भाग 23 / अंक 4 अक्तूबर 2019 त्रैमासिक पत्रिका

ISO 9001 : 2015

TEC

दूरसंचार अभियांत्रिकी केन्द्र
TELECOMMUNICATION ENGINEERING CENTRE

टी ई सी संचारिका
NEWSLETTER

IoT Experience Center

An IoT Experience Center was inaugurated by Mr. A K Sanghi, the then Advisor, TEC & Mr. Arvind Chawla, the present Sr. DDG, TEC on 27th Sept 2019 in Telecommunication Engineering Centre, Khurshid Lal Bhawan, Janpath, New Delhi. It is located on 6th floor of TEC building. This IoT Center is having 17 IoT use cases working in real time. These use cases have been provided by STMicroelectronics, TATA Communications Ltd. (TCL), SenRa, Sensorise Digital Services Pvt. Ltd. and Trusted Objects.

Inauguration of IoT Experience Center in TEC on 27th September, 2019

Continue from cover page……

Visit during Inauguration of IoT Experience Centre

Group Photograph during Inauguration of IoT Experience Centre

Mandatory Testing and Certification of Telecom Equipment (MTCTE)

MTCTE portal was opened on 5th July'19 and acceptance of applications for 13 Nos. of telecom equipment covered under Phase-I commenced on 9th July'19. Certification for these telecom equipments was made mandatory w.e.f. 1st Oct'19. The smooth implementation of Phase-I of MTCTE has been appreciated by various stakeholders and their representative organizations viz. COAI/MAIT, ITI.

Following notifications/office memorandums for the purpose of MTCTE have been issued: -

i. Mechanism for grant of exemption from submission of test reports against few parameters has been finalized and the office memorandum in this regard.
ii. Notification for relaxation of Customer Premises Equipment with RF interface from testing against IEC:60215 standards.
iii. Notification for consideration of date of dispatch of telecom equipment from foreign port as date of import for the purpose of MTCTE.

First batch of MTCTE certificates, issued by TC division, TEC were presented by Ms. Aruna Sundarajan, the then Secretary (Telecom) to first two applicants: M/s Matrix Comsec Pvt. Ltd. & M/s Panasonic India Pvt. Ltd. on 30th July'2019. Fiftieth CAB (Conformity Assessment Bodies) certificate of Lab designation, issued by MRA division, TEC was presented by Ms. Aruna Sundarajan, the then Secretary (Telecom) to M/s ERTL, New Delhi on 30th July'2019.

Telecom News: At a Glance

1. Shri Ravi Shankar Prasad, Hon'ble Minister of Communications met with Ambassador of Japan to India Kenji Hiramatsu on 15-07-2019 and discussed the ways to enhance mutual cooperation between India and Japan in the field of telecommunications and digital technologies.

2. On the occasion of CSC Diwas on 16th July 2019, Common Service Centres Scheme (CSC) exchanged an agreement with Bharat Net for operations and maintenance of optical fibre network. This will not only ensure better services using Bharat Net as well as create job opportunity in rural areas.

3. An MoU was signed between Department of Telecommunications & Indian Council for Research on International Economic Relations [ICRIER] for preparation of Broadband Readiness Index for States/UTs in the presence of Shri Sanjay Dhotre,

Hon'ble Minister of State for Communications. On this occasion Secretary, Department of Telecommunications was also present.

4. Shri Ravi Shankar Prasad, Hon'ble Minister of Communications met CEOs of the Telecom Service Providers at Sanchar Bhawan, New Delhi on dated 27 July 2019. On this occasion Secretary (Telecom), Department of Telecommunications was also present.

5. Ms. Aruna Sundararajan, Secretary (Telecom), DoT chaired the Inauguration Ceremony of 4 day ITU-DoT Training Programme on "Human and Technical Capacity Challenges through Digital Skills" at C-DoT Campus, New Delhi on dated 29 July 2019.

6. Shri Anshu Prakash, IAS has taken over as Secretary (Telecom) and Chairman, Digital Communications Commission, on dated 1st Aug 2019 in Department of Telecommunications.

