Cyber Security for Intelligent World with Internet of Things and Machine to Machine Communication

Vandana Rohokale and Ramjee Prasad

Center for TeleInFrastruktur (CTIF), Aalborg University,
Aalborg, Denmark
Corresponding Authors: vmr.301075@gmail.com; Prasad@es.aau.dk

Received 5 February 2015; Accepted 25 February 2015;
Publication 22 May 2015

Abstract

The growth of interconnected objects through Internet of Things (IoT) and Machine to Machine Communication (M2M) is no doubt inevitable. The researchers have predicted that by 2020, around fifty billion objects throughout the world will be connected with each other with the help of internetwork of smart objects. With the number of networked objects, grows the number of cyber-crime threats. Forthcoming fifth generation of mobile communication will be the converged version of all the wired and wireless networking services and technologies. The heterogeneous networking approach gives rise to various cyber threats. Design of robust cyber security solutions for such heterogeneous networks with smart devices is challenging task.

Keywords: Internet of Things (IoT), Machine to Machine Communication (M2M), Cyber Security, Cybercrime, etc.

1 Evolution of Internet

Internet first generation dates back to 1970's when the Advanced Research Projects Agency Network (ARPANET) introduced first Internet service which was intended for Military, Government and Educational Institutes in United

Journal of Cyber Security, Vol. 4, 23–40.
doi: 10.13052/jcsm2245-1439.412

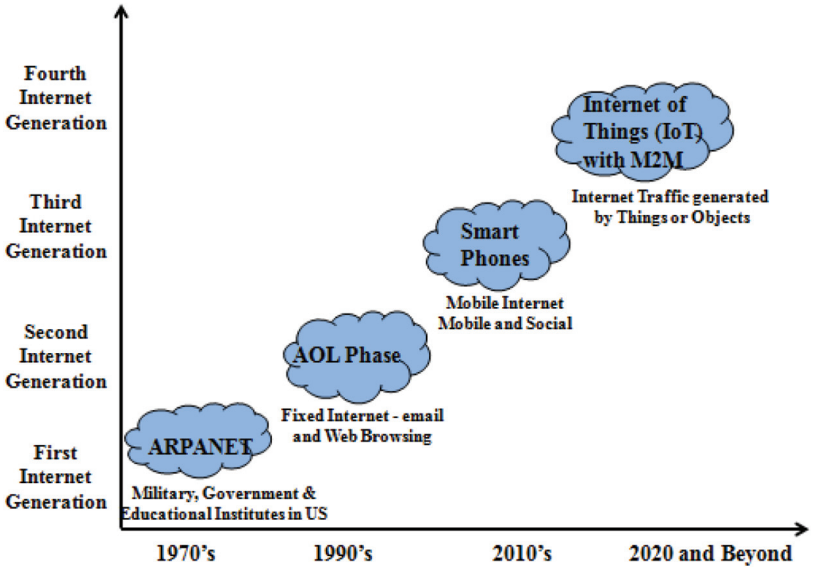
Fourth Internet Generation
Third Internet Generation
Second Internet Generation
First Internet Generation
ARPANET
Military, Government & Educational Institutes in US
AOL Phase
Fixed Internet - email and Web Browsing
Smart Phones
Mobile Internet Mobile and Social
Internet of Things (IoT) with M2M
Internet Traffic generated by Things or Objects
1970's
1990's
2010's
2020 and Beyond

Figure 1 Internet evolution from ARPANET to IoT and M2M.

States. Following that, America Online (AOL) second phase emerged which gave birth to fixed internet that facilitated email and web browsing during 1990's. Current third phase that is 2010's is the era of smart phones with mobile internet experience which is faster and better. Now the whole world is looking forward for the revolutionary fifth generation (5G) of mobile communication. Internet of Things (IoT) and Machine to Machine Communication (M2M) are the integral part of 5G. So the fourth generation of Internet is termed as Internet of Things or objects where most of the traffic will be generated by the interaction of smart objects of the physical world with the digital world [1]. Figure 1 depicts the evolution of Internet from ARPANET to IoT and M2M. On global scenario, per person at least five gadgets are considered to be networked and as a whole, the count of networked objects may go beyond 50 Billion.

