India Smart Grid Forum

ISGF White Paper

M2M Communications in the Indian Power Sector

Abstract

The objective of this Paper is to provide a high level summary of the current scenario of M2M communications in the Indian power sector. The Telecommunications Engineering Centre (TEC) may send the recommendations mentioned in this report to the Department of Telecommunications (DoT) for expediting the use of M2M communications in India. TEC has formed five working groups on M2M communications, namely, M2M Power, M2M Health, M2M Automotive, M2M Surveillance, and M2M Architecture and Gateway. This document comes under the purview of the M2M Power working group which is focussing on establishing a framework for M2M communications in the Indian power sector.

Disclaimer

The information and opinions in this document were prepared by India Smart Grid Forum (ISGF). ISGF has no obligation to communicate with all or any readers of this document when opinions or information in this document change. We make every effort to use reliable and comprehensive information but we do not claim that it is accurate or complete. In no event shall ISGF or its members be liable for any damages, expenses, loss of data, opportunity or profit caused by the use of the material or contents of this document.

Author

Hem Thukral – Research Officer
Reji Kumar Pillai – President

India Smart Grid Forum (ISGF)
CBIP Building, Malcha Marg
New Delhi, India
www.indiasmartgrid.org

About India Smart Grid Forum

India Smart Grid Forum (ISGF) is a public private non-partisan initiative of the Ministry of Power (MoP), Government of India for accelerated development of smart grid technologies in the Indian power sector. ISGF was set up in 2010 to provide a mechanism through which academia, industry; utilities and other stakeholders could participate in the development of Indian smart grid systems and provide relevant inputs to the government's decision making.

Table of Contents

Abbreviations 2
1. Introduction 3
2. Objective 3
3. M2M communication in the Indian Power Sector 3
3.1 Current Scenario 3
3.3.1 Applications in the power sector 3
3.3.2 Challenges 3
3.2 Possible solutions and recommendations 4
3.2.1 Low-power RF 4
3.2.2 Wi-Fi 6
3.3.3 Power Line Communications (PLC) 6
3.3.4 Architecture for AMI 7
3.3 Cyber-physical security 8
4. References 9

Abbreviations

M2M – Machine-to-Machine
IoT – Internet of Things
DoT – Department of Telecommunications
TEC – Telecommunications Engineering Centre
ISGF – India Smart Grid Forum
AMI – Advanced Metering Infrastructure
AMR – Automatic Meter Reading
PMU – Phasor Measurement Unit
PDC – Phasor Data Concentrator
IED – Intelligent Electronic Device
GSM – Global System for Mobile communications
CDMA – Code Division Multiple Access
DGQA – Directorate General Quality Assurance
SCADA – Supervisory Control And Data Acquisition
RFC – Request For Comments
IPv6 – Internet Protocol version 6
6LoWPAN – IPv6 over Low Power Wireless Personal Area Network
TCO – Total Cost of Ownership
PLC – Power Line Communications
TWACS – Two Way Advanced Communications System
IEEE – Institute of Electrical and Electronic Engineers
IEC – International Electrotechnical Commission
ITU – International Telecommunication Union
CENELEC - European Committee for Electrotechnical Standardization
R-APDRP – Restructured Accelerated Power Development and Reforms Program
BIS – Bureau of Indian Standards
WPA – Wi-Fi Protected Access
NCIIPC – National Critical Information Infrastructure Protection Centre

1. Introduction

Machine-to-Machine (M2M) communications is an emerging area in the field of telecommunications in which devices are capable of communicating with each other and/or to a control centre. This will enable the Internet of Things (IoT) initiative that the world has already embarked upon. In the year 2000, there were 6 billion humans living on Earth and 500 million devices connected to the internet. In 2011, the number of devices connected to the internet was almost twice the number of humans. It is predicted that by 2020, there will be 50 billion connected devices for only 7.6 billion humans[1]. This would create a global market of about USD 4.5 trillion[2].

2. Objective

The objective of this report is to provide the Telecommunications Engineering Centre (TEC)[3] a high level summary of the current scenario of M2M communications in the Indian power sector. TEC may send the recommendations mentioned in this report to the Department of Telecommunications (DoT) for expediting the use of M2M communications in India.