7. An India Africa ICT Expo was held in Kigali, Rwanda on 5-6 August, 2019 and inaugurated by Dr. Edouard Ngirente, Hon'ble Prime Minister of Rwanda. Delegation of DoT, India and 40 companies from India participated in this event.

8. Indian delegation attended the 5th BRICS Communications Ministers Meeting held in Brasilia, Brazil from 12-14 August 2019.

9. Shri Ravi Shankar Prasad, Hon'ble Minister of Communications launched "Maritime Telecommunication services" and a pilot project "Central Equipment Identity Register" in Mumbai on dated 13th Sep 2019 in the presence of Shri Sanjay Dhotre, Hon'ble Minister of State for Communications. Shri Anshu Prakash, Secretary (Telecom) was also present on this occasion. Maritime Telecommunication services will provide voice and data services on ships within Indian territorial waters through Indian gateways. Pilot project called Central Equipment Identity Register system has been launched in Maharashtra for blocking and tracing of lost/stolen mobile phones.

Workshop on "5G Technology and Applications" organized by RTEC Mumbai

A one-day workshop on "5G Technology and Applications" was organized by RTEC Mumbai on 19.09.2019 at Mumbai. About 115 officers and professionals from DoT, BSNL, MTNL, CABs (Conformity Assessment Bodies) and Industry participated in the event. A total of 8 distinguished speakers gave their presentations. It was an effort by RTEC, Mumbai to bring Research, Industry and Telecom Professionals at a common platform for dissemination of latest technical knowledge, research findings and field deployment issues in mobile technology with a focus on 5G. All the participants and speakers were welcome by Shri Ashok Kumar Jha, DDG(WR). Shri Abhay Shankar Verma, DDG(MT), TEC and Shri Manoj Mishra, CGM, BSNL Maharashtra Circle Mumbai gave their opening remarks followed by addresses by speakers. Prof. Vikram Gadre, Electrical Engineering Department, IIT Bombay delivered key address of "Introduction to 5G and Modulation Techniques for 5G". Shri Abhay Shanker Verma, DDG(MT), TEC presented on "5G Applications and Use Cases". Dr. Vinosh Babu James, Associate Director, Technical Standards, Qualcomm presented on the topic "Leading the World to 5G ". Shri B Sunil Kumar, PGM, BSNL presented on the topic "Migration to 5G: An Indian Perspective". Shri Prakash R, Technical Expert, CDoT presented on the topic "5G and Beyond: Overview,Trends and Standardization". Dr. S Ramakrishnan, Nokia Networks presented on the topic "5G Technology and Use Cases". Shri Rajiv Kamrani, Ericsson India Pvt. Ltd presented on "5G Market Update, Device Eco System, 5G Deployment & Spectrum, Use Cases ". Shri Kundana K Lal, VITTI Research Foundation delivered presentation on "Rise of Artificial Intelligence and its Impact on Industry". The event was highly appreciated by all the participants which included senior officers of BSNL, MTNL and DoT.

Shri Abhay Shanker Verma, DDG(MT), TEC delivering presentation

Security in Wireless Sensor Network

1.0 Introduction

Wireless sensor networks (WSNs) consist of hundreds or even thousands of small devices each with sensing, processing, and communication capabilities to monitor the real-world environment. They are envisioned to play an important role in a wide variety of areas ranging from critical military surveillance applications to forest fire monitoring and building security monitoring in the near future. In these networks, a large number of sensor nodes are deployed to monitor a vast field, where the operational conditions are most often harsh or even hostile. Each node has the abilities of calculation, detection, and communication. These nodes that can be randomly distributed in the environment to be observed can recognize each other and can perform the task of measuring in a wide area by working together.

2.0 Wireless Security Network (WSN) Architecture

In a typical WSN, we see following network components;

2.1 Sensor nodes (Field devices)

Field devices are mounted in the process and must be capable of routing packets on behalf of other devices. In most cases they characterize or control the process or process equipment.