2 Internet of Things (IoT) and Machine to Machine Communication (M2M)

M2M comes under the huge umbrella of IoT. There are different opinions among researchers about IoT and M2M. It is becoming the debatable question like egg first or hen first. But these two concepts are technically very much different. M2M is the communication protocol for the interactions among machines with intelligence, or machine to human interface. IoT is the networking service which enables interworking of all such smart machines. For example, credit or debit card of the bank ATM is the example of M2M because the ATM machine reads the information on the card and acts according to the requirements of user. But when user leaves the bank, automatically the fans and lights are off, which is the example of IoT where in, the human presence is detected and accordingly the electrical appliances are turned on or off. In essence, M2M is the plumbing for strong connectivity among network objects for best networking experience in IoT [2].

The Internet of Things is expansion of the current Internet services for each and every object which exists in this world or likely to exist in the coming future. As IoT has become an active research area, different methods from various points of view have been explored to promote the development and popularity of IoT [3]. One trend is viewing IoT as Web of Things where the open Web standards are supported for information sharing and device interoperation. While bringing smart things into existing web, the conventional web services are needed to be enriched and integrated with the physical world [4]. The IoT is rapidly gaining much of the attention in the scenario of modern wireless telecommunications. The basic idea of the concepts such as Radio Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc., which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbours to reach common goals [5].

Actually, many challenging issues addressed on both technological as well as social knots have to be untied before the IoT idea is widely accepted. Central issues must try to support possible interoperability of interconnected devices, providing with higher degree of smartness by enabling their adaptation and autonomous behaviour, while guaranteeing trust, privacy, and security. Also, the IoT idea poses several new problems concerning the networking aspects. In fact, the things composing the IoT will be characterized by lesser requirement of resources in terms of computation and energy capacity. Accordingly, the proposed solutions need to pay special attention to resource efficiency besides the obvious scalability problems. The Internet of Things, an emerging global Internet-based technical architecture facilitating the exchange of goods and services in global networks has an impact on the security and privacy of the involved stakeholders. Measures ensuring the architectures for data authentication, access control and client privacy need to be established.

M2M means Machine to Machine communication which is the most popular interface for Internet of Things (IoT) in the present mobile wireless communication, whose data transmission is supported by cable, wireless, mobile and other technologies, which may suffer from significant security vulnerabilities and risks. M2M is widely used in power, transportation, industrial control, retail, public services management, health, water, security and other industries. M2M is typically required to be small, inexpensive and those able to operate unattended by humans for extended periods of time and to communicate over the wireless area network. It can achieve vehicle theft security, safety monitoring, auto sales, mechanical maintenance, and public transport management, logistic and other functions. The most important part in IoT Internets is the connection and interoperability between machines, which is called M2M. Security services such as data integration, authentication and key establishment are critical in M2M [6, 7]. Figure 2 shows various machine intelligence perspectives necessary for the IoT with the help of M2M.

There are great prospects of development and applications in IoT, which can be applied in almost every aspect of human life, such as environmental

