ERICSSON WHITE PAPER
Uen 284 23-3269 | June 2017

ERICSSON

5G SECURITY

SCENARIOS AND SOLUTIONS

Security and privacy are cornerstones for 5G to become a platform for the Networked Society. Cellular systems pioneered the creation of security solutions for public communication, providing a vast, trustworthy ecosystem – 5G will drive new requirements due to new business and trust models, new service delivery models, an evolved threat landscape and an increased concern for privacy.

INTRODUCTION

5G systems are the next step in the evolution of mobile communication. As a fundamental enabler of the Networked Society, 5G networks need to provide capabilities not only for voice and data communication as we know it today, but also for new use cases and new industries, and for a multitude of devices and applications to connect society at large.

Research and standardization have started in many technology areas of fundamental importance for 5G (such as cloud and the Internet of Things). These efforts have achieved various degrees of maturity, although the definition of 5G mobile networks has not yet reached standardization phase in the 3GPP.

The evolution of LTE is a vital part of 5G. However, 5G will include the evolution of all parts of the network, such as core and management systems, as well as all protocol layers ranging from radio to applications. As a result, security is potentially affected everywhere.

Current 4G cellular systems provide a high level of security and trustworthiness for users and operators. Second generation (GSM) systems were the first to have standardized, built-in security functions, which then evolved through 3G and now 4G networks. Although the security designs of previous and current systems have provided a platform of undisputed socioeconomic success, with the number of global mobile subscriptions exceeding 7 billion in 2014 [1], 5G introduces many new aspects that require the following important questions to be addressed:

- Are there fundamentally new security requirements, and if so, how should they be identified?
- Can 5G security be a carbon copy of 4G security?
- Are previous design approaches still valid?

It is easy to think of 5G networks as mainly a quantitative evolution similar to previous transitions, such as higher bitrate, lower latency and more devices. But this is not the case: 5G security will just as much be a qualitative leap forward to meet the demands of a Networked Society.

2G-4G SECURITY RATIONALE

Some 25 years ago, when GSM systems were developed and standardized, security functions were introduced partly because of shortcomings discovered in previous analog systems, but also because of emerging threats.

First of all, encryption of the radio interface was introduced. With earlier systems, use of simple radio receivers enabled eavesdropping on conversations through mobile communication. However, at the time, export and public use of encryption was a contentious issue, which resulted in a design of only moderate strength. Nevertheless, it was regarded as strong enough for the estimated economic lifetime of GSM at that time (roughly 10 years).

Secondly, risk of fraud – such as making calls charged to other subscribers – was considered a major problem. This led to the introduction of a tamper-resistant SIM card, adding strong authentication of the subscriber and, consequently, a strong binding to robust charging.

Finally, subscriber privacy entered the scene, and a mechanism with randomly assigned temporary identifiers was introduced to make it harder to track or identify subscribers.

Moving to 3G, further security improvements were made. Examples include mutual authentication to mitigate threats of rogue radio base stations, and moving the encryption deeper into the network and making it state-of-the-art in terms of strength.

When the 4G LTE standard was set, the main additional security measures were a consequence of returning the user data encryption down to the base station. Specifically, more elaborate key management was introduced to protect against potential physical break-ins to radio base stations. Overall, the security offered by LTE is very similar to the strong protection of 3G.

Reflecting on the rationale behind 2G-4G security, it can be said that security was introduced to protect a basic connectivity service (voice and later packet data) in order to earn users' trust in terms of privacy, and to safeguard the ecosystem in terms of correct charging. Indeed, it must be acknowledged that this has worked extremely well. Although some attacks on GSM security have become possible over the past 10 years, this was beyond the economic lifetime for which GSM was originally designed. GSM security goals were therefore met and exceeded. Furthermore, all generations of mobile networks offer completely zero-config security from the user's point of view, thanks to automatic provisioning through SIM and universal SIM (USIM) cards. However, 5G will drive additional requirements regarding security.