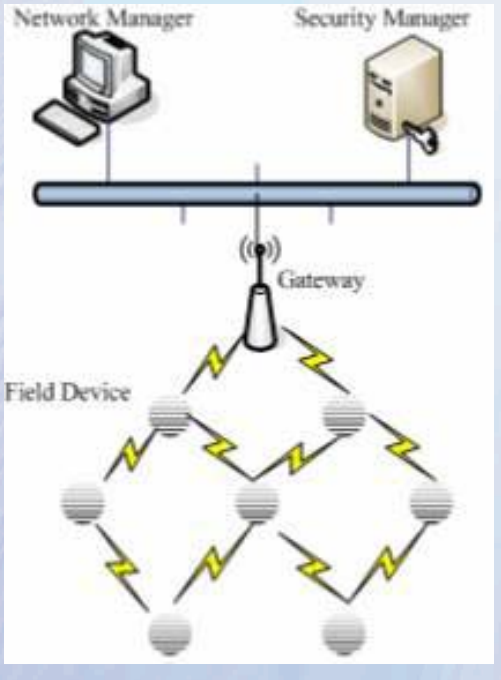

Fig. 1. WSN Architecture

2.2 Gateway or Access points

A Gateway enables communication between Host application and field devices.

2.3 Network manager

It is responsible for configuration of the network, scheduling communication between devices, management of the routing tables and monitoring and reporting the health of the network.

2.4 Security manager

The Security Manager is responsible for the generation, storage, and management of keys.

3.0 Constraints/Limitations in Wireless Sensor Networks

A WSN consists of a large number of sensor nodes that are inherently resource-constrained devices. These nodes have limited processing capability, very low storage capacity, and constrained communication bandwidth. These constraints are due to limited energy and physical size of the sensor nodes. Due to these constraints, it is difficult to directly employ the conventional security mechanisms in WSNs.

3.1 Power Limitation

The extra power consumed by sensor nodes due to security is related to the processing required for security functions (e.g., encryption, decryption, signing data, verifying signatures), the energy required to transmit the security related data or overhead.

3.2 Memory limitations

A sensor, a tiny device with only a small amount of memory and storage space. (includes flash memory and RAM). There is usually not enough space to run complicated algorithms after loading the OS and application code.

3.3 Unreliable Communication

Unreliable communication is another serious threat to sensor security. The unreliable wireless communication channel may lead to damaged or corrupted packets. The security of the network relies heavily on a defined protocol, which in turn depends on communication.

3.4 Conflicts

Even if the channel is reliable, the communication may still be unreliable. This is due to the broadcast nature of the wireless sensor network. If packets meet in the middle of transfer, conflicts will occur and the transfer itself will fail. In a crowded (high density) sensor network, this can be a major problem.

3.5 Latency

The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

3.6 Unattended Operation

In most cases, the nodes in a WSN are deployed in remote regions and are left unattended. The likelihood that a sensor encounters a physical attack in such an environment is therefore, very high. Remote management of a WSN makes it virtually impossible to detect physical tampering. This makes security in WSNs a particularly difficult task.

3.7 No Central Management

A sensor network should be a distributed network without a central management point. This will increase the vitality of the sensor network. However, if designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

4.0 Security Requirements

A WSN is a special type of network. The security services in a WSN should protect the information communicated over the network and the resources from attacks and misbehaviour of nodes. The most important security requirements in WSN are listed below:

4.1 Data Confidentiality

The security mechanism should ensure that no message in the network is understood by anyone except intended recipient.

4.2 Data Integrity

With the implementation of confidentiality, an adversary may be unable to steal information. However, this doesn't mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray. Thus, data integrity ensures that any received data has not been altered in transit.

4.3 Data Freshness

It implies that the data is recent and ensures that no adversary can replay old messages. This requirement is especially important when the WSN nodes use shared-keys for message communication, where a potential adversary can launch a replay attack using the old key as the new key is being refreshed and propagated to all the nodes in the WSN.

4.4 Self-Organization

Each node in a WSN should be self-organizing and self-healing. This feature of a WSN also poses a great challenge to security. The dynamic nature of a WSN makes it sometimes impossible to deploy any pre-installed shared key mechanism among the nodes and the base station.

4.5 Time Synchronization

Most of the applications in sensor networks require time synchronization. Any security mechanism for WSN should also be time-synchronized. A collaborative WSN may require synchronization among a group of sensors.