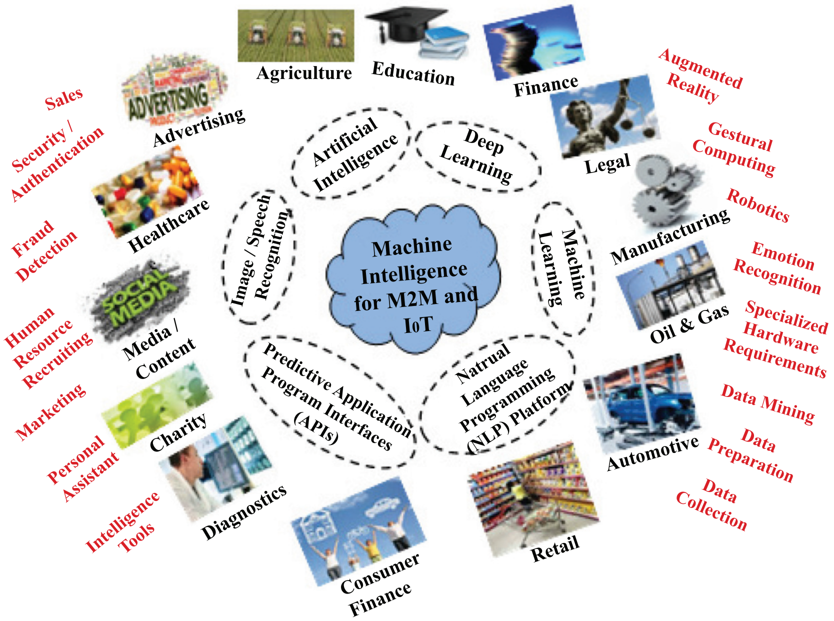

Figure 2 Machine intelligence perspectives for IoT through M2M with Cyber Security.

monitoring, medical treatment and public health, Intelligent Transportation System (ITS), smart grid and other areas. Main enabling factor for promising paradigm in the integration of several technologies and communications solutions is the IoT. Identification, sensing and monitoring technologies, wired and wireless sensor and actuator networks, enhanced communication protocols and distributed intelligence for smart objects are just the most relevant. Table 1 shows some of the recent news related to IoT and M2M Communication.

Table 1 Recent news related to IoT and M2M communications

News Headline	Description	Ref
The upcoming boom in smart buildings	After several years of slower than expected growth, the smart building sector is poised to skyrocket. IDC expects the market to triple to $21.9 billion in just four years.	[8]
Smart grid advice from SMUD (Home gateways? Really?)	SMUD's Smart Sacramento smart grid program deployed 615,000 smart meters. The AMI network also connected to home area network (HAN) devices. SMUD deployed 6,700 HAN devices. The project was funded in part by a $127.5 million grant from the Department of Energy. News Date: 2014-7-21	[9]
Smart-Grid Sensor Market Steadily Climbing to $39 Billion by 2019	The market for all types of sensors used in smart grid applications will grow from $26.4 billion this year to $36.5 billion in 2019 and nearly $46.8 billion by 2021, according to a new report from industry analyst firm NanoMarkets. News Date: 2014-9-15	[10]
Electric scooter with Smartphone connection is launched in Europe by Terra Motors	Terra Motors Corporation, Japan's manufacturer of electric two-wheelers and three-wheelers, starts commercial sale of "A4000i" in European countries, the electric scooter with smartphone connection. News Date: 2014-9-12	[11]
Smart connected homes driving IoT	The Internet of Things is set to create a market worth almost US$9 trillion by 2020. According to some analysts, a large chunk of this business will be generated by smart connected homes. Antony Savvas reports on business developments in the smart home sector. News Date: 2014-9-1	[12]
Advancing LTE migration heralds massive change in global M2M modules markets	A central element of research for this report involved extensive interviews with 20 modules manufacturers, mobile network operators,	[13]

(*Continued*)