TEC has formed five working groups in the M2M domain, namely, M2M Power, M2M Health, M2M Automotive, M2M Surveillance, and M2M Architecture and Gateway. As part of activities under the purview of the M2M Power working group, ISGF has taken this initiative to summarize the state of affairs.

3. M2M communication in the Indian Power Sector

3.1 Current Scenario

3.3.1 Applications in the power sector

Today the Indian power sector is at a transformational phase. The traditional grid is being revamped to a smart grid and communication will serve as a backbone. Smart meters along with numerous Intelligent Electronic Devices (IEDs) will be used in the following areas in the Indian power sector:

- Automatic Meter Reading (AMR)
- Advanced Metering Infrastructure (AMI)
- Mini pillars
- SCADA/EMS (Supervisory Control and Data Acquisition/Energy Management System) for TRANSCOS
- SCADA/DMS (Supervisory Control and Data Acquisition/Distribution Management System) for DISCOMS
- Wide Area Monitoring System (using PMUs)
- Substation Automation
- Distributed Generation
- Electric Vehicles
- Energy Storage
- Microgrids
- Demand Response
- Home/Building Automation

[1] http://www.alexandra.dk/uk/expertise/publications/documents/iot_comic_book.pdf

[2] Machine-to-Machine: Vision 2020 – Is India ready to seize a USD 4.5 trillion M2M opportunity? By Deloitte, Confederation of Indian Industry (CII) and MIT School of Telecom Management (MITSOT)

[3] TEC is a unit under DoT

3.3.2 Challenges

The following are the challenges associated with M2M communications in the Indian power sector in the current scenario:

- Limited bandwidth
- High latency
- No/limited availability
- Low reliability
- Low level of information security
- Limited scalability
- Limited range
- High power consumption
- Short technology life-cycle
- Not compliant with regulations
- Not interoperable
- High Cost of Ownership (TCO)
    - Cost of infrastructure acquisition
    - Cost of communications media acquisition
    - Operating cost

Many technologies are available in India for a variety of applications. However, the selection of a technology will depend on the criticality of the application for which it is being used. For example,

- For mission critical applications (such as Distribution Automation and Substation Automation), security, latency and reliability will be the key. Cost will be of least priority during selection.
- For non-critical applications (such as AMI), cost will be decisive.

3.2 Possible solutions and recommendations

The following gives an insight into the various communication technologies that could be used in the M2M domain in the Indian power sector:

3.2.1 Low-power RF

Low-power RF technologies are used for providing last mile connectivity. Devices that operate on these technologies consume low power, have less processing capabilities and storage, and offer a low data rate/throughput.

3.2.1.1 Choice of frequency band

Selecting the frequency band is of utmost importance. The sub-GHz frequency bands offer compelling advantages as compared to other (higher) frequency bands. These include (but are not limited to) the following:

- Long range
  Range is inversely proportional to frequency and hence the range offered by sub-GHz bands is much more than that provided by the higher frequency bands.
- High signal-to-noise ratio because of low interference
  The 2.4-2.483 GHz band is used by Wi-Fi and Bluetooth devices, microwave ovens, cordless phones etc. This has increased the traffic in this band and hence interference is a serious issue. The sub-GHz bands are much less congested and hence offer enhanced quality of service.

- Low power consumption
  Since the power dissipation is directly proportional to frequency of operation, a device operating in sub-GHz bands will consume less power.
- Deep penetration
  Since low frequency signals are reflected to a lesser extent, signals in the sub-GHz penetrate deeper into thick walls.
- Low Total Cost of Ownership (TCO)
  Since sub-GHz bands offer a higher range, less number of repeaters/concentrators are needed. Hence the TCO is lower when sub-GHz bands are used.

ZigBee is a technology that provides wireless connectivity over short distances. However, it offers certain limitations such as:

- Larger size of the complete stack (64 KB as compared to 30 KB in 6LoWPAN)
- Not interoperable with devices on other communication networks
- The new ZigBee protocol works on 910 MHz and cannot be adopted in India as that spectrum is for 2G cellular operators.
- Need a middleware for translation for interacting with IP-based networks
- Not very reliable for FAN/NAN in areas with thick vegetation, rainfall, etc.