4.6 Secure Localization

Often, the utility of a sensor network will rely on its ability to accurately and automatically locate each sensor in the network. A sensor network designed to locate faults will need accurate location information in order to pinpoint the location of a fault.

4.7 Authentication

While constructing the sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle).

5.0 Types of attacks

Simplicity in Wireless Sensor Network with resource constrained nodes makes them extremely vulnerable to variety of attacks. Attackers can eavesdrop on our radio transmissions, inject bits in the channel, replay previously heard packets and many more. These are:

5.1 Denial of Service

Denial of Service (DoS) is any event that diminishes or eliminates a network's capacity to perform its expected function. Most of the defense mechanisms require high computational overhead and hence not

suitable for resource-constrained WSNs. Some important types of DoS attacks in WSNs are:

5.1.1 Physical layer attacks

The physical layer is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption. As with any radio-based medium there exists the possibility of jamming in WSNs. There are two broad categories of attack on WSNs in the physical layer;

a) Jamming

it is a type of attack which interferes with the radio frequencies that the nodes use in a WSN for communication.

b) Tampering

Sensor networks typically operate in outdoor environments. Due to unattended and distributed nature, the nodes in a WSN are highly susceptible to physical attacks.

5.1.2 Link layer attacks

The link layer is responsible for multiplexing of data-streams, data frame detection, medium access control, and error control. Attacks in this layer are:

a) Collision: A collision occurs when two nodes attempt to transmit on the same frequency simultaneously.

b) Exhaustion: Repeated collisions can also be used by an attacker to cause resource exhaustion.

c) Unfairness: It is weak form of DoS attack. An attacker may cause unfairness by intermittently using the above link layer attacks.

5.1.3 Network layer attacks

The network layer of WSNs is vulnerable to the different types of attacks such as:

a) Spoofed routing information

The most direct attack against a routing protocol is to target the routing information in the network. An attacker may spoof, alter, or replay routing information to disrupt traffic in the network.
These disruptions include creation of routing loops, attracting or repelling network traffic from selected nodes, extending or shortening source routes, generating fake error messages, causing network partitioning, and increasing end-to-end latency.

b) Selective forwarding

In a multi-hop network like a WSN, for message communication all the nodes need to forward messages accurately. An attacker may compromise a node in such a way that it selectively forwards some messages and drops others.

c) Sinkhole

In a sinkhole attack, an attacker makes a compromised node look more attractive to its neighbours by forging the routing information. The result is that the neighbour nodes choose the compromised node as the next-hop node to route their data through. This type of attack makes selective forwarding very simple as all traffic from a large area in the network would flow through the compromised node.

d) Sybil attack

Sybil attack is defined as a “malicious device illegitimately taking on multiple identities”. Using the Sybil attack, an adversary can “be in more than one place at once” as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, disparity and multipath.

e) Wormhole

In the wormhole attack, an adversary tunnels messages received in one part of the network over a low latency link and replays them in a different part. An adversary situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An adversary could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole.

f) Blackhole and Grayhole

In the blackhole attack, a malicious node falsely advertises good paths (e.g., the shortest path or the most stable path) to the destination node during the path-finding process (in reactive routing protocols) or in the route update messages (in proactive routing protocols). A more delicate form of this attack is known as the grayhole attack, where the malicious node intermittently drops data packets thereby making its detection more difficult.

g) Hello Flood

Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbours, and a node receiving such a packet may assume that it is within (normal) radio range of the sender. An attacker may use a high-powered transmitter to fool a large number of nodes and make them believe that they are within its neighbourhood.

h) Acknowledgment spoofing

Some routing algorithms for WSNs require transmission of acknowledgment packets. An attacking node may overhear packet transmissions from its neighbouring nodes and spoof the acknowledgments thereby providing false information to the nodes.

5.1.4 Transport layer attacks

The attacks that can be launched on the transport layer in a WSN are flooding attack and de-synchronization attack.

a) Flooding

Whenever a protocol is required to maintain state at either end of a connection, it becomes vulnerable to memory exhaustion through flooding. An attacker may repeatedly make new connection request until the resources required by each connection are exhausted or reach a maximum limit. In either case, further legitimate requests will be ignored.

b) De-synchronization

It refers to the disruption of an existing connection. An attacker may, repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist.

