Ericsson Review

The communications technology journal since 1924

2014 • 8

Capillary networks – a smart way to get things connected

September 9, 2014

ERICSSON

Capillary networks – a smart way to get things connected

A capillary network is a local network that uses short-range radio-access technologies to provide groups of devices with connectivity. By leveraging the key capabilities of cellular networks – ubiquity, integrated security, network management and advanced backhaul connectivity – capillary networks will become a key enabler of the Networked Society.

JOACHIM SACHS, NICKLAS BEIJAR, PER ELMDAHL, JAN MELEN, FRANCESCO MILITANO AND PATRIK SALMELA

People and businesses everywhere are becoming increasingly dependent on the digital platform. Computing and communication are spreading into every facet of life with ICT functionality providing a way to manage and operate assets, infrastructure, and commercial processes more efficiently. The broad reach of ICT is at the heart of the Networked Society, in which everything will become connected wherever connectivity provides added value[1,2].

Ubiquitous connectivity and the Networked Society

Connectivity in the Networked Society is about increasing efficiency, doing more with existing resources, providing services to more people, reducing the need for additional physical infrastructure, and developing new services that go beyond human interaction. For example, smart agricultural systems monitor livestock and crops so that irrigation, fertilization, feeding and water levels can be automatically controlled, which ensures that crops and livestock remain healthy and resources are used wisely. In smart health care, patients and the elderly can get assistance through remote monitoring – again using resources in an intelligent way – which improves the reach of health care services, reduces the need for, say, physical day clinics and cuts the need for patients to travel.

As a whole, communication is progressively shifting from being human-centric to catering for things as well as people. The world is moving toward machine-type communication (MTC), where anything from a smart device to a cereal packet will be connected; a shift that is to some extent illustrated by the explosive growth of the Internet of Things (IoT).

However, the requirements created by object-to-object communication are quite different from those of current systems – which have primarily been built for people and systems to communicate with each other. In scenarios where objects communicate with each other, some use cases require battery-operated devices; therefore, low energy consumption is vital. Barebones device architecture is essential for mass deployment; typically the data rate requirements for small devices are low, and the cost of connectivity needs to be minimal when billions of devices are involved. Meeting all of these new requirements is a prerequisite for the MTC business case.

Cellular communication technologies are being enhanced to meet these new service requirements[3,4]. The power-save mode for example, introduced in the most recent release (Rel-12) of LTE, allows a sensor that sends hourly reports to run on two AA batteries for more than 10 years, and simplified signaling procedures can provide additional battery savings[5]. Rel-12 also introduces a new LTE device category, which allows LTE modems for connected devices to be significantly less complex and cheaper than they are today – the LTE features proposed in 3GPP reach complexity levels below those of a 2G EGPRS modem[6]. In addition, 3GPP has identified ways to increase the coverage of LTE by 15-20dB. This extension helps to reach devices in remote or challenging locations, like a smart meter in a basement[6].

Capillary networks and the short-range communications technologies that enable them are another key development in the Networked Society: they play an important role providing connectivity for billions of devices in many use cases. Examples of the technologies include Bluetooth Low Energy, IEEE 802.15.4, and IEEE 802.11ah.

This article gives an overview of the significant functionality that is needed to connect capillary networks, including how to automatically configure and manage them, and how to provide end-to-end connectivity in a secure manner.

Capillary networks

The beauty of short-range radio technologies lies in their ability to provide connectivity efficiently to devices within a

BOX A Terms and abbreviations

CoAP	Constrained Application Protocol	MTC	machine-type communication
EGPRS	enhanced general packet radio service	M2M	machine-to-machine
eSIM	embedded SIM card	OSPF	Open Shortest Path First
GBA	Generic Bootstrapping Architecture	SLA	Service Level Agreement
IoT	Internet of Things	TLS	transport layer security

specific local area. Typically, these local – or capillary – networks need to be connected to the edge of a communication infrastructure to, for example, reach service functions that are hosted somewhere on the internet or in a cloud.

Connecting a capillary network to the global communication infrastructure can be achieved through a cellular network, which can be a wide-area network or an indoor cellular solution. The gateway between the cellular network and the capillary network acts just like any other user equipment.

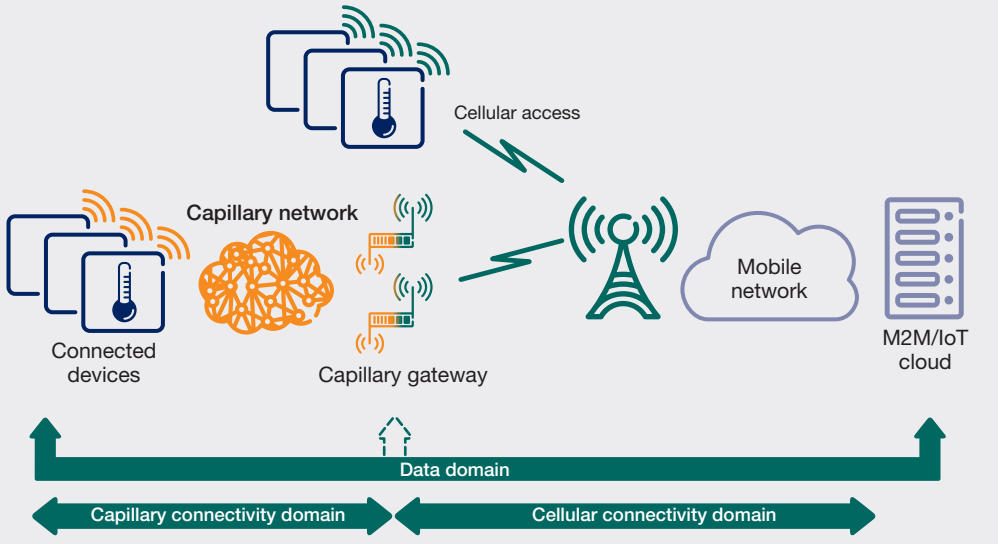
The architecture, illustrated in **Figure 1**, comprises three domains: the capillary connectivity domain, the cellular connectivity domain, and the data domain. The first two domains span the nodes that provide connectivity in the capillary network and in the cellular network respectively. The data domain spans the nodes that provide data processing functionality for a desired service. These nodes are primarily the connected devices themselves, as they generate and use service data though an intermediate node, which like a capillary gateway, would also be included in the data domain if it provides data processing functionality (for example, if it acts as a CoAP mirror server).

All three domains are independent from a security perspective, and so end-to-end security can be provided by linking security relationships in the different domains to one another.

The ownership roles and business scenarios for each domain may differ from one case to the next. For example, to monitor the building sensors of a real estate company, a cellular operator might operate a wide-area network and possibly an indoor cellular network, as well as owning and managing the capillary network that provides the sensors with connectivity. The same operator may also own and manage the services provided by the data domain and, if so, would be in control of all three domains.

Alternatively, the real estate company might own the capillary network, and partner with an operator for connectivity and provision of the data domain. Or the real estate company might own and manage both the capillary network and the data domain with the operator providing connectivity. In all of these scenarios, different service agreements are needed to cover the interfaces between the domains, specifying what functionality will be provided.

FIGURE 1 System architecture for capillary network connectivity



Like most telecom networks, a capillary network needs a backhaul connection, which is best provided by a cellular network. Their quasi-ubiquitous coverage allows backhaul connectivity to be provided practically anywhere; simply and, more significantly, without installation of additional network equipment. Factoring in that a capillary network might be on the move, as is the case for monitoring goods in transit, leads to the natural conclusion that cellular is an excellent choice for backhaul.

In large-scale deployments, some devices will connect through a capillary gateway, while others will connect to the cellular network directly. Regardless of how connectivity is provided, the bootstrapping and management mechanisms used should be homogeneous to reduce implementation complexity and improve usability.

Smart capillary gateway selection

Ideally, any service provider should be able to deploy a capillary network, including device and gateway configuration. For this to be possible, deployment needs to be simple and use basic rules – circumventing the need for in-depth network planning. To achieve this, a way to automatically configure connectivity is needed.

When deploying a capillary network, a sufficient number of capillary gateways need to be installed to provide a satisfactory level of local connectivity. Doing so should result in a certain level of connectivity redundancy – a device can get connected through several different gateways. Some systems (such as electricity meter monitoring) need to be in operation for years at a time, during which the surrounding environment may change; nodes may fail, additional network elements may be added, and even the surrounding physical infrastructure can change. But, by allowing the capillary network configuration to change, some slack in maintaining constant connectivity is built into the system, which allows it to adapt over time.

The key to maintaining connectivity and building flexibility into connected systems lies in optimal gateway selection. The decision-making process – what gateway a device chooses for connectivity – needs to be fully automated and take into consideration a number of network and gateway properties. Network parameters – such as the

quality of the cellular radio link and the load in the cellular cell that a gateway is connected to – fluctuate, and so a given capillary gateway will provide different levels of backhaul connectivity at different times. Other considerations, like the amount of power a battery-operated gateway has left, have an impact on which gateway is optimal for a given device at a specific point in time. Consequently, optimal gateway selection should not be designed to balance load alone, but also to minimize delays, maximize availability and conserve power. The gateway selection mechanism should support device reallocation to another gateway when the properties or the connectivity to a gateway change. By designing gateway selection to be smart, flexibility in connectivity is inbuilt, allowing systems to continue to function as the environments around them evolve.

As illustrated in **Figure 2**, gateway selection relies on three different types of information: connectivity, constraints and policy.

Connectivity information describes the dynamic radio connectivity between devices and gateways. Devices typically detect connectivity by listening to the beacon signals that gateways transmit. Some capillary short-range radio technologies allow connectivity to be detected by the gateway.

Constraint information describes the dynamic and static properties of the network and the gateways that are included in the selection process. Properties such as battery level, load level (which can be described by the number of connected devices per gateway), support for QoS, cost of use, and sleep schedule are all included. The cellular backhaul connectivity of a gateway, such as link quality, can also be included, and future enhancements might include properties such as cell load – obtained from the management system of the cellular network. Devices may provide additional constraint information, such as device type, battery level, QoS requirements and capillary network signal strength.

Policy information determines the goal of gateway selection. A policy might be a set of weightings or priorities that determine how the various constraint parameters affect the best choice of gateway. Policy information may also include requirements set by the management system, such as allowing certain types of device to always connect to given gateways. Policies are static and are defined by network management.

The process of gateway selection includes the following phases:

- the information regarding connectivity, constraints, and policy is gathered by the element making the selection;
- the gateway selection algorithm applies the policies to the constraints while taking connectivity into consideration and determines the optimal gateway;
- once a gateway has been selected for each device, the selection is implemented, which may imply that a device needs to switch gateway; and
- when a device moves to another gateway, new routes to the device must be set up in the cellular network so that the incoming traffic is routed correctly.

The selection process can be controlled at various locations in the network. The location of control in turn affects the need to transport information concerning constraints, policies and connectivity to the control point and to signal the selection to devices.

If the control point is located in the connected device, the device performs the selection autonomously through local computation based on information sent by the gateway. As devices have just a local view of the network, it may not always be possible to optimize resources globally and balance load across a group of gateways.

If the control point is located in the capillary gateways, the gateways need to communicate with each other and run the selection algorithm in a distributed manner. This implies that gateways are either connected via the capillary network, via the mobile network or via a third network such as Wi-Fi, and use a common protocol, like OSPF, for data distribution. The main challenge here is to reach convergence quickly and avoid unnecessary iteration due to changes in topology.

Alternatively the control point could be a single node in the network that collects the entire set of available information. This centralized method enables resource usage to be optimized globally across the entire network. However, it increases communication needs, as it requires all of the capillary gateways to communicate with a single point.

Managing QoS across domains

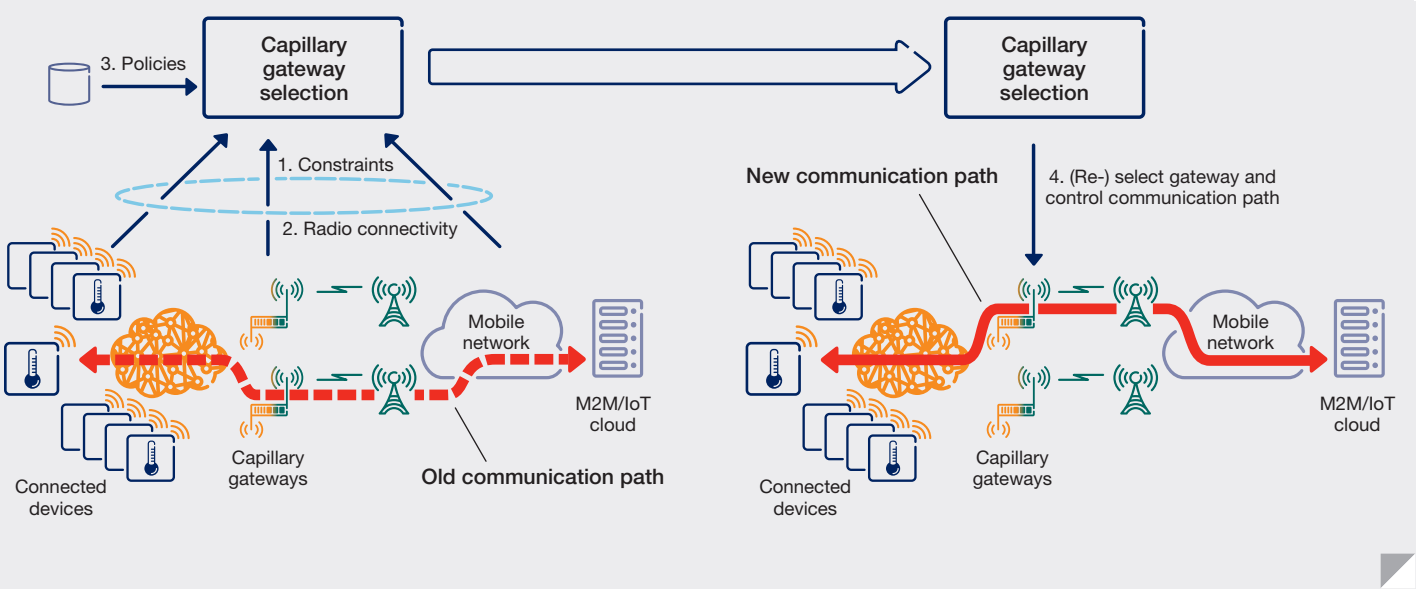
The QoS requirements for machine-type communication are typically different from those used for traditional multimedia communication in terms of bandwidth, latency and jitter. For MTC, the requirement is often for guaranteed network connectivity with a minimum throughput, and some use cases may include stricter constraints for extremely low latency.

For example, a sensor should be able to reliably transmit an alarm within a specified period of time after the detection of an anomaly – even if the network is congested. To achieve this, low latencies are needed for real-time monitoring and control, while the bandwidth requirements for this type of scenario tend to be low. That said, QoS requirements for machine-type communication can vary tremendously from one service to another. In some cases, like surveillance, the QoS requirements are comparable to those of personal multimedia communication.

QoS needs to be provided end-to-end. So for the capillary network case, the distinct QoS methods of both the short-range network and the cellular network need to be considered. Each type of short-range radio technology provides different methods for QoS, which can be divided into two main groups: prioritized packet transmission (for example, in 802.11) and bandwidth reservation (for example, in 802.15.4 and Bluetooth Low Energy). As short-range technologies work in unlicensed spectrum, the level of interference at any given time is uncertain, which limits the level of QoS that can be guaranteed. QoS methods for the cellular networks that provide connectivity, however, are well established and are based on traffic separation with customized traffic handling.

To provide QoS end-to-end, a bridge is needed between the QoS domains of the capillary and cellular networks. This bridge specifies how traffic from one domain (through a domain specific QoS treatment) is mapped to a specific QoS level in the other. The specifics of the QoS bridge are determined in a Service Level Agreement (SLA) established between the providers of the capillary

FIGURE 2 **Smart capillary gateway selection**



network domain and the cellular connectivity domain, or between the service owner (in the data domain) and the connectivity domain providers.

Security for connected devices

The devices deployed in capillary networks are likely to vary significantly in terms of size, computational resources, power consumption and energy source. This variation makes implementing and deploying security measures challenging. Security in capillary networks, or within MTC in general, does not follow a one-size-fits-all model because the constrained devices in the capillary network are just that: constrained. It is probably not possible to apply a generic security solution: even if such a solution ensures security in the most demanding of scenarios, highly-constrained devices will probably not have the resources to implement it. What is needed is a security solution that fulfills the security requirements of the use case at hand.

For example, a temperature sensor installed in a home is unlikely to have the same strict security requirements as, say, a pacemaker or a sensor in a power plant. A successful attack on any one of these three use cases is likely to yield drastically different consequences. So risk needs to be assessed in the development of security requirements for the specific scenario, which in turn determines what security solutions are suitable. The choice of a suitable security solution may then impact the choice of device hardware, as it needs to be capable of implementing the selected security solution.

For end-to-end protection of traffic between authenticated end-points, widely used security mechanisms such as TLS would improve interoperability between constrained devices and services that are already deployed. In some cases, there might be a need for more optimized security solutions to be deployed, such as by using a protocol that entails fewer round-trips or incurs less overhead than legacy solutions.

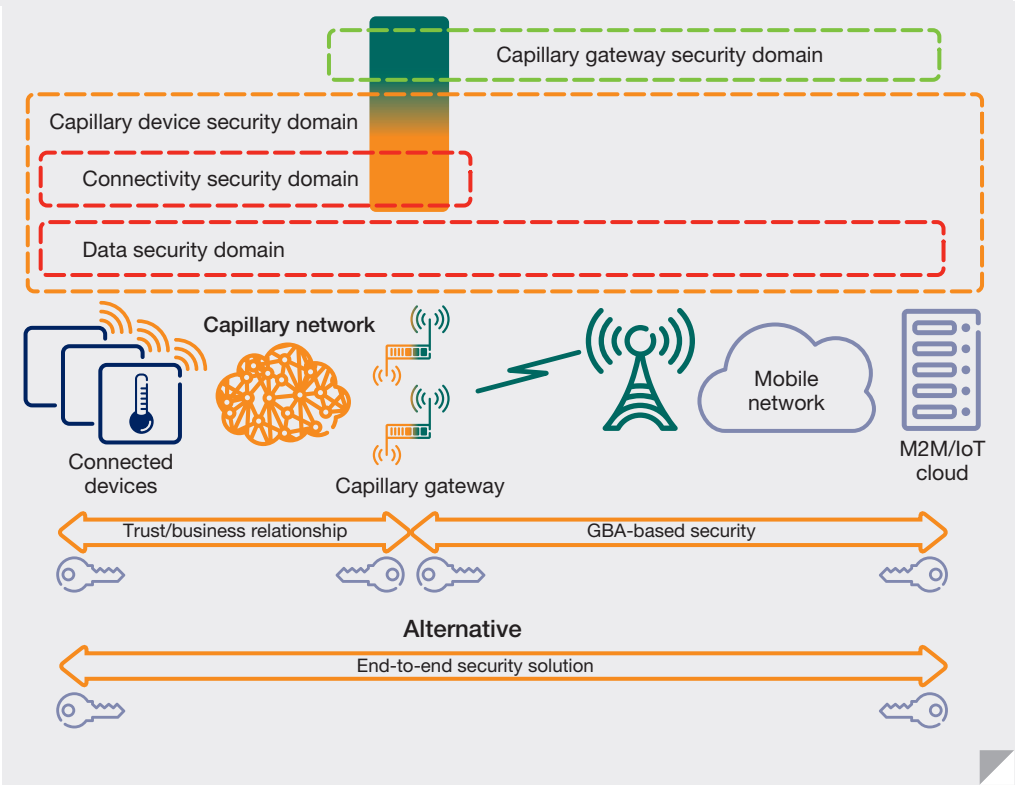
Identification

When a device is installed in a capillary network, in most cases it needs to possess some credentials – that is to say an identity and something it can use to prove it owns the identity, such as a key. Typical solutions include public key certificates, raw public keys or a shared secret. With its stored credentials, the device needs to be able to authenticate itself to the services it wants to use – such as a management portal through which the device is managed, a data aggregation service where the device stores its data, as well as the capillary gateway, which provides the device with global connectivity.

One way to implement device identification and credentials is to use the same method used in 3GPP networks – basically the 3GPP subscription credentials. The subscription identity and a shared secret that can be used for authentication in 3GPP networks are stored on the SIM card of the device. In addition to using the credentials to get network access, they can also be used for authenticating the device to various services in the network. This can be done using the 3GPP-standardized Generic Bootstrapping Architecture (GBA). For MTC scenarios, GBA is a good solution, as it provides strong identification and communication security without requiring any user interaction or configuration at the device end; the security is based on the 3GPP credentials stored in a tamper-resistant environment, to which not even the user has direct access.

To apply GBA, first of all the device needs to have 3GPP credentials; and then the 3GPP network, the desired service as well as the device itself all need to support GBA. Unfortunately, many capillary network devices do not possess 3GPP credentials, which limits the use of GBA to capillary gateways. In such cases, the gateway can provide GBA-based authentication and security for services on behalf of the entire capillary network, but device authentication

FIGURE 3 Security domains – bootstrapping and management



still needs to be performed between the device and the service.

Security domains

Capillary networks have two distinct security domains, as illustrated in **Figure 3:** the capillary devices and the capillary gateway that provides wide-area connectivity. The security domain for devices can further be split into connectivity and data domains. The data domain incorporates the device and the services it uses, such as management and data storage, and the connectivity domain handles the interaction between the device and the capillary gateway.

The security domain for the capillary gateway is based on the 3GPP subscription and the security that the subscription credentials can provide for access services and 3GPP-aware services; for example, through the use of GBA.

The two security domains intersect at the capillary gateway; there is a need for mutual trust and communication security between the device and the gateway. At this intersection there is an opportunity to apply the strong identification and security features of the 3GPP network for the benefit of the capillary device. If strong trust exists between the device and the capillary gateway, the security domains can be partially merged to provide the device with 3GPP-based security for the GBA-enabled services it uses.

Bootstrapping

When a device is switched on or wakes up, it may be able to connect to a number of capillary gateways, possibly provided by different gateway operators. The device needs to know which gateway it has a valid association with and which it can trust. Once global connectivity has been established, the device also needs to know which services to connect to. Capillary devices will be deployed in the thousands, and as a consequence of their bare-boned architecture, they do not tend to be designed with easy-to-use user interfaces. Manual configuration of massive numbers of capillary devices has the potential to be extremely time consuming, which could cause costs to rise.

Bootstrapping devices to their services using a bootstrap server is one way of automating configuration and avoiding the manual overhead. Such a service, which could be operated by the device manufacturer, would ensure that the device is redirected to the selected management service of the device owner. During the manufacturing process, devices can be pre-configured with information about the bootstrap server, such as how to reach it and how to authenticate it. When switched on or upon waking up, the device will connect to the bootstrap server, which helps it to find its current home.

If a device gets corrupted, or for some reason resets itself, it can – once rebooted – use the bootstrap server to reach its current management portal. From the management portal, either the device owner or an assigned manager can configure the device with the services it should use – and possibly even provide the service specific credentials to the device. This approach removes the need to individually configure each device, and can instead provide a centralized point for managing all devices, possibly via batch management.

The ability to remotely manage devices becomes significant when, for example, 3GPP subscription information needs to be updated in thousands of deployed devices. Today, 3GPP credentials tend to be stored on a SIM card, and updating this information typically requires replacing the SIM card itself. Embedded SIM cards (eSIM) and SIM-less alternatives are now being researched. While eSIM is a more MTC-friendly option, as it allows for remote management of subscription information, SIM-less is of most benefit to constrained devices, to which adding a SIM is an issue simply because they tend to be quite small.

Network management

A range of tasks, such as ensuring automatic configuration and connectivity – for devices connected through a capillary network – are fulfilled by network management. In addition, network management needs to establish access control restrictions and data treatment

rules for QoS based on SLAs, subscriptions and security policies. In addition, a service provider should be able to use the management function to adapt service policies and add or remove devices.

By nature, connected devices are rudimentary when it comes to manual interaction capabilities. Additionally, the fact that service providers tend to have no field personnel for device management implies that a remote management and configuration interface is needed to be able to interact with deployed devices.

Network management of connected devices in capillary networks poses new challenges compared with, for example, the management of cellular networks. This is partly due to the vast number of devices, which are orders of magnitude larger than the number of elements handled by today's network management systems. Instead of handling devices as individual nodes, economy of scale can be achieved by handling them in groups that use policies and managed parameters that are more abstract and also fewer in number.

Consider the case of a service provider that wants to reduce costs by replacing sensor batteries less frequently. To achieve this, the service provider increases the life length policy of the node in the management system. The management system interprets this policy and sets the reporting frequency to every two hours, instead of every hour, for a group of sensors in a particular geographical region.

Connected devices will often be battery powered, and so all operations, including management, need to be energy optimized to reduce the impact on battery usage. Additionally, connected devices tend to sleep during extended periods of time, and so management operations cannot be expected to provide results instantly, but only after the device wakes up.

A significant challenge for network management is the provision of full end-to-end scope, an issue that is particularly evident when different domains in the end-to-end chain are provided by different business entities – as discussed and indicated in Figure 1. Based on analysis of the connectivity information provided just by the devices, the connectivity state can only be estimated at a high level, extracted from the information available at each end of the communication path. Estimating the connectivity in this way can lead to a significant overhead to obtain and maintain such information; it is also limits the configuration possibilities of the connectivity layer.

The best way to overcome this limitation is to interconnect the network management systems in the different domains. In this way, connectivity information from the nodes along the communication path, between the end points, can also be included. If the domains are operated by separate entities, this can be achieved through SLAs specifying the usage and exchange of information. The resulting cross-domain management provides end-to-end management opportunities. For example, QoS in both the capillary and the 3GPP domains can be matched, and alarms from both domains can be correlated to pinpoint faults.

Summary

As the Networked Society starts to take shape, a vast range of devices, objects and systems will be connected, creating the Internet of Things (IoT). Within this context, cellular networks have a significant role to play as connectivity providers, to which some things will connect directly, and another significant portion will connect using short-range radio technologies through a capillary network.

Cellular networks can provide global connectivity both outdoors and indoors by connecting capillary networks through special gateways. However, achieving this will require some new functionality.

Due to the massive numbers of connected things, functionalities – such as self-configuring connectivity management and automated gateway selection – are critical for providing everything in the capillary network with a reliable connection.

To ensure that communication remains secure and trustworthy, a security bridge is needed between the capillary and the cellular domains. With this functionality in place, a future network can provide optimized connectivity for all connected things anywhere no matter how they are connected.

References

1. Morgan Stanley, April 2014, Blue Paper, The 'Internet of Things' Is Now: Connecting The Real Economy, available at: http://www.morganstanley.com/views/perspectives/
2. J. Höller, V. Tsiatsis, C. Mulligan, S Avesand, S. Karnouskos, D. Boyle, 1st edition, 2014, From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Elsevier, available at: http://www.ericsson.com/article/from_m2m_to_iot_2026626967_c
3. Alcatel Lucent, Ericsson, Huawei, Neul, NSN, Sony, TU Dresden, u-blox, Verizon Wireless, White Paper, March 2014, A Choice of Future m2m Access Technologies for Mobile Network Operators, available at: http://www.cambridgewireless.co.uk/docs/Cellular%20IoT%20White%20Paper.pdf
4. Ericsson, NSN, April 2014, LTE Evolution for Cellular IoT, available at: http://www.cambridgewireless.co.uk/docs/LTE%20Evolution%20for%20Cellular%20IoT%2010.04.14.pdf
5. Emerging Telecommunications Technologies, April 2014, T. Tirronen, A. Larmo, J. Sachs, B. Lindoff, N. Wiberg, Machine-to-machine communication with long-term evolution with reduced device energy consumption, available at: http://onlinelibrary.wiley.com/doi/10.1002/ett.2643/abstract
6. 3GPP, TR 36.888, June 2013, Study on provision of low-cost Machine-Type Communications (MTC) User Equipments (UEs) based on LTE, available at: http://www.3gpp.org/DynaReport/36888.htm

Ericsson Review

To bring you the best of Ericsson's research world, our employees have been writing articles for Ericsson Review – our communications technology journal – since 1924. Today, Ericsson Review articles have a two-to-five year perspective and our objective is to provide you with up-to-date insights on how things are shaping up for the Networked Society.

Address:
Ericsson
SE-164 83 Stockholm, Sweden
Phone: +46 8 719 00 00

Publishing:
Ericsson Review articles and additional material are published on: www.ericsson.com/review. Use the RSS feed to stay informed of the latest updates.

Ericsson Technology Insights
All Ericsson Review articles are available on the Ericsson Technology Insights app available for Android and iOS devices. The link for your device is on the Ericsson Review website:www.ericsson.com/review. If you are viewing this digitally, you can:
download from Google Play or
download from the App Store

Publisher: Ulf Ewaldsson

Editorial board:
Hans Antvik, Ulrika Bergström, Joakim Cerwall, Stefan Dahlfort, Åsa Degermark, Deirdre P. Doyle, Dan Fahrman, Anita Frisell, Geoff Hollingworth, Jonas Högberg, Patrick Jestin, Cenk Kirbas, Sara Kullman, Börje Lundwall, Hans Mickelsson, Ulf Olsson, Patrik Regårdh, Patrik Roséen, Gunnar Thyrsin and Tonny Uhlin.

Editor:
Deirdre P. Doyle
deirdre.doyle@jgcommunication.se

Subeditors:
Paul Eade, Nathan Hegedus and Ian Nicholson

Art director and layout:
Carola Pilarz

Illustrations:
Claes-Göran Andersson

ISSN: 0014-0171

Volume: 91, 2014

Joachim Sachs

is a principal researcher at Ericsson Research. He joined Ericsson in 1997 and has worked on a variety of topics in the area of wireless communication systems. He holds a diploma in electrical engineering from Aachen University (RWTH), and a doctorate in electrical engineering from the Technical University of Berlin, Germany. Since 1995 he has been active in the IEEE and the German VDE Information Technology Society (ITG), where he is currently co-chair of the technical committee on communication.

Nicklas Beijar

is a guest researcher at Ericsson Research in the Cloud Technologies research area. He joined Ericsson in 2013 to work with the Internet of Things and, in particular, he has been working on the capillary network prototype demonstrated at Mobile Word Congress 2014. His current focus is on cloud-based solutions supporting the IoT. He holds a D.Sc. in networking technology from Aalto University and an M.Sc. from the Helsinki University of Technology, both in Finland.

Per Elmdahl

is a senior researcher at Wireless Access Networks, Ericsson Research. He holds an M.Sc. in computer science and technology from Linköping University, Sweden. He joined Ericsson in 1990 researching network management and network security. He served as an Ericsson 3GPP SA5 delegate for seven years, working on network management. While his interest in the IoT began privately, he has worked on the subject professionally for the last two years, specifically on network management and Bluetooth Low Energy.

Jan Melen

is a master researcher at Ericsson Research in the Services Media and Network Features research area. He joined Ericsson in 1997 and has worked with several 3GPP and IP related technologies. He studied at the electrical engineering department at Helsinki University of Technology, Finland. He has been involved in several EU projects, IETF and 3GPP standardization. He has been leading the IoT related research project at Ericsson Research since 2011.

Francesco Militano

is an experienced researcher at Ericsson Research in the Wireless Access Networks department. He joined Ericsson in 2011 to work with radio architecture and protocols. At present, he is investigating the field of M2M communications with LTE and capillary networks. He holds an M.Sc. in telecommunications engineering from University of Siena, Italy, and a post-graduate degree in networks innovation and ICT sector services from the Polytechnic University of Turin (Politecnico di Torino), Italy.

Patrik Salmela

is a senior researcher at Ericsson Research focusing on security. He joined Ericsson in 2003 to work for Ericsson Network Security and moved one year later to Ericsson Research, where he focused for several years on the Host Identity Protocol. He has since been working on security topics related to 3GPP, Deep Packet Inspection, and most recently, the Internet of Things. He holds an M.Sc. in communications engineering from Helsinki University of Technology, Finland.

Ericsson
SE-164 83 Stockholm, Sweden
Phone: + 46 10 719 0000

ISSN 0014-0171
284 23-3239 | Uen