Low-Power Low-Rate Goes Long-Range: The Case for Secure and Cooperative Machine-to-Machine Communications

Andrea Bartoli, Mischa Dohler, Juan Hernández-Serrano, Apostolos Kountouris, Dominique Barthel

Low-Power Low-Rate Goes Long-Range: The Case for Secure & Cooperative Machine-to-Machine Communications

Andrea Bartoli[1], Mischa Dohler[1], Juan Hernández-Serrano[2], Apostolos Kountouris[3] and Dominique Barthel[3]

[1]Centre Tecnològic de Telecomunicacions de Catalunya (CTTC), Spain
[2]Universitat Politècnica de Catalunya (UPC), Spain
[3]Orange, France Telecom, France

Abstract. The vision of connecting a large amount of objects on this planet to improve well-being and safety is slowly taking shape. Preceded by a decade-long era of research on low-power low-rate short-range wireless sensor networks, first proprietary and later standards-compliant embedded technologies have successfully been put forward. Cellular machine-to-machine (M2M) is taking this technology to a next step where communication ranges are significantly extended by relying on cellular infrastructure. This position paper discusses these emerging paradigms and highlights how cooperative as well as security requirements are core to their designs.

1 Introductory Remarks

The world is becoming increasingly connected. Information and communications technologies (ICT) are a true facilitator of this connectivity. The revolution, which a few decades ago began to connect people by means of mobile phones, is slowly ebbing down as virtually every human being is "cellphoned" today. Similarly, the revolution, which a few decades ago began to connect computers via the (today) Internet, is also ebbing down as virtually every computer is essentially "interneted" today. Another revolution, however, has slowly began to take shape: the one of interconnecting objects around us and thereby allowing to create an Internet of Things (IoT) [1].

Not all objects will be connected, however; and the majority not even in short term. Objects important to the well being and safety of humans will likely be connected first, leading to the vision of Internet of Important Things (IoIT) and acting as physical extension of the current Internet. The myriad of applications is huge and the benefit well understood [2].

Connecting objects, devices, things is clearly an opportunity but also poses serious challenges. The opportunity is in instrumenting and interconnecting the physical world around us and thus allowing it to act intelligently; this is essentially the vision of IBM's Smarter Planet initiative [3]. The main challenges remain in viably networking this large amount of objects given their obvious constraints in power, processing capabilities, memory and size.

Projections on the number of connected objects differ wildly [4]. The WWRF predicts that by 2017 there will be around 7 Trillion devices connected; Market Study estimated in 2009 that there will be 50 Billion devices by 2010; and ABI Research estimated in 2010 that there will be 225 Million objects connected by means of a cellular link by 2014. These visions differ by orders of magnitude. Only time will tell how many objects will get eventually connected. This paper however addresses the important issue of how these objects get connected.

Related to "how" connectivity is facilitated, the major design driver is the need to draw low power during the sensing, communication and actuation process. This is due to fact that batteries cannot be changed too often and perpetual energy scavenging typically only yields low energy volumes. Since the wireless communication module is typically the one drawing most current, most efforts in the past concentrated in designing suitable wireless communication mechanisms operating over short distances and yielding fairly low rates.

The era of wireless sensor networks (WSNs) had been born and occupied mainly academic circles for more than a decade. Having gathered a great expertise in the area and published hundreds of articles, the academic community has essentially proven that, from a technology point of view, WSNs can be used to viably connect objects over short distances.

Naturally, various pioneering companies dedicated to WSNs emerged trying to capitalize on the commercial value of the emerging technology. Among the pioneers, were companies like Crossbow, Dust Networks, Arch Rock and Coronis. They played a central role in the development of the Internet of Things and acted as a first bridge between academic findings and industrial needs. An example of a pertinent academic finding is that cooperation and relaying are great tools to save energy when covering larger geographical areas; an example of industrial need is that security is a must for any of the real-world deployments.

With more and more companies emerging, and thus proving the viability of an IoT, the community realized quickly that a plethora of propitiatory technologies is counterproductive to the vision of a quickly scaling IoT. The emergence of standards developing organizations (SDOs) in the area of short-range low-power low-rate wireless systems has hence been a natural development. The various standardization bodies aimed to creating a common understanding of the architecture, protocols and functionality of the IoT. Developments in SDOs typically reflected industrial needs whilst incorporating findings of academia. Examples of said bodies are the IEEE, IETF, HART, ISA, DASH7, among others.

On the longer term, however, we will likely experience another shift in designing the IoT and/or IoIT. Notably, to be able to truly cover large geographic areas (with often heterogenous devices) is either not possible with known short-range technologies or would simply require too much investment in multihop infrastructure. In addition, applications with mobility, roaming and alike cannot be supported, thus short-cutting large markets, such as car and logistics telemetry. The vision of machine-to-machine (M2M) communication enabled by cellular network connectivity has hence been taking shape in past years, ignited by pioneering developments of Swedish company Maingate in 1998 as well as

European manufacturing giants Ericsson and Nokia shortly after. The SDOs dominant in this area are ETSI M2M and 3GPP LTE.

Both short range systems, in M2M language referred to as *Capillary M2M*, and long range system, in M2M referred to as *Cellular M2M*, will likely co-exist until (almost) full migration to cellular system will have been achieved. Independent however of whether the system is short or long range, there will be two issues which need to be considered from the moment of conception, i.e. 1) a proper security design meeting the industrial requirements of the 21st century; and 2) a proper cooperation and networking design meeting the requirements of a functional IoT. These aspects, w.r.t. systems discussed above, are the focus of this overview and positioning paper.

The paper is structured as follows. In Section 2, we discuss in some more details the impact and importance of security and cooperation in general; we then apply these insights to specific technologies. Notably, in Section 3, we elaborate on current developments which will shape the near future of the IoT. In Section 4, we will elaborate on likely future developments which will shape the IoT of the long-term future. Section 5 concludes this position paper.

2 Security and Cooperation

Security refers to the process of protecting assets. In the context of ICT, these assets traditionally refer to data contents (syntax) and the network itself (protocols, routers, etc). However, latest trends indicate that the data meaning (semantics) and data ownership (privacy) commence playing a central role in asset management. The trend thus extends the need of providing security by means of confidentiality, integrity and authentication (CIA) to more advanced issues of trust and privacy. All these issues are a necessity but their incorporation is complicated by the following facts:

1. **Devices are unattended.** This generally requires a higher level of security and also trust mechanisms since devices are easier to comprise and not supervised; however, the increase in complexity is often not justifiable requiring other measures, such as cooperation, to be taken.
2. **Devices are of low complexity.** This prevents the use of sophisticated and powerful security schemes. Recent research however has shown that asymmetric cryptography [5] could efficiently be implemented in these networks, easing computing requirements (as well as key management). Yet, only a very limited number standards provide the possibility of using it.
3. **Devices are large in numbers.** This complicates key distribution and management as well as fast authentication approaches. In fact, most cryptographic schemes are very secure but serious security leaks occur due to poor key management. Yet, very few standards issue recommendations of how to properly manage keys for specific cryptographic algorithms.
4. **Data ownership is not always clear.** This requires privacy issues to be potentially respected from the beginning of design, where of importance is to clearly separate personal from technical data. Different approaches are

gaining in popularity, among them the use of escrow-type system architectures [6].

In summary, whilst security in terms of cryptographic mechanisms is fairly well understood, the joint consideration and inclusion of trust, privacy and key management are largely unexplored.

Cooperation refers to the process of devices helping each other in one form or another to jointly achieve a goal more efficiently than each device could do on its own. Whilst notions of cooperation through routing have been core to the networking community since its beginnings, cooperation has also been found beneficial from a capacity point of view [7], at physical layer [8], medium access control layer [9] and application layer [10]. Cooperation within the context of low-power system is a necessity as per below reasons:

1. **Range is limited.** This requires multihop, one form of cooperation, to be used. Long distances towards gateways can hence be covered by means of multiple short hops.
2. **Complexity is limited.** Cooperation allows counteracting the limited per-device complexity to achieve a more powerful system-wide complexity. In the context of security, for instance, whilst each device in the network might be fairly vulnerable to security threats, a good system design ought to ensure that the ensemble of cooperating devices exhibits a significantly higher degree of resistance to threats.

In summary, whilst cooperation has been well explored in the past by different communities, it offers enormous potentials in the context of designing a more secure system.

Both security as well as cooperation, however, are only part of a larger design exercise for a viable future-proof IoT architecture. Notably, a strong requirement of such an architecture is to be fully IP(v6) compliant. Therefore, all security and cooperation mechanisms ought to fit this framework. In addition, most IoT networks today require devices to do some form of data aggregation along the data collection path, which further complicates design if IP's end-to-end paradigm is not to be violated.

3 Capillary M2M Solutions – IoT of the Present

The short range capillary M2M solutions are being standardized by various SDOs, notably the IEEE, IETF and interest groups relying thereupon.

3.1 IEEE Standards Solutions

The IEEE is standardizing the physical (PHY) and medium access control (MAC) layers. There are three families facilitating low-power short-range IoT operation, i.e. IEEE 802.15.4 (as used by ZigBee); IEEE 802.15.1 (as used by Bluetooth); and IEEE 802.15.11 (as used by Wifi). We subsequently briefly discuss their role in the capillary M2M ecosystem.

IEEE 802.15.4. It is maintained by the IEEE 802.15 working group. IEEE 802.15.4-2006 intends to offer the fundamental lower network layers of a type of wireless personal area network (WPAN) which focuses on low-cost, low-speed ubiquitous communication between devices. The link layer is generally very secure, accept that the acknowledgements are sent in clear thus constituting a very serious security hole which has been greatly underestimated by many real-world deployments, including those using ZigBee. The following list summarizes the currently evolving versions:

- **IEEE 802.15.4e.** The IEEE 802.15.4e task group is in charge to modify the MAC sub-layer of IEEE 802.15.4 to meet the requirements of various industrial applications overcoming limitations of the current MACs. The application includes factory automation, process automation, intelligent building, asset tracking, and smart grid. This task group has emphasized three major elements: media management to minimize listening costs, improved security mechanisms, and increased link level reliability through the use of multiple channels, especially in the narrow, lower frequency bands. Now, with the 4e standard approaching ratification, IP networks will be able to improve their performance. Security has been taken very seriously, where the loophole of the unsecured acknowledgement has been rectified.
- **IEEE 802.15.4f.** It has been chartered to define new wireless PHYs and MAC enhancements required to support active RFID system for bi-directional and location determination applications. An active RFID tag is a device which is typically attached to an asset or person with a unique identification and the ability to produce its own radio signal not derived from an external radio signal. Currently, three PHY layers are under discussion.
- **IEEE 802.15.4g.** The role of IEEE 802.15 Smart Utility Networks (SUN) Task Group 4g is to create a PHY amendment to 802.15.4 to provide a global standard that facilitates very large scale process control applications such as the utility smart-grid network capable of supporting large, geographically diverse networks with minimal infrastructure, with potentially millions of fixed endpoints. It is currently under development.
- **IEEE 802.15.4k.** It addresses applications such as critical infrastructure monitoring. It defines an alternate PHY and only those MAC modifications needed to support its implementation. It is fully concentrated on ultra-low power operation, thus allowing for connectivity where no permanent energy sources are available.

IEEE 802.15.4 is the basis for the ZigBee, WirelessHART, and ISA 100.11a specification, each of which further attempts to offer a complete networking solution by developing the upper layers which are not covered by the standard.

IEEE 802.15.1. Bluetooth has originally been a proprietary wireless technology developed by Ericsson in 1994 as a wireless alternative to RS-232 data cables. Today Bluetooth is managed by the Bluetooth Special Interest Group with the aim to guarantee true interoperability between Bluetooth-enabled devices; a goal

it has not fully lived up to. Bluetooth has however been the forerunner of the IoT with many devices being Bluetooth enabled today. Whilst current realizations of Bluetooth will be part of the IoT arena, latest developments into low-power designs are likely going to be some further steps forward.

- **IEEE 802.15.1 Bluetooth Low Energy.** Bluetooth low energy is an alternative to the Bluetooth standard that was introduced in Bluetooth v4.0, and is aimed at very low power applications running off a coin cell. It has a communication range of a few dozen meters, also operates in the 2.4GHz ISM band, supports data rates of around 200kbps, and draws less than 15mA in transmission. First chips have appeared in late 2010, such as the TI CC2540.
- **Security Issues.** Bluetooth has some serious security concerns not all of which have been addressed in recent standards revisions. Some of these issues are summarized in [11].

IEEE 802.11. In 1997 the IEEE adopted IEEE Standard 802.11-1997, the first wireless LAN (WLAN) standard. This technology is promoted from WiFi Alliance that is a trade association in charge of certifies products if they conform to certain standards of interpretability. Wifi has had a tremendous success in recent years and has also technically been advanced through various amendments. As such, IEEE 802.11 networks are not suitable to low-power networking designs; however, latest developments into low-power solutions may yield some surprises. Notably, if low-power Wifi really takes off, the problem of coverage which IEEE 802.15.4 networks try to overcome by means of multihop will automatically be reduced.

- **IEEE 802.11 Low Power.** With the growing market for smart objects and wireless sensors, several companies have developed application specific integrated circuits that are optimized for sensing applications. These products achieve a similar power profile as above low power architectures whilst leveraging the huge installed base of over 2 billion Wifi certified devices; a vibrant standard and industry alliance of close to 300 members; well proven encryption, authentication and end to end network security; mature network management systems; etc. Among one of the first companies promoting the concept of low power Wifi was Ozmo Devices. They tune the .11 protocol stack as well as introduce aggressive power saving operations.
- **Security Issues.** The Wifi Protected Access (WPA) security protocol has become the industry standard for securing .11 networks. Using a pre-shared encryption key (PSK) or digital certificates, the WPA algorithm Temporal Key Integrity Protocol (TKIP) securely encrypts data and provides authentication to said networks. TKIP was designed to be a transition between old hardware and new encryption models. The IEEE 802.11i protocol improved upon the WPA algorithm (TKIP) to the new WPA2 [12] that uses a better encryption algorithm: Advanced Encryption Standard (AES). As a major step forward, the protocol also specifies more advanced key distribution techniques, which result in better session security to prevent eavesdropping.

3.2 IETF Standards Solutions

The Internet Engineering Task Force (IETF) is actually not an SDO since not approved by the US government. It is composed of individuals, not companies. It meets about three times a year, and gathers an average of 1,300 individuals. It enjoys more than 120 active working groups organized into various areas. The general scope of the IETF is *above the wire/link and below the application*. However, layers are getting fuzzy (MAC & APL influence routing) and we lately hence experience a constant exploration of edges. There are three working groups pertinent to capillary M2M where we will concentrate on two, i.e. IETF 6LoWPAN (establishing gateway to Internet); IETF ROLL (facilitating routing in low-power network); IETF CoRE (defining application transfer protocol). We subsequently briefly discuss their role in the capillary M2M ecosystem.

IETF 6LoWPAN. IPv6 over Low power WPAN (6LoWPAN) acts as a simplified gateway between the low power embedded network and the Internet. It facilitates neighborhood discovery, header compression with up to 80% compression rate, packet fragmentation (1260 byte IPv6 frames → 127 byte IEEE 802.15.4 frames), and thus direct end-to-end Internet integration. However, it does not provide routing. Security is also catered for [13].

IETF ROLL. Routing Over Low power and Lossy networks (ROLL) deals with the design of a routing protocol for wireless low power mesh networks. It is in its final stage of standardization. It is based on a gradient routing protocol where nodes acquire a rank based on the distance to the collecting node and the messages follow the gradient of ranks to reach the destination. Again, security is currently being catered for [14].

IETF CoRE. Constrained RESTful Environments (CoRE) aims to extend the web architecture using constrained networks and devices [15]. Two items are dealt with, i.e. definition of the application transfer protocol Constrained Application Protocol (CoAP) that realizes a minimal subset of the known protocols REST along with resource discovery, subscription/ notification, and the use of appropriate security measures; and define a set of security bootstrapping methods for use in constrained environments in order to associate devices and set up keying material for secure operation.

3.3 WirlessHart Standard Solution

WirelessHART (Highway Addressable Remote Transducer)is an open-standard wireless networking technology developed by HART Communication Foundation. It is the wireless version of the HART protocol, which is the most used in the automation and industrial applications which require real time responses. The protocol utilizes a time synchronized, self-organizing, and self-healing mesh architecture. The protocol currently supports operation in the 2.4 GHz ISM

Band using IEEE 802.15.4 standard radios. With respect to the stack of WirelessHart, the PHY layer is based on the IEEE 802.15.4-2006 whereas the MAC layer has been modified to meet the industrial needs. Its MAC layer is based on TSMP and similar to IEEE 802.15.4e with the only difference that a set of time/frequency hopping patterns are fixed. The frequency hopping approach allows to mitigate fading and interferences in the communication channel.

- **Security Provisioning.** The WirelessHART Security Manager is responsible for the generation, storage, and management of the keys that are used for device authentication and encryption of data. In order to provide authentication WirelessHart provides the MIC that is generated with CCM* (counter with CBC-MAC) using the AES-128 algorithm. For its generation it is necessary to include a 128-bit key, a nonce of 13 bytes and the message header without encryption. Public, Join, Network and Session Keys must be provided from the WirelessHART Network Manager:
  - **Network key:** it is shared by all network devices and is used to generate the MIC on the MAC layer.
  - **Public key:** it is pre-configured in every node and is used to provide authentication during joining process; in this case network key cannot be used because it is delivered from the security manager after the first authentication.
  - **Join key:** it is pre-configured in every new node and whenever a new node joins in the network it will be authenticated by the network manager that will send to it the network and the session keys.
  - **Session key:** it is the unique key between two network devices. It is used to provide confidentiality and integrity to any interchanged messages in order to ensure privacy to end-to-end communication. The delivery of this key is managed by the security manager.

  Providing secure links core to the WirelessHART design.

3.4 ISA 100.11a Standard Solution

ISA100.11a is a wireless communication standard aiming to provide reliable and secure operation for non-critical monitoring, alerting, and control applications specifically focused to meet the needs of industrial users.

ISA100.11a defines a subset of the OSI stack and an organization structure of permitted networks, system management, gateway, and security specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices, including support for very limited power consumption.

ISA100.11a utilizes the 802.15.4 PHY layer, provides extensions to the 802.15.4 MAC and defines network layer through application layer functions and services. The medium and part of the data link layer is based on IEEE 802.15.4 2.4GHz DSS PHY and extends the 802.15.4 MAC layer including methods for channel hopping, TDM based bandwidth management, mesh networking (forming, routing and discovery support). The network layer is based on IETF RFC 4944 [16]

(transport of IPv6 packets over IEEE 802.15.4) with constraints to focus on security and low power; network layer services include address translation (and compression), fragmentation and routing. The Transport layer is based on UDP per RFC4944, and includes security services. The Application layer provides and object model and object-to-object communication services. Key goals are robustness in harsh industrial applications, coexistence in the presence of other wireless services, and low cost/low complexity deployment. Security services are extended throughout the entire stack and are based on the security offered by IEEE 802.15.4-2006 with symmetrical and asymmetrical keys, configuration, operation and maintenance.

3.5 ZigBee Alliance

ZigBee, created by the ZigBee Alliance, is a set of recommendations to facilitate interoperability between wireless low power devices. The relationship between IEEE 802.15.4 and ZigBee is similar to that between IEEE 802.11 and the Wifi Alliance. ZigBee relies today on the PHY and MAC layers of IEEE 802.15.4, will shortly rely on the networking layer of the IETF 6LoWPAN (and likely ROLL), and then builds its industrial profiles on top. We shall briefly focus on the security services offered for its most popular modes, i.e. standard security mode for ZigBee stack 1; and high security mode for ZigBee stack 2 (ZigBee PRO). However, no matter how secure the system is, the reliance on the insecure IEEE 802.15.4 MAC layer makes it a vulnerable design choice.

3.6 DASH7 Alliance

DASH7 is the name of a technology promoted by the DASH7 Alliance. It is an emerging embedded low power networking technology using the ISO/IEC 18000-7 standard for active RFID, operating at in the 433MHz unlicensed spectrum. DASH7 provides multi-year battery life, range of up to 2km, low latency for tracking moving objects, small protocol stack, sensor and security support, and data transfer of up to 200 kbit/s. It has found interest in military circles too where the US DoD awarded a $429 million contract for DASH7 devices, making it one of the largest wireless sensor networking deployments in the world.

3.7 Wavenis Open Standards Alliance

Wavenis technology relies on ultra-low power RF components allowing for decade long battery-driven operation with applications. Wavenis-OSA is an independent standards alliance whose participants work together to define the Wavenis technology roadmap and to deliver new Wavenis features and capabilities Based on Wavenis features and capabilities, similar to the ZigBee profiles, all new Wavenis adopters can define their own Wavenis profiles to meet specific application requirements: frequency bands, data rate, output power, channel bandwidth, network topology, self-routing and self-healing options, etc. The work is driven by the Technical Committee, composed of the four PHY/MAC, IP, Application and security working groups.

4 Cellular M2M Solutions — IoT of the Future

Cellular M2M technology developments are commencing to take momentum, with many companies and various SDOs envisioning future IoT applications to run over such networks. From a rate and range point of view, current cellular systems already meet the M2M requirements; however, from a power consumption point of view, many issues remain open. We will thus briefly discuss various cellular M2M initiatives.

4.1 ETSI M2M

ETSI M2M is composed by various manufacturers, operators and service providers, among others. ETSI typically provides the framework, requirements and architecture, whereupon technologies such as 3GPP or IEEE can be used to populate the developed architecture. The work is organized in stages:

- **Stage 0: Use cases documents.** Several use case documents have been developed in parallel, such as M2M requirements for smart metering, health applications, etc.
- **Stage 1: Services requirements.** The thus resulting service requirements have then been developed which aims to unify the requirements of the different use case documents.
- **Stage 2: Architecture.** Here, capabilities and interfaces are developed, as well as message flows, etc.
- **Stage 3: Refinement.** In this stage, the architecture is refined to meet the prior outlined user requirements.

ETSI M2M currently (Q1 2011) also works on security requirements which influence the entire M2M architectural design.

4.2 3GPP LTE-M

The concept of M2M has been born out from 2G cellular systems and, early adopters of GSM/GPRS data plans, clearly demonstrated the its value. 3GPP thus naturally issued in January 2007 a technical report TR 22.868 “Study on Facilitating Machine to Machine Communication in 3GPP Systems” which identified that a huge market potential for M2M beyond the current market segment. However, due to CDMA-based 3G systems not being suitable to low power operations, there have been little developments until recently. With OFDM-based LTE on the horizon, cellular M2M has suddenly become of interest again and a set of further documents has been issued lately, e.g. TS 22.368 “Service Requirements for Machine-Type Communications (MTC)” and TR 23.888 “System Improvements for MTC”.

Not all MTC applications have the same characteristics and not every optimization is suitable to all applications; therefore, features are defined to provide some structure to the customer and the network is then tuned accordingly to needs. These features are offered on a per subscription basis and include items

such as Low Mobility, Time Controlled, Time Tolerant, Packet Switched only, Small Data Transmissions, Mobile originated only, Infrequent Mobile Terminated, MTC Monitoring, Priority Alarm Message (PAM), Secure Connection, Location Specific Trigger, Network Provided destination for Uplink Data, Infrequent transmission, Group Based Policing, Group Based Addressing, etc.

Whilst the potential and market value are clear, technical problems − mainly in the area of low-power consumption, support of large amount of nodes and low delays − still remain. These and other problems are currently being addressed by the 3GPP and the EU integrated projected EXALTED [17].

5 Conclusions

The same way as highways have changed the way people travel, mobile phones have transformed the way people communicate and the Internet the way computers and, by extension, people connect. This paved the way for an emerging trend which calls for connecting objects around us, thus forming an Internet of Things. This position paper has discussed the history behind developments in this area as well as current and future technologies used to facilitate the needed connectivity breakthrough. Driven by the low power requirements, cooperative techniques will be core to these systems; driven by the unsupervised operation, security will play a pivotal role in the system design, which is complicated by the fact that complexity has to be kept low whilst handling a large amount of objects and devices.

To summarize, pioneering academic work in the early 90s by people like Prof Kris Pister, Berkeley University, US, has ignited a two-decade long research era on low power embedded networks which later became to be known as wireless sensor networks. Spurned by these advances, proprietary commercial solutions have appeared by pioneering companies like Crossbow and Dust Networks.

The success of these companies has been a turning point in that various standardization activities have kicked in to ensure that the plethora of emerging technologies are interoperable to ensure the needed scalability of the emerging IoT. Key standards are those of the IEEE (802.15.4-2006/e/f/g/k) and IETF (6LoWPAN/ROLL), as well as all the interest groups which have formed around it (ZigBee/WirelesHART/ISA100.11) or developed independently (DASH7/ANT+/WOSA).

Recognizing the disadvantages of these low-power systems, i.e. lack of true ubiquitous coverage and inability to support mobility/roaming, the concept of machine-to-machine (M2M) was born. It facilitates low-power low-rate connectivity between objects over large distances by relying on existing cellular infrastructures. To make this a viable technology, however, much work is needed, notably to reduce the power consumption of the cellular modules. The driving standards dedicated to making this reality are ETSI M2M and 3GPP LTE-M.

Connecting objects around us is hence becoming reality, the more so with the plethora of available short-range and long-range communication technologies.

Security and cooperative paradigms have already been playing a pivotal role in their design, and will continue doing so in the years to come.

Acknowledgements

This work has in part been supported by a France Telecom research contract on M2M security as well as the EU project ICT-258512 EXALTED.

References

1. A. Iera, C. Floerkemeier, J. Mitsugi, and G. Morabito, "The internet of things [guest editorial]," *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 8 –9, 2010.
2. G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the internet of things," *Internet Computing, IEEE*, vol. 14, no. 1, pp. 44 –51, 2010.
3. (2010) Smarter planet initiative. [Online]. Available: http://www.ibm.com/smarterplanet/us/en/overview/ideas/
4. M. Dohler, T. Watteyne, and J. Alonso-Zarate, "Machine-to-machine: An emerging communication paradigm," Globcom Miami, USA, Tutorial, Dec 2010.
5. R. Roman and C. Alcaraz, "Applicability of public key infrastructures in wireless sensor networks," in *Public Key Infrastructure*, ser. Lecture Notes in Computer Science, J. Lopez, P. Samarati, and J. Ferrer, Eds. Springer Berlin / Heidelberg, 2007, pp. 313–320.
6. C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 238 –243.
7. B. Sirkeci-Mergen and M. Gastpar, "On the broadcast capacity of wireless networks with cooperative relays," *Information Theory, IEEE Transactions on*, vol. 56, no. 8, pp. 3847 –3861, 2010.
8. M. Dohler and Y. Li, *Cooperative Communications: Hardware, Channel & PHY*. Corporate Headquarters 111 River Street Hoboken, NJ 07030-5774: Wiley, 2010.
9. J. Alonso-Zarate, E. Kartsakli, L. Alonso, and C. Verikoukis, "Cooperative arq: A medium access control (mac) layer perspective," in *Radio Communications*. A. Bazzi, Sciyo, 2011.
10. F. Fitzek, *Cooperation in Wireless Networks: Principles and Applications*. New York, NY 10036: Springer, 2006.
11. R. Bouhenguel, I. Mahgoub, and M. Ilyas, "Bluetooth security in wearable computing applications," in *High Capacity Optical Networks and Enabling Technologies, 2008. HONET 2008. International Symposium on*, 2008, pp. 182 –186.
12. J.-C. Chen, M.-C. Jiang, and Y. wen Liu, "Wireless lan security and ieee 802.11i," *Wireless Communications, IEEE*, vol. 12, no. 1, pp. 27 – 36, 2005.
13. R. Barker, "Security aspects in 6lowpan networks," in *Design, Automation Test in Europe Conference Exhibition (DATE), 2010*, 2010, p. 660.
14. *A Security Framework for Routing over Low Power and Lossy Networks*, IETF Std. ROLL, Work in progress.
15. Z. Shelby, "Embedded web services," *Wireless Communications, IEEE*, vol. 17, no. 6, pp. 52 –57, 2010.
16. (2007) Rfc 4944. [Online]. Available: http://www.ietf.org/rfc/rfc4944.txt
17. (2010) The ICT EXALTED project. [Online]. Available: http://www.ict-exalted.eu