5.2 Attacks on secrecy and authentication:

There are different types of attacks under this category.

5.2.1 Node replication attack

In a node replication attack, an attacker attempts to add a node to an existing WSN by replication (i.e. copying) the node identifier of an already existing node in the network. Such node can potentially cause severe disruption in message communication in the WSN by corrupting and forwarding the packets in wrong routes. This may also lead to network partitioning and communication of false sensor readings.

5.2.2 Attacks on privacy

Privacy preservation of sensitive data in a WSN is particularly difficult challenge. An adversary may gather seemingly innocuous data to derive sensitive information if he knows how to aggregate data collected from multiple sensor nodes. The privacy preservation in WSNs is even more challenging since these networks make large volumes of information easily available through remote access mechanisms. Some of the common attacks on sensor data privacy are

a) Eavesdropping and passive monitoring.
b) Traffic analysis
c) Camouflage

It may be noted that WSNs are vulnerable to a number of attacks at all layers of the TCP/IP protocol stack. However, there may be other types of attacks possible which are not yet identified. Securing a WSN against all these attacks may be a quite challenging task.

6.0 Counter Measures

6.1 Outsider attacks and link layer security

The majority of outsider attacks against sensor network routing protocols can be prevented by simple link layer encryption and authentication using a globally shared key.

6.2 The Sybil attacks

An insider cannot be prevented from participating in the network, but one should only be able to do so using the identities of the nodes one has compromised. Using a globally shared key allows an insider to masquerade as any (possibly even non-existent) node. In the traditional setting, identities are verified using public key cryptography, but generating and verifying digital signatures is beyond the capabilities of sensor nodes. When a node is compromised, it is restricted to communicating only with its verified neighbours. This is not to say that nodes are forbidden from sending messages to base stations or aggregation points multiple hops away, but they are restricted from using any node except their verified neighbours to do so.

6.3 HELLO flood attacks

The simplest defense against HELLO flood attacks is to verify the bi directionality of a link before taking meaningful action based on a message received over that link. The identity verification protocol is sufficient to prevent HELLO flood attacks.

6.4 Wormhole and Sinkhole attacks

Wormholes are hard to detect because they use a private, out of-band channel invisible to the underlying sensor network. Sinkholes are difficult to defend against in protocols that use advertised information such as remaining energy or an estimate of end-to-end reliability to construct a routing topology because this information is hard to verify. Routes that minimize the hop-count to a base station are easier to verify, however hop-count can be completely misrepresented through a wormhole. When routes are established simply based on the reception of a packet as in Tiny OS beaconing or directed diffusion, sinkholes are easy to create because there is no information for a defender to verify.

6.5 Leveraging Global Knowledge

A significant challenge in securing large sensor networks is their inherent self-organizing, decentralized nature. When the network size is limited or the topology is well structured or controlled, global knowledge can be leveraged in security mechanisms.

6.6 Selective forwarding

Even in protocols completely resistant to sinkholes, wormholes, and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or a base station. Multipath routing can be used to counter these types of selective forwarding attacks. Messages routed over paths whose nodes are completely disjoint are completely protected against selective forwarding attacks involving at most compromised nodes and still offer some probabilistic protection whenever nodes are compromised.

6.7 Authenticated broadcast and flooding

If we have base stations trustworthy, adversaries must not be able to spoof broadcast or flooded messages from any base station. This requires some level of asymmetry: since every node in the network can potentially be compromised, no node should be able to spoof messages from a base station, yet every node should be able to verify them. Proposals for authenticated broadcast intended for use in a more conventional setting either use digital signatures and/or have packet overhead that well exceed the length of typical sensor network packet. TESLA is a protocol for efficient, authenticated broadcast and flooding that uses only symmetric key cryptography and requires minimal packet overhead. SPIN and gossiping algorithms are techniques to reduce the messaging costs and collisions which still achieve robust probabilistic dissemination of messages to every node in the network.