Recommendations

The existing 865-867 MHz band would not be sufficient to cater to the needs of millions of smart meters and IEDs present in the smart grid. Also, the Internet of Things in which billions of devices would be connected to the internet would hog this 2MHz band. For the power sector, we could consider using the 433-434 MHz band[4] which was un-licenced in September 2012. As per the technical specifications of this frequency band, the maximum effective radiated power should be less than 10mW in a channel bandwidth of 10KHz. **DoT/TEC is requested to issue clarifications on the use of the 433-434 MHz frequency band**.

Since DoT has mandated all electronic devices capable of communications to be based on IPv6, 6LoWPAN (IPv6 over Low Power Wireless Personal Area Network) is touted as the technology of the future (for providing wireless links), as it is scalable, interoperable, based on open and has a smaller stack size as compared to other technologies. Other advantages include (but are not limited to):

- Ubiquitous: end-to-end IP solution
- Universal availability of IP technology
- Versatile, future proof with easy learning curves, stable and resilient
- Easy Network maintainability (Tools for managing, commissioning and diagnosing IP-based networks already exists)
- Capable of managing multiple applications from a single network view
- Globally deployed by many leading utilities for smart grid applications. It features in the road-map of many utilities.

[4] http://www.bureauveritas-adt.com/news.php?KindID=2&ID=142

3.2.2 Wi-Fi

Wi-Fi is best suited for in-home communications because of its limited coverage. However, it offers inadequate network security. According to the DGQA (Directorate General Quality Assurance) policy (2014 version) for cyber security[5] released by the Ministry of Defence, use of Wi-Fi is banned as it offers feeble security. If access is allowed via the Pre-Shared Key (PSK) option along with the WPA2 protocol, the network would be considerably secure as compared to other options used in Wi-Fi routers. Also, Wi-Fi offers a very low latency, hence could be used in latency-critical applications such as Demand Response.

Recommendations

The use of Wi-Fi needs to be abolished in critical applications where information security is of top priority. However, in other applications, the WPA2 protocol with access using Pre-Shared Key option should be used for achieving a considerable level of security provided the access points are configured properly and a strong passphrase is used.

3.3.3 Power Line Communications (PLC)

PLC technology is at a nascent stage in India. It can be used for providing last mile connectivity as well as for creating a wide area network. A key requirement of this technology is the existence of a clean network of cables for carrying information. Issues such as noise generated by different loads on the power line, dynamic changes in the line impedance and absence of trained man-power capable of bespoke engineering are some of the issues that will need to be addressed in order to make this technology ready to use.

In addition to the above mentioned, there needs to be a frequency band allocated for PLC communications.

Globally, IEEE 1901.2-2013[6], PRIME, G3-PLC, ITU-T G.hnem[7], IEC 61334, TWACS, Meters&More and HomePlug C&C are some of the popular standards/protocols available for implementing **Narrowband PLC** systems.

The following table throws more light into the technical details:

Standard/Protocol	Frequency band	Maximum data rate
IEEE 1901.2 - 2013	<500 KHz	500 Kbps
PRIME	42-89 KHz	128.6 Kbps
G3-PLC	35-91 KHz	33.4 Kbps
ITU-T G.hnem	10-490 KHz	1 Mbps
IEC 61334	60-76 KHz	Upto 2.4 Kbps
TWACS	200-600 Hz	100 bps
Meters&More	3-148.5 KHz	28.8 Kbps (nominal) and 4.8 Kbps (effective)
HomePlug C&C	10-450 KHz	7.5 Kbps

[5] http://www.dgqadefence.gov.in//documents/pdf/DGQA-CYBER-SECURITY-POLICY-2014.pdf
[6] http://standards.ieee.org/findstds/standard/1901.2-2013.html

[7] Developed by ITU-T:
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6094004&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6094004

For **Broadband PLC** systems, IEEE 1901-2010, HomePlug Green PHY and ITU-T G.hn (G.9960/G.9961) are some of the popular technologies used globally.