Table 1 Continued

News Headline	Description	Ref
	M2M service providers and M2M device manufacturers in order to assess current pricing trends for the 13 most common variants of M2M modules available in the global market. News Date: 2013-12-22	
Technology migration strategies of US carriers will trigger a new era of LTE for the M2M industry	The combination of falling module pricing and the high costs of replacing legacy modules will fundamentally change the technology planning and cost analysis of long-term M2M deployments. News Date: 2013-12-18	[14]
The connected car: a US$282 billion opportunity, but who pays?	The automotive sector is probably the most exciting in M2M, particularly for mobile network operators, module vendors, and sundry others associated with cellular M2M. Machina Research forecasts that by 2022 there will be 1.5 billion automotive M2M connections globally, up from 109 million at the end of 2012. News Date: 2013-12-18	[15]
The rise of M2M/IoT Platforms highlights new commercial dynamics, and new challenges	Any potential provider of M2M/IoT Application Platform solutions must move significantly beyond this core capability in order to attract application developers and build the ecosystems necessary to gain critical mass. News Date: 2013-12-17	[16]
Berg Insight says 2.8 million patients are remotely monitored today	According to a new research report from the analyst firm Berg Insight, around 2.8 million patients worldwide were using a home monitoring service based on equipment with integrated connectivity at the end of 2012. News Date: 2013-12-15	[17]
M2M: The focus is still on people	The idea of machines speaking to machines makes some people worry that there is an impending machine age. In reality, machine-to-machine (M2M) communication is not science fiction, but science fact and, says Daryl Miller of Lantronix, human beings are being anything but left out. News Date: 2013-12-11	[18]
V2V penetration in new vehicles to reach 62% by 2027, according to ABI Research	Vehicle-to-vehicle technology based on DSRC (Dedicated Short Range Communication) using the IEEE 802.11p automotive Wi-Fi standard will gradually be introduced in new vehicles driven by mandates and/or automotive industry initiatives, resulting in a penetration rate of 61.8% by 2027. News Date: 2013-12-10	[19]

3 Security and Privacy Issues in IoT

With the existence of IoT, users will be surrounded and tracked by thousands of smart objects. Security and privacy of the user is of utmost importance. There are various issues related to these parameters such as data confidentiality and trust negotiations which are discussed below.

Dynamicity and Heterogeneity: IoT is the most diverse network where many devices will be added and removed from the network on the go. Privacy and security provision for such diverse and heterogeneous network is the great challenge.

Security for Integrated Operational World with Digital World: Control planes designed till date have not considered security provisions. But the integration of physical and digital world with internetwork connectivity demands security.

Data Security with Device Security: Lot of research work has been contributed in the direction of device security. Now is the time for data security with device security. IoT and M2M aims at communication among objects which demands data security.

Data Source Information: It is critically important to know that from where the data has originated. Knowledge about data source is very important for control, audit, manage and ultimately secure the IoT and M2M communication [27].

Data Confidentiality: Data confidentiality represents a fundamental issue in IoT scenarios, indicating the guarantee that only authorized entities can access and modify data. This is particularly relevant in the business context, whereby data may represent an asset to be protected to safeguard competitiveness and market values. In the IoT context not only users, but also authorized objects may access data. This requires addressing two important aspects: first, the definition of an access control mechanism and second, the definition of an object authentication process (with a related identity management system).

Trust negotiation: The concept of trust is used in a large number of different contexts and with diverse meanings. Trust is a complex notion about which no consensus exists in the computer and information science literature, although its importance has been widely recognized. Different definitions are possible depending on the adopted perspective. A main problem with many approaches towards trust definition is that they do not lend themselves to the establishment of metrics and evaluation methodologies.

A widely used security policies are for regulating accesses to resources and credentials that are required to satisfy such policies. Trust negotiation refers to the process of credential exchanges that allows a party requiring a service or a resource from another party to provide the necessary credentials in order to obtain the service or the resource. This definition of trust is very natural for secure knowledge management as systems may have to exchange credentials before sharing knowledge. For this reason, we base our analysis of trust issues in IoT upon it. Trust negotiation relies on peer-to-peer interactions, and consists of the iterative disclosure of digital credentials, representing statements certified by given entities, for verifying properties of their holders in order to establish mutual trust. In such an approach, access resources are possible only after a successful trust negotiation has been completed [28].

4 Security in Machine to Machine Communication

M2M devices will ultimately connect to core network services through a variety of means, from direct broadband or capillary wireless networks, to wired networks [29]. Capillary networks used by M2M systems are made of a variety of links, either wireless or wired. Network's role is to provide a more comprehensive interconnection capacity, effectiveness and economy of connection, as well as reliable quality of service. Because of the large number of nodes in M2M, it will result in denial of service attacks when data spread, since a large number of machines sending data results into network congestion. In the service network, an attacker may eavesdrop user data, signalling data and control data and unauthorized access to stored data within the system network elements, or do passive or active flowing analysis.

An attacker through the physical layer or protocol layer can interfere in the transmission of user data, signalling data or control data may use network services to impersonate legitimate users, or take advantage of posing access to legitimate users by pretending services network to access network services, to obtain unauthorized network services. To prevent unauthorized access to services in Remote Validation processes, the relying party directly assesses the validity of the device based on the evidence for the verification received. Local verification is only passive, just measuring integrity values of the loaded and started components.

Attackers often access, modify, insert, delete, or replay the user communication information by physical theft, online listening, posing as legitimate users and other means, such as the Man-in-the-Middle (MITM) attacks, which can steal or change the course of M2M communication of information between devices in the process of "intercept data-modification of data – sending data", resulting in the loss of legitimate users [30]. Typically, to obtain certain confidential information, an attacker will obtain communications data in any ways, such as the use of online listening, MITM attacks and other. Hence the data communication between M2M devices needs to be integrity and confidentiality protection, and M2M equipment should have appropriate mechanisms to accomplish this function.

An attacker may access the applications software and signing information for M2M by malware, Trojans or other means, and then replicate in other M2M devices to restore to fraudulent use of M2M identity of the user; he also can change, insert, and remove the user's communications data by a virus or malicious software. Anti-virus software applications will reduce viruses and malware damage on M2M equipment, and M2M equipment should be able to regularly update antivirus software.

Data transmission is prevented from reaching the end of service, so that the attacker is able to obtain user data, signalling data or control data though physical theft or online listening to achieve the aim for unauthorized access. To obtain the secure communication between heterogeneous network systems, we can use the existing technology on embedded chip, which provides a singularly security architecture that operates as a security service to any application. It is uniquely serialized during manufacturing. It is easy to implement and there are no certificate servers to deploy, configure or maintain [31].

Privacy is defined in the area such as [32]:

i. Storage
ii. Processing
iii. Communication
iv. Device

From security point of view, attributes mentioned below are of prime importance [33].

- Reliability refers to the fact that the service can be continued in spite of the system becoming vulnerable.
- For catastrophic systems, no security consequences are available there in nature.
- Maintainability stands for the ability of the normal system to undergo repairs and evolutions.
- Availability refers to the fact that data and systems can be accessed by authorized persons within an appropriate period of time.
- Integrity means the data or/and programs have not been modified or destroyed accidentally (e.g. transmission errors) or with malicious intent (e.g. sabotage).

Confidentiality describes the state in which sensitive information is not disclosed to unauthorized recipients. Table 2 shows existing work done in M2M security with parameters like message confidentiality, technology used, data authentication and solution for Man in the Middle Attack (MITM). A loss of confidentiality occurs when the contents of a communication or information

Table 2 M2M security state of the art

Ref. No	Existing Research	Data Integrity/ Authentication	Technology Used	Solution for Man in Middle Attack	Message Confidentiality
[1]	Internet of Things-New Security and privacy challenge	✓	Privacy enhancing technology (PET) like VPN, TLS, Onion routing	X	X
[2]	Cyber security for home user: a new way of protection through awareness enforcement	✓	E-Awareness Model used	X	✓
[3]	On the feature and challenges of security and privacy in distributed Internet of thing	✓	Cryptography algorithm	✓	X
[4]	The cyber threat landscape: challenges and future research direction	✓	Public private partnership(PPP)	X	✓
[5]	A framework for security quantification of networked machine	✓	Markov process tool used	X	✓

[6]	The evolution of M2M in IoT	✓	Store and forward, AAA services	X	X
[7]	Advancing M2M Communications Management: A Cloud-based System for Cellular Traffic Analysis	✓	Traffic management and fault tolerance technique	X	X
[8]	Large Scale Cyber-Physical Systems: Distributed Actuation, In-Network Processing and Machine-to-Machine Communications	✓	localized cooperative access, stabilization algorithm	X	X
[9]	Wireless Sensor Networking, Automation Technologies and Machine to Machine Developments on the Path to the Internet of Things	✓	Symmetric Algorithm, Hash Algorithm	X	✓

are leaked. Table 3 indicates currently available Security Provisions for IoT and M2M Communications.

5 Summary and Outlook

Next generation mobile communication will witness integration of various wired and wireless communication networks or services. IoT and M2M are going to hold maximum portion of all these wired and wireless communication networks because it has touched almost every possible field of communication. There exist security protocols for IoT and M2M communication but still new cyber-attacks are emerging every day. So cyber security solutions should

Table 3 State of the art security provisions for IoT and M2M communications

Entities	Protective Countermeasures
Consumers and end users	Guidance Provision for best practices to protect personal data and avoid problems in the mobile environment. Make the loading of applications and software permissions more intuitive and easier to understand.
Devices	Anti-malware and Anti- spam settings, Strong Authentication and Secure device connectivity.
Network-based security policies	Network operators provide numerous tools, guides and support to consumers, enterprise managers and end users to enable them to protect their information.
Authentication and controls for devices and users	Authorized access to Information Storage on mobile device system.
Cloud, networks and services	Aspects of these security solutions include consumer and enterprise applications, features for secure storage and virtual solutions and backup and disaster recovery
Security policies and risk management	Enhancements to security policies and risk management protocols; covering definitions and documentation; ongoing scans of the threat environment; and security assessments.
Monitoring and vulnerability scans	Automated periodic real time assessment of threats
Monitoring malware and cyber-threat profiles	From the cloud to Internet gateways, network servers and devices.
Wearable smart devices (watches, glasses)	Encryption, Authentication techniques
Smart Meters (information transport to utility provider)	Encryption
Home automation for convenience and protection	Encryption and VPN
Retail Near Field Communication (NFC)	Encryption, Malware security, Access controls

also grow accordingly and this is going to remain as a continuous process. Role based access control mechanisms are going to play vital roles in the robustness of the cyber security solution development for these services. Trust level based authentication mechanisms may result in the robust and secure communication.

References

[1] Georgios Tselentis, "Towards the Future Internet: A European Research Perspective", IOS Press, Netherlands, 2009.

[2] CTIA IoT White Paper, "Mobile Cybersecurity and the Internet of Things – Empowering M2M Communication", May 2014.

[3] Luigi Atzori, Antonio Iera, Giacomo Morabito, "The Internet of Things: A Survey", Elsevier 2010.

[4] Elgar Fleisch, "What is the Internet of Things? – An Economic Perspective", Auto-ID Labs White Paper WP-BIZAPP-053, January 2010.

[5] Sudha Nagesh, "Roll of Data Mining in Cyber Security" Journal of Exclusive Management Science, Vol. 2 Issue 5, pp. 2277–5684, May 2013.

[6] A. Q. Ansari, Tapasya Patki, A. B. Patki, V. Kumar, "Integrating Fuzzy Logic and Data Mining: Impact on Cyber Security", Fourth International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2007.

[7] Chen Hongsong, "Security and Trust Research in M2M System", IEEE International Conference on Vehicular Electronics and Safety (ICVES), 2011.

[8] Fibocom Perfect Wireless Experience, "The Coming Boom in Smart Buildings", http://www.fibocom.com/news/2-4-4-2-44.html

[9] Smart Grid News, "Smart grid advice from SMUD (Home gateways? Really?) http://www.smartgridnews.com/story/smart-grid-advice-smud-home-gateways-really/2014-07-21

[10] Nano Markets, "Smart-Grid Sensor Market Steadily Climbing to $39 Billion by 2019", http://nanomarkets.net/news/article/smart-grid-sensor-market-steadily-climbing-to-39-billion-by-2019-according

[11] M2M Now, Sep 12 2014, "Electric scooter with smartphone connection is launched in Europe by Terra Motors". http://news.ne2ne.com/articles/951843/electric-scooter-with-smartphone-connection-is-lau/

[12] Fibocom Perfect Wireless Experience, "Smart connected homes driving IoT". http://www.fibocom.com/news/2-4-4-2-39.html

[13] Machina Research, m2m now- Latest Machine to Machine Industry News, Connected Car Report http://www.connectedcar.org.uk/machinaltem2mnow/4586932250

[14] Machina Research, m2m now- Latest Machine to Machine Industry News http://www.m2mnow.biz/2013/10/25/16033-technology-migration-strategies-of-us-carriers-will-trigger-a-new-era-of-lte-for-the-m2m-industry/

[15] Machina Research, m2m now- Latest Machine to Machine Industry News http://www.m2mnow.biz/2013/11/26/16748-the-connected-car-a-usd282-billion-opportunity-but-who-pays/

[16] Machina Research, m2m now- Latest Machine to Machine Industry News http://www.m2mnow.biz/2013/12/13/17392-the-rise-of-m2miot-platforms-highlights-new-commercial-dynamics-and-new-challenges/

[17] Telematics Business Arena | Avlgps M2m Lbs | Fleet Management, Tracking, Rastreo, Gestion De Flotas Https://Www.Linkedin.Com/Groups/Berg-Insight-Says-28-Million-1878321.S.204554388

[18] m2m now- latest machine to machine industry news http://www.m2mnow.biz/2013/06/17/12936-m2m-the-focus-is-still-on-people/

[19] ABI Research, Technology Market Intelligence. https://www.abiresearch.com/press/v2v-penetration-in-new-vehicles-to-reach-62-by-202

[20] Yi Cheng, Mats Naslund, Goran Selander, and Eva Fogelstrom, "Privacy in Machine-to-Machine Communications", IEEE International Conference on Communication Systems (ICCS), 2012.

[21] A. Q. Ansari, Tapasya Patki, A. B. Patki, V. Kumar, "Integrating Fuzzy Logic and Data Mining: Impact on Cyber Security", Fourth International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2007.

[22] Radrigo Roman, Jianiying Zhou, "On the feature and challenges of security and privacy in distributed Internet of Things", Elsevier Journal on Computer Networks, Volume 57, Issue 10, Pages 2266–2279, July 2013.

[23] Danny Palmer, Computing News Security Threats and Risks, 2014. http://www.computing.co.uk/ctg/news/2323661/cyber-attack-launched-through-fridge-as-internet-of-things-vulnerabilities-become-apparent

[24] Kaoru Hayashi, Computing News Security Threats and Risks, 2013. http://www.computing.co.uk/ctg/news/2309972/new-internet-of-things-worm-discovered

[25] Orlando Debruce, Proofpoint U.S. http://www.computing.co.uk/ctg/news/2309972/new-internet-of-things-worm-discovered

[26] M2M – Latest Machine to Machine Industry News http://www.m2mnow.biz/2014/09/10/25004-9-meals-anarchy-take-cybersecurity-threat-iot-seriously-says-beecham-report/

[27] Manu Namboodiri, "Thoughts on M2M and IoT security and privacy for 2015" Blog on Thoughts about M2M and Internet of Things as well as related worlds from the M2Mi team.

[28] Michael Huth N. Asokan, Srdjan Capkun Ivan Flechais, Lizzie Coles-Kemp (Eds.), "Trust and Trustworthy Computing", 6th International Conference, TRUST 2013, London, UK, June 2013 Proceedings, Springer.

[29] Vangelis Gazis, Konstantinos Sasloglou, Nikolaos Frangiadakis, and Panayotis Kikiras, "Wireless Sensor Networking, Automation Technologies and Machine to Machine Developments on the Path to the Internet of Things," 16th Panhellenic Conference on Informatics, 2012.

[30] Ivan Stojmenovic, "Large Scale Cyber-Physical Systems: Distributed Actuation, In-Network Processing and Machine-to-Machine Communications", Mediterranean Conference on Embedded Computing, 2013.

[31] Giacomo Ghidini, Stephen P. Emmons, Farhad A. Kamangar, and Jeffrey O. Smith, "Advancing M2M Communications Management: A Cloud-based System for Cellular Traffic Analysis", 15th International IEEE Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014.

[32] Min Chen, Jiafu Wan, "A Survey of Recent Developments in Home M2M Networks", IEEE Communications Surveys and Tutorials, Volume: 16, Issue: 1, 2014.

[33] Hui Wang, Suman Roy, Amitabha Das, and Sanjoy Paul, "A Framework for Security Quantification of Networked Machines", Second International IEEE Conference on Communication Systems and Networks (COMSNETS), 2010.

Biographies

V. M. Rohokale received her B.E. degree in Electronics Engineering in 1997 from Pune University, Maharashtra, India. She received her Masters degree in Electronics in 2007 from Shivaji University, Kolhapur, Maharashtra, India. She received her PhD degree from CTIF, Aalborg University, Denmark under the guidance of Prof. Ramjee Prasad. She is presently working as Dean, R and D at SKN Sinhgad Institute of Technology and Sciences (SKN-SITS), Lonavala, Maharashtra, India. Her research interests include Cooperative Wireless Communications, AdHoc and Cognitive Networks, Physical Layer Security, Information Theoretic security and its Applications, Cyber Security, etc.

R. Prasad is currently the Director of the Center for TeleInFrastruktur (CTIF) at Aalborg University, Denmark and Professor, Wireless Information Multimedia ommunication Chair.

Ramjee Prasad is the Founder Chairman of the Global ICT Standardisation Forum for India (GISFI:www.gisfi.org) established in 2009. GISFI has the purpose of increasing of the collaboration between European, Indian, Japanese, North-American and other worldwide standardization activities in the area of Information and Communication Technology (ICT) and related application areas. He was the Founder Chairman of the HERMES Partnership – a network of leading independent European research centres established in 1997, of which he is now the Honorary Chair. He is a Fellow of the Institute of Electrical and Electronic Engineers (IEEE), USA, the Institution of Electronics and Telecommunications Engineers (IETE), India, the Institution of Engineering and Technology (IET), UK, Wireless World Research Forum (WWRF) and a member of the Netherlands Electronics and Radio Society (NERG), and the Danish Engineering Society (IDA). He is also a Knight ("Ridder") of the Order of Dannebrog (2010), a distinguished award by the Queen of Denmark. He has received several international award, the latest being 2014 IEEE AESS Outstanding Organizational Leadership Award for: "Organizational Leadership in developing and globalizing the CTIF (Center for TeleInFrastruktur) Research Network". He is the founding editor-in-chief of the Springer International Journal on Wireless Personal Communications. He is a member of the editorial board of other renowned international journals including those of River Publishers. Ramjee Prasad is a member of the Steering committees of many renowned annual international conferences, e.g., Wireless Personal Multimedia Communications Symposium (WPMC); Wireless VITAE and Global Wireless Summit (GWS). He has published more than 30 books, 900 plus journals and conferences publications, more than 15 patents, a sizeable amount of graduated PhD students (over 90) and an even larger number of graduated M.Sc. students (over 200). Several of his students are today worldwide telecommunication leaders themselves.