6.8 OSI Layer wise threats and countermeasures

In this section, we discuss some of the known threats and countermeasures classifying in different OSI layers.

Physical Layer: In Table 1, we describe Physical Layer Threats & Countermeasures in case of Wireless Sensor Network.

Table 1. Physical Layer Threats and Countermeasures

Threat	Countermeasure
Interference	Channel hopping and Blacklisting
Jamming	Channel hopping and Blacklisting
Sybil	Physical Protection of devices
Tampering	Protection and Changing of key

Data-link Layer: In Table 2, we describe Data-Link Layer Threats & Countermeasures in case of Wireless Sensor Network.

Table 2. Data-link Layer Threats and Countermeasure

Threat	Countermeasure
Collision	CRC and Time diversity
Exhaustion	Protection of Network ID and other information that is required to joining device
Spoofing	Use different path for re-sending the message
Sybil	Regularly changing of key
De-synchroni-zation	Using different neighbors for time synchronization

Threat	Countermeasure
Traffic analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network
Eavesdropping	Key protects DLPDU from Eavesdropper

Network Layer: In Table 3, we describe Network Layer Threats & Countermeasures in case of Wireless Sensor Network.

Table 3. Network Layer Threats and Countermeasures

Threat	Countermeasure
Wormhole	Physical monitoring of Field devices and regular monitoring of network using Source Routing. Monitoring system may use Packet Leach techniques
Selective forwarding	Regular network monitoring using Source Routing
DoS	Protection of network specific data like Network ID etc. Physical protection and inspection of network.
Sybil	Resetting of devices and changing of session keys
Traffic Analysis	Sending of dummy packet in quite hours; and regular monitoring WSN network.
Eavesdropping	Session keys protect NPDU from Eavesdroppers.

7.0 Conclusion and way forward

Although research efforts have been made on cryptography, key management, secure routing, secure data aggregation, and intrusion detection in WSNs, there are still some challenges to be addressed. First, the selection of the appropriate cryptographic methods depends on the processing capability of sensor nodes, indicating that there is no unified solution for all sensor networks. Instead, the security mechanisms are highly application-specific. Second, sensors are characterized by the constraints on energy, computation capability, memory, and communication bandwidth. The design of security services in WSNs must satisfy these constraints. Third, most of the current protocols assume that the sensor nodes and the base station are stationary. However, there may be situations, such as battlefield environments, where the base station and possibly the sensors need to be mobile.

[Prepared by Smart Network Division, TEC]

हिंदी पखवाड़ा–2019

दूरसंचार अभियांत्रिकी केंद्र, नई दिल्ली में 13 से 27 सितंबर, 2019 तक हिंदी पखवाड़े का आयोजन सफलतापूर्वक एवं उत्साहपूर्वक किया गया। हिंदी पखवाड़े का शुभारंभ श्री अनिल कुमार संघी, सलाहकार, टी.ई.सी. द्वारा दीप प्रज्वलित कर किया गया। इस अवसर पर श्री संघी साहब द्वारा माननीय गृह मंत्री जी का संदेश पढ़कर सुनाया गया। हिंदी पखवाड़े के दौरान कुल 10 प्रतियोगिताओं का आयोजन किया गया। पखवाड़े के दौरान आयोजित प्रतियोगिताओं में अधिकारियों/ कर्मचारियों ने बढ़–चढ़कर भाग लिया।

हिन्दी पखवाड़े का शुभारंभ

हिन्दी पखवाड़े के दौरान सरस्वती वंदना करते हुए

हिंदी पखवाड़े का समापन समारोह श्री अनिल कुमार संघी, सलाहकार, टी.ई.सी. की अध्यक्षता में सम्पन्न हुआ जिसमें सभी विजेताओं को पुरस्कार राशि एवं प्रमाण–पत्र प्रदान किए गए। उन्होंने सभी उपस्थित अधिकारियों/कर्मचारियों को हिंदी के प्रचार–प्रसार हेतु अधिक से अधिक योगदान करने के लिए प्रेरित किया।

हिन्दी पखवाड़े में सलाहकार, टी.ई.सी. सम्बोधन करते हुए

हिन्दी कार्यशाला में उपस्थित अधिकारी/कर्मचारी गण

Activities at NTIPRIT (JUL-19 to SEP-19)

1. Foundation Course for ITS-2016 and P&T BWS-2016 batch Officer Trainees at HIPA Gurugram Haryana:

As part of Induction Training, Officer Trainees of ITS-2016 were deputed to attend 15 weeks Foundation Course at HIPA, Gurugram. The officer trainees of P&T BWS-2016 batch also joined the Foundation Course which was inaugurated on 29.07.2019 by Director General, HIPA, Gurugram and Sh. Anil Kumar Sanghi, Sr. DDG, NTIPRIT, Ghaziabad. The inaugural function was followed by group photograph and lunch. Mrs. V Sobhana, DDG (Training) was present during the event.

Goup Photograph of ITS-2016 and P&T BWS-2016 batch with faculties of NTIPRIT and HIPA on Inaugural Day of Foundation course at HIPA, Gurugram

2. Valedictory Module of ITS-2015 batch

After completion of 15 weeks Foundation course at HIPA, Gurugram, the Officers of ITS-2015 batch joined back to NTIPRIT to attained 1-week valedictory module. Sh. Anil Kumar Sanghi, Advisor, NTIPRIT blessed the occasion by motivating the young officers for future endeavors.

Goup Photograph of ITS-2015 batch with faculties of NTIPRIT on the occation of Valedictory Programme

3. In-Service Course on 'Cyber and Network Security' (26.09.2019 to 27.09.2019)

Two days In-Service course on 'Cyber and Network Security' was conducted by NTIPRIT at Hotel Citrus, RDC, Ghaziabad. During the course the experts from government organizations and private agencies were invited to deliver the lectures and share the experiences. 26 Officers from various LSAs had attended the course.

4. ITEC Course on 'ICT in Disaster Management' (02.09.2019 to 13.09.2019)

Two weeks ITEC course on 'ICT in Disaster Management' was conducted by NTIPRIT at CDTI, Ghaziabad. Total 14 participants from 10 countries participated in this course. During the course the officers were given the exposure of live Demo of rescue during disaster by NDRF team. During the course the experts from government organizations were invited to deliver the lectures and share the experiences. The participants also visited Delhi and Agra as the part of cultural visit to India.

5. Induction Training of the following batches of Officer Trainees of ITS/BWS probationers was conducted during the period

i. ITS-2015 batch (33 officers)

ii. ITS-2016 batch (34 officers)

iii. BWS-2016 batch (3 Officers)

v. BWS-2017 batch (2 Officers)

vi. ITS-2018 batch (15 Officers)

vii. JTO-2016 batch (1 Officer)

viii. JTO-2018 batch (10 Officers)

Various training programs like technical modules, BSNL/MTNL attachment, were conducted during this period as per respective training calendar.

6. In-service training courses for DoT Officers were conducted at NTIPRIT on the following topics

i. In-Service course on "Cyber and Network Security" (26-27 September, 2019) [26 Participants]

Approvals from JUL-19 to SEP-19

Sl. No.	Name of the Manufacturer/Trader & Name of Product & Model No.
A	M/s.Progility Technologies Pvt. Ltd.
1	PABX For Network Connectivity, OpenScape Business X5
2	PABX For Network Connectivity, OpenScape Business X8
B	M/s MVD Technologies Pvt. Ltd.
3	PABX For Network Connectivity, Mivoice MX-one
C	NxValue Solutions India Pvt. Ltd.
4	Group 3 Fax Machine/Card, SEOLA-1906-00
D	M/s Fibcom India Ltd.
5	STM-4 Synchronous Multiplexer for TM, ADM & Multi-ADM (M-ADM) Applications, Fibcom 6325 Edge Node
6	STM-4 Synchronous Multiplexer for TM, ADM & Multi-ADM (M-ADM) Applications, Fibcom 6335 Switch Node
E	C-DOT (Centre for Development of Telematics)
7	High Speed Wi-Fi Access Point (HAP), HAP2S

Important Activities of TEC during JUL 19 to SEP 19

Brief About TEC

Telecommunication Engineering Centre (TEC) functions under Department of Telecommunications (DOT), Government of India. Its activities include:

- Issue of Generic Requirements (GR), Interface Requirements (IR), Service Requirements (SR) and Standards for Telecom Products and Services
- Field evaluation of products and Systems
- National Fundamental Plans
- Support to DOT on technology issues
- Testing & Certification of Telecom products

For the purpose of testing, four Regional Telecom Engineering Centers (RTECs) have been established which are located at New Delhi, Bangalore, Mumbai, and Kolkata.

For more information visit TEC website www.tec.gov.in

GRs/IRs/SDs/ERs issued

- GR on VRLA batteries for high rate of discharge (UPS application)
- GR on SHDSL system
- GR on OTDR Type-1, OTDR(mini)
- GR on double walled corrugated HDPE ducts (DWC)
- GR on Permanently lubricated HDPE telecom ducts for use as underground optical fibre cable conduits

DCC/Sub DCC meeting conducted for:

- GR on IDMS
- GR on Media Server
- GR on Signalling Gateway

Contributions submitted to ITU-T/R/D

- 2 contributions were presented in ITU-T SG-17 meeting
  - Suggestion for inclusion in X.STR.DLT security threats in digital payment services using Distributed ledger technology
  - Suggestion for inclusion in Security guidelines for V2 X communication system for determination.
- The contribution on X.str-dlt was accepted as TD.2360 and India was made Editor of this Work item. India is also made editor of one more contribution on X. GCSDLT related to Security management controls for distributed Ledger technology.

Meeting/Seminar/Workshop attended by TEC officials:

- ITU–T SG-5, SG-15, SG-17 meetings were held at Geneva
- Meeting on 3GPP SA6#33 at Sophia Antipolis, France
- LITD11 external meeting organised by BIS, New Delhi
- TEC speakers made presentations in CDoT one M2M event on 26-08-2019 and one M2M industry day event at Hyderabad on 25-09-2019
- A delegation headed by Advisor, TEC visited Samsung and Nasscomm IoT CoE at Gurgaon on 4th July 2019. Delegation was having members from TEC and C-DOT.

Presentation/Training/Seminar/Workshop organised by TEC

- Presentations on the topics '5G transport carrier', 'Next Generation Optical Transport Technologies' & 'Overview of FTTH and PON Technologies' in NTIPRIT, Ghaziabad was given by TEC officers.
- One-day training programme on "IoT Standardization: oneM2M and OCF" was arranged as a capacity building measures for the members of Consultative committee formed for adoption of oneM2M Rel 2 standards transposed by TSDSI, having speakers from India and abroad, with remote participation also, TEC New Delhi, 5th August 2019.
- Two days training programme on IoT & 5G was designed and conducted by TEC with industry experts for ITI executives, Rae Bareli during 1-2 July 2019.
- A Seminar on IEEE document download process was held in TEC in July 2019
- Interaction workshop with Startups in 5G was organised in TEC.
- A presentation on Interoperable Setup Box was given by M/s CDoT in TEC.

Other Important Activities

- Meetings of NWG-5, NSG-5, NWG-11, NWG-12, NWG-13, NWG-15, NWG-16 & NWG-17 were held in TEC
- ISO 9001:2015 Certification granted to TEC
- 10 Labs were designated as CAB of TEC & total CABs 54 nos.
- TEC has been assigned the reviewer of Ready logo results of Asia pacific region. IPv6 ready logo certificate has been assigned to 29 devices based on review done on IPv6 ready logo lab. HP Xerox_B215 has been awarded IPv6 ready logo certificate based on testing done on IPv6 ready logo set up.

Suggestions/feedback are welcomed, if any for further improvement.

टी ई सी संचारिका : दूरसंचार अभियांत्रिकी केन्द्र
अक्तूबर 2019 : खुर्शीद लाल भवन
भाग 23 : जनपथ
अंक 4 : नई दिल्ली–110001

Editor : Ram Lal Bharti, DDG (NGS) Phone : 23329354 Fax : 23318724 E-mail : ddgs.tec@gov.in

Printed at : Yugantar Prakashan Pvt. Ltd., New Delhi; M: 9811349619