The following table throws more light into the technical details:

Standard/Protocol	Frequency band	Maximum data rate
IEEE 1901-2010	< 100 MHz	> 100 Mbps
HomePlug Green PHY	2-30 MHz	10 Mbps
ITU-T G.hn (G.9960/G.9961)	25-200 MHz	2 Gbps

Europe, USA, Japan and China are some examples of regions where frequency bands have been allocated for PLC communications. The following table mentions the regions and frequency bands allocated for PLC:

Region	Frequency band for PLC
Europe	CENELEC A: 3-95 KHz for power utilities CENELEC B: 95-125 KHz for any application CENELEC C: 125-140 KHz for in-home networking with mandatory CSMA/CA protocol CENELEC D: 140-148.5 KHz Alarm and Security systems
USA	10-490 KHz, and 2-30 MHz
Japan	10-450 KHz
China	3-500 KHz

Recommendations

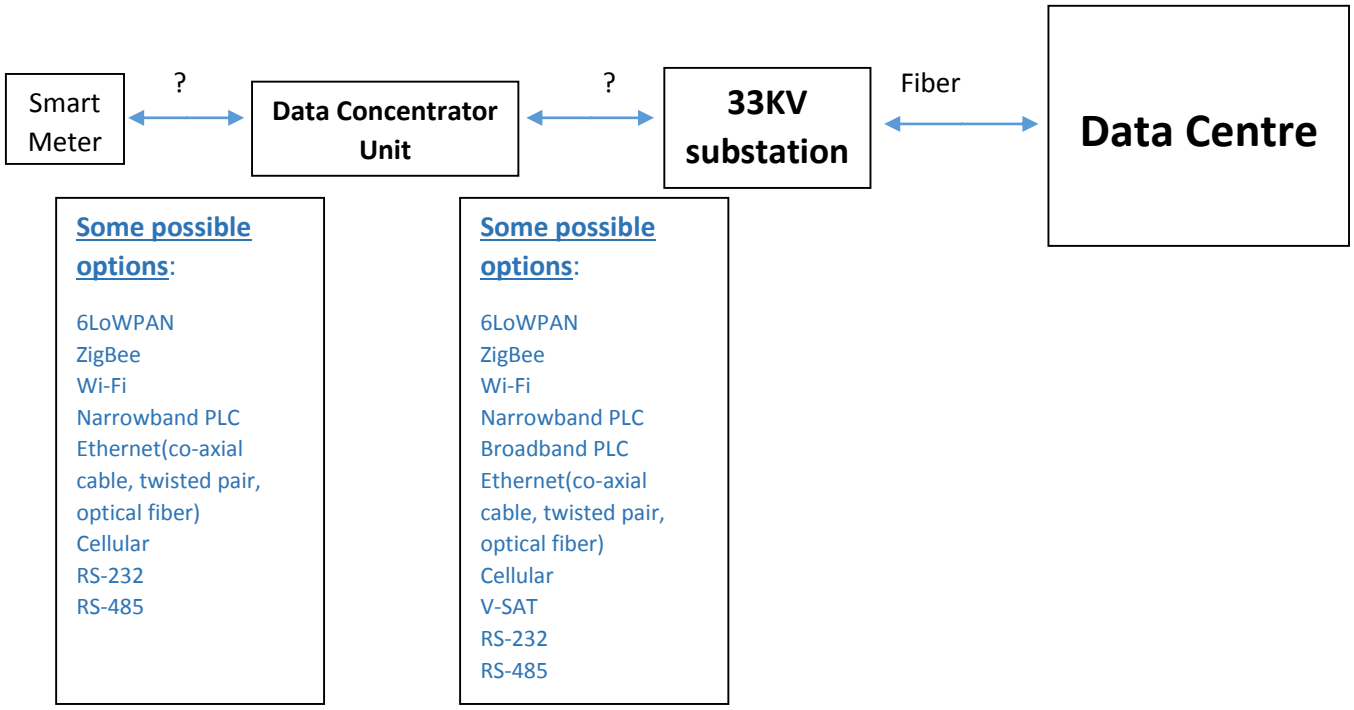
There is an urgent need to allocate frequency bands for narrowband and broadband PLC communications. The above mentioned frequency bands and standards need to be studied and reviewed for adoption (with or without modification) in India.