SECURITY CHARACTERISTICS OF 5G

DRIVERS FOR 5G

So far, the drivers for mobile network evolution have mainly been about improving throughput and latency, and being able to better support the mobile internet. The drivers for security have remained in place to provide a trustworthy basic connectivity service. This basic trust will continue to be a driver for 5G networks as a high data-rate, mobile broadband service. However, additional key driving factors will enter the scene.

First of all, 5G networks will be designed to serve not only new functions for people and society, but also to connect industries (such as manufacturing and processing, intelligent transport, smart grids and e-health). With 5G, it is possible to foresee new models of how network and communication services are provided. For example, a car manufacturer may wish to provide management services for cars. Establishing direct roaming agreements with various access network providers could be a cost-efficient way to achieve this. Similarly, the concept of terminal/device will change: unattended machines and sensors will connect; sometimes entire capillary networks comprising tens or hundreds of individual devices will simultaneously attach to the 5G network.

Next, new service delivery models will be used, involving new actors in the ecosystem. Cloud and virtualization technologies and anything-as-a-service will be used to reduce costs, and to deploy and optimize services more rapidly. Telecom networks will expose application programming interfaces (APIs) toward users and third-party service providers to a higher degree, for example, for the purpose of optimized delivery using location awareness, content adaptation and caching. Such optimizations will sometimes be provided by third-party software executing on shared hardware platforms alongside dedicated telecom software.

Furthermore, general awareness of user privacy in society has increased, leading to a greater focus on the protection of user metadata and communication. This issue becomes even more central with the developments in big data analytics.

What characterizes 5G, even more than 4G, is that it will have a crucial role in the operation of society. The full scope of security, privacy and resilience will be a concern that spans far beyond technology. It will ultimately impact legal frameworks, regulation and actions by commercial entities and individuals. There will be increased regulatory involvement in how entire 5G systems will operate.

IMPLICATIONS FOR SECURITY AND PRIVACY

The drivers listed above can be grouped into four characteristics of 5G networks and their usage, each with implications for security and privacy. These characteristics are: new trust models, new service delivery models, an evolved threat landscape, and increased privacy concerns.

So, how do these characteristics affect the way we need to approach security and privacy in 5G? Are there technological or other types of limitations in current 4G security?

New trust models

Trust models change over time. As a simple example, consider the bring-your-own-device trend in enterprises. Previously, all user devices could be assumed to be trustworthy, as they were all of the same type, all issued and managed by the corporate IT department. Today, users want to use their personal devices instead, posing threats as potential Trojan horses behind corporate firewalls.

For current mobile systems, the trust model is rather straightforward, involving a subscriber (and their terminal) and two operators (the home and serving networks). Since 5G is aimed at supporting new business models and involves new actors, trust models will change, giving rise

to extended requirements in areas such as authentication between various actors, accountability and non-repudiation. For example, for new critical services such as public safety, what security requirements will be projected onto the 5G networks?

The new types of devices will span an extremely wide range of security requirements and will at the same time have very different security postures: industry automation control devices, shipping containers, vehicles forming entire capillary networks, tiny climate monitoring sensors and, next-generation tablets and smartphones.

Devices have so far been assumed to comply with standards and not to deliberately attempt to attack networks. But how well protected are very low-cost devices? Can a single connected device be used as a stepping stone for cyber-attacks deep into the system? And what is the attack surface of a 5G system with billions of inexpensive, connected devices?

The existing trust model obviously does not capture this evolved business and technological scenery of 5G. To ensure that 5G can support the needs of new business models, and ensure sufficient security, the trust model map must be redrawn. As such, this does not necessarily mean completely redesigning security. However, it is crucial to identify any significant shortcomings. This must begin by defining a new trust model.

Security for new service delivery models

The use of clouds and virtualization emphasizes the dependency on secure software, and leads to other effects on security. Current 3GPP-defined systems are based on functional node specifications and abstract interfaces (reference points) between them, and as such provide a good starting point for virtualization. Until now, however, dedicated/proprietary hardware has still often been used for these nodes and interfaces. Decoupling software and hardware means that telecom software can no longer rely on the specific security attributes of a dedicated telecom hardware platform. For the same reason, standard interfaces to the computing/network platforms – such as those defined by ETSI (the European Telecommunications Standards Institute) in their Network Functions Virtualization work – are necessary to ensure a manageable approach to security.

When operators host third-party applications in their telecom clouds, executing on the same hardware as native telecom services, there are increased demands on virtualization with strong isolation properties.

Evolved threat landscape

5G networks will serve an even more central role as critical infrastructure. Many people will have already experienced occasions when fixed telephone lines, internet access and the TV service have all stopped working at the same time during a major network outage. And societies certainly do not want to lose electrical power, mobile telephony and more at the same time.

Today's networks host various values – examples include revenue streams and brand reputation. The accessibility of these values via the internet has already attracted hacktivists, underground economies, cybercrime and cyber-terrorists. The values hosted in, and generated by, the 5G system are estimated to be even higher, and the assets (hardware, software, information and revenue streams) will be even more attractive for different types of attacks. Furthermore, considering the possible consequences of an attack, the damage may not be limited to a business or reputation; it could even have a severe impact on public safety.

This leads to a need to strengthen certain security functional areas. Attack resistance needs to be a design consideration when defining new 5G protocols. Questionable authentication methods such as username/password need to be phased out. More fundamentally, however, the new threats emphasize the need for measurable security assurance and compliance; in other words, verifying the presence, correctness and sufficiency of the security functions. Those using 5G will need answers to questions such as: is it safe to deploy a virtual machine on a given piece of hardware? And what security tests have been applied to the software?

A key asset of the Networked Society will be data. The role that data currently plays in processes such as decision-making and value creation is changing. Being in control of personal data will be crucial for operational reasons, but this will also increase in importance in order to create competitive advantages. As the carriers of this data, 5G networks will need to provide adequate protection in the form of isolation and efficient transport of protected (encrypted/authenticated) data.

The ubiquity of 5G devices and connectivity will not only affect the technological attack surface; the exposure to social engineering attacks will also increase. People claiming to be work

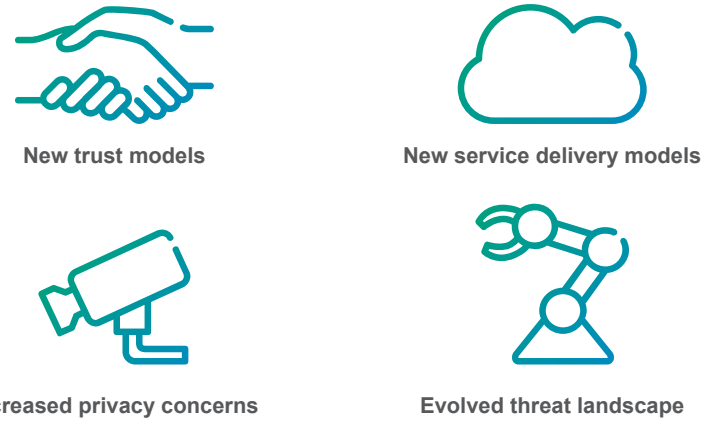

Figure 1: The defining characteristics of 5G security.

colleagues or repair technicians, for instance, may contact an individual and request various kinds of access – not only to the individual's information, but also to their devices.

Increased privacy concerns

There have been several recent news stories related to allegations of mass surveillance. Reports have also emerged of rogue base stations tracking users in major cities, and of extracting personal data without user knowledge. The protection of personal data has been discussed within the framework of the EU. It is being reviewed in standardization bodies such as the 3GPP and the IETF (Internet Engineering Task Force), and debated in many other forums.

A particularly sensitive asset is the user identifier(s). Ever since 2G, user privacy has been an important consideration. However, the benefits of full International Mobile Subscriber Identity (IMSI) protection have so far not seemed to outweigh the complexity of implementing it.

THE ROAD AHEAD

STANDARDIZATION APPROACH

Accepting that 5G security needs are not mainly driven by increased bitrates and other quantitative aspects, there is also a need to avoid the temptation of addressing 5G security solutions as a quantitative issue. In the main, the level of 5G security is not defined by the number of security mechanisms specified. On the contrary, trying to address all possible requirements of every stakeholder in the same network could well lead to a reduced security level, or at least to a solution with security properties that are difficult to grasp. The first requirement is rather a well-designed, flexible security baseline, and assurance in the implementation of this baseline will be more important than the number of requirements as such.

A multi-stakeholder approach involving operators, vendors, regulators, policy-makers and representatives of 5G users (for example, industry segments) is fundamental to the security baseline of trustworthy, cost-efficient and manageable 5G networks. Pre-standardization consensus building, such as joint research by the different stakeholders, will be important.

One example of such an initiative is the 5G for Sweden research program. This is a joint collaboration between academic institutions, telecom companies and other industries, with the purpose of taking a leading position in digitalization. Another example is 5G-ENSURE, which is a cooperation between equipment vendors, operators, academic institutions and SMEs. This EU Horizon 2020 project will study the 5G security architecture and build basic enablers for 5G, such as network virtualization and identity management. A lack of such efforts can have a detrimental effect on time to market. For example, during the 4G LTE standardization phase, there was almost one year of discussions within the 3GPP before a decision could be made on whether to allocate radio interface protection in the eNodeB or in the core network. ETSI (3GPP) and the IETF will continue to be two important standardization bodies for 5G security, and defining a new trust model will be one of their first priorities.

Depending on the role that 5G aspires to play in new usages – for example, for enterprises, public safety and industrial automation, standards defined (or to be defined) by bodies such as the ISO (International Organization for Standardization), the IEC (International Electrotechnical Commission) and the CSA (Cloud Security Alliance) will also have an impact on the technology. Open source has already started to play a role in the development of 3G and 4G networks, and its importance will likely continue to grow.

CORE 5G SECURITY TOPICS

Security assurance

As discussed, it is likely that 5G networks will play an even more central role as critical infrastructure than earlier generations, and that security assurance will enter the picture to a higher degree. This is not a completely new development. The 3GPP has already observed the need to extend security specifications from functional ones for interfaces to assurance specifications on the node/interface implementations, and has initiated work known as SECAM. However, in combination with cloud-based implementation (virtualization and on-demand service) there is a likely need to separate software assurance more concretely from platform assurance, and to allow on-demand measurements of assurance as part of Service Level Agreements (SLAs) and orchestration.

Regarding the role of 5G networks as critical infrastructure, a decision must be made on just how critical these should be, since increasing criticality comes with a price tag in terms of assurance. The standard assurance for IT products is Common Criteria (ISO 15408). If 5G is to become a general platform for the Networked Society vision, it seems clear that Common Criteria compliance could enter as an additional assurance requirement on top of SECAM. However, the impact may not stop there.

Assume that in some use cases, vehicle/road safety would be dependent on 5G network security. What does this imply? Today, safety-related car systems need to follow very comprehensive standards, such as ISO 26262. This is a 10-part standard, where, for example, part six covers safety related to software. Similarly, the health care sector is governed by standards such as ISO 27799 and, in the US, the HIPAA (Health Insurance Portability and Accountability Act). For smart

grids, demonstrated compliance with standards from the IEEE (Institute of Electrical and Electronics Engineers), the IEC and the NIST (National Institute of Standards and Technology) may apply. If 5G security becomes a critical link in the control loop of all of these applications, would it imply that 5G networks need to be certified against (parts of) all these standards? Although there will most likely be many overlapping compliance requirements, it is clear that considerable costs will be incurred on 5G network products. Will these costs be prohibitive and prevent 5G from providing valuable services to these applications? The answer is no, and there are at least two ways to handle this security overload on the 5G network.

First, the concept of network slicing could be an important tool to handle the very diverse requirements of different applications and user groups. Slicing is often seen as a way to provide isolated sub-networks, each optimized for specific types of traffic characteristics. One such characteristic could be related to security and safety requirements. By having a properly implemented, high-assurance isolation mechanism to support slicing, it will be possible to confine the impact of security requirements to single slices, rather than the whole network. The cost of high assurance and certification can therefore be concentrated onto an infrastructure virtualization/ isolation layer.

The general approach could be to define a limited number of standardized, interoperable, high-assurance security enablers that are present in all slices as a baseline. On top of this, more application-specific security mechanisms are enabled by boot-strapping into specific slices, providing the additional security functions. Indeed, with a properly operating virtualization layer, external parties such as enterprises could securely deploy their own (certified) software inside the 5G network, thereby offering governance to organizations using 5G, and at the same time reducing the number of certifications that the 5G network must undergo.

Secondly, we have the choice to "factor out" security requirements from the 5G network slices by simply putting the responsibility in the endpoints; in other words, in connected devices or organization data centers. Data security is an example of a service that could be handled this way.

In summary, the fact that 5G is designed to be a platform for a wide range of new user groups and applications does not automatically mean that it is necessary (or even desirable) for the 5G network to carry all security responsibility and related costs. On the other hand, 5G networks clearly can provide some highly valuable security services. Besides the isolation/slicing itself, many other examples of network-enabled security as a service will be attractive to multiple user groups, including network enforced security policies, authentication, key management and data security services.

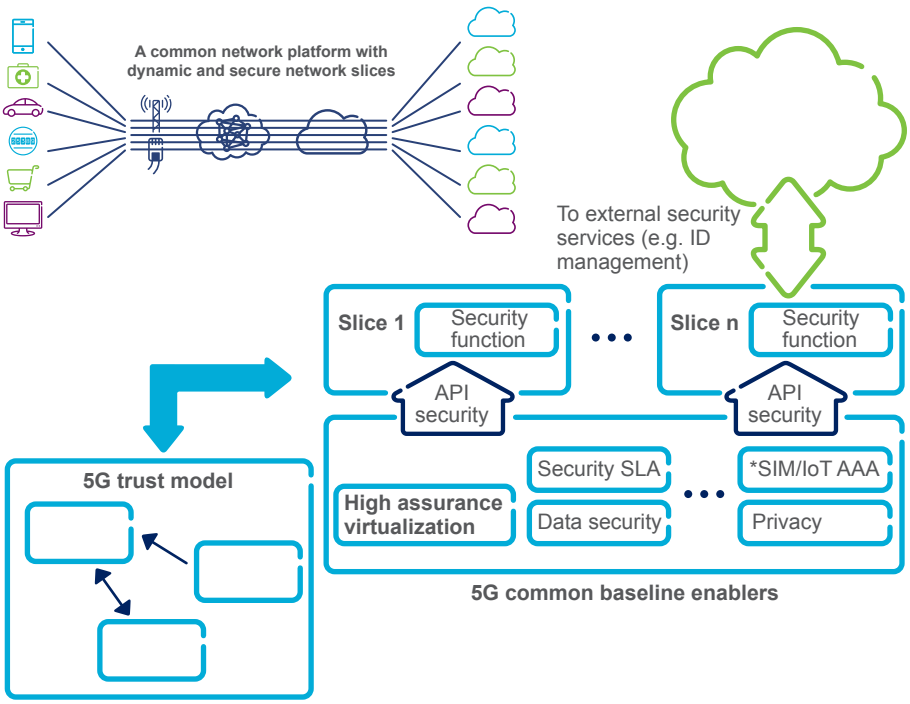

Figure 2: High-level 5G security principles.

Identity management

The 4G LTE standard requires USIM on physical Universal Integrated Circuit Cards to gain network access. This way of handling identity will continue to be an essential part of 5G for reasons such as the high level of security and user friendliness. Embedded SIM has also significantly lowered the bar for deployment issues related to machine-to-machine communication. Still, there is a general trend of bring-your-own-identity, and the 5G ecosystem would generally benefit from a more open identity management architecture that allows for alternatives. One example would be to allow an enterprise with an existing, secure ID management solution to reuse it for 5G access. Examining new ways to handle device/subscriber identities is therefore a key consideration that should enter the investigation of the new trust models for 5G. Concepts such as network slicing can provide an enabler for securely allowing different ID management solutions side-by-side by confining usage to virtual, isolated