VLSI Design and Microelectronics Technology, Department of Electronics and Telecommunication Engineering, Jadavpur University, Kolkata-700 032, India has received IETE- Brig M L Anand Award -2019 for his experience in Network area as is evident from your 183 research papers, 20 PG and 18 PhD thesis guidance and publication of two books (CRC Press & Artech House) whose review came in IEEE Communication Magazine and has been cited 500 times (now more than 550) times. The condition of the award was to give a talk on the topic in the Local section of IETE that is IETE Kolkata Center. In this connection Prof. (Dr.) Subir Kumar Sarkar delivered his expert talk on "Zero Trust: A model for more effective security to stop data breaches in Wireless Self-Organizing Networks" on 9th January, 2020 at 4 pm in the VSNL Auditorium of the IETE Kolkata Center. More than 30 participants including corporate members, faculty members of different Universities and Institutes were present in the occasion.



Institution of Electronics and Telecommunication Engineers

Kolkata Centre.

Plot No J1-7, EP-Block, Sector V, Salt Lake, Electronics Complex

Contact: 03323577054 Mail: ietekolkata@gmail.com

www.ietekolkata.org