3.3.4 Architecture for AMI

With the National Optical Fibre Network (NOFN) envisaging to connect all 33KV substations using optical fiber, reliable wide area connectivity can be achieved using these fiber links. The DCUs could send meter data to these 33KV substations using any of the available technologies.

Recommendations

It is recommended to study the following architecture for adoption in India for AMI:



For the communications between smart meters, DCUs and 33 KV substations, the results of the pilots would give India a clear picture regarding the technologies that need to be selected for large scale roll out. From the 33KV substations to the data centre, the optical fiber links provided by NOFN would provide reliable wide area connectivity.

3.3 Cyber-physical security

Protection of the critical infrastructure is the primary objective of any nation and the power sector is of top priority. A smart grid is a superposition of the information infrastructure over the electrical infrastructure. With this convergence of the electrical technologies, information technologies and operational technologies, security of industrial control systems has become extremely important. The reliability of the power system infrastructure is directly decided by the security of the information infrastructure.

ISGF, in collaboration with NCIIPC, is in the process of implementing a survey-based project, 'ISGF-NCIIPC Cyber Security Assessment Project' wherein 15 Utilities (Generation, Transmission and Distribution) have been identified as participants. This is a unique research project to assess the cyber security readiness amongst the Indian Utilities. Obtaining realistic understanding of the cyber security challenges and raising awareness amongst the stakeholders are the key objectives of this project. The assessment will be informal in nature as the intention is not to formally audit and certify for compliance but to benchmark for assessing cyber security preparedness. The assessment domains comprise Asset Management, Management Controls, Personnel and Training, Physical Security, Network Security, Systems Security, Incident Response, Backup and Recovery, and Audit and Compliance. After the completion of the survey, a consolidated report containing guidelines will be published for the benefit of the entire country which will not include individual findings. In addition, each organization taking part in the survey, will be provided with their own copy of cyber security gap analysis report.

Recommendations

The BIS standard, IS 3292 – Security Standard for Power Control Systems (currently in RFC stage) focusses on IT security and it is recommended to comply with this standard once this is released.

Utilities need to appoint a Chief Information Security Officer (CISO) which would oversee the hardware and software inventory not just as book keeping exercise, but identify the ownership and operation after ensuring accountability within the organisation. Some utilities have appointed a CISO and others are following suit.

Identification of the cyber security posture of the organisation is something that Utilities need to do on a priority basis in order to plug the loopholes. In addition to a regular cyber security audit, performing a vulnerability, threat and risk analysis is extremely important. This is only possible if the Utility has a sound cyber security policy, which would act as yard-stick against which the audit will take place. Having a 'sectoral' regulator and 'sectoral' incident sharing would be highly beneficial for enforcing regulations and raising awareness amongst the 'sector'. For this, it is imperative to define and identify 'sectors' – as per region/area, Utility (Generation, Transmission or Distribution), energy domains (power, gas, water) or so. Insuring the Utility against cyber-physical attacks might just be the long term solution that is required for the protection of the industrial control systems.

4. References

1. http://www.alexandra.dk/uk/expertise/publications/documents/iot_comic_book.pdf
2. Machine-to-Machine: Vision 2020 – Is India ready to seize a USD 4.5 trillion M2M opportunity? By Deloitte, Confederation of Indian Industry (CII) and MIT School of Telecom Management (MITSOT)
3. http://www.bureauveritas-adt.com/news.php?KindID=2&ID=142
4. http://www.dgqadefence.gov.in//documents/pdf/DGQA-CYBER-SECURITY-POLICY-2014.pdf
5. http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6094004&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6094004
6. http://standards.ieee.org/findstds/standard/1901.2-2013.html
7. http://webstore.iec.ch/preview/info_iec61334-5-1%7Bed2.0%7Db.pdf
8. http://orbit.dtu.dk/fedora/objects/orbit:75562/datastreams/file_6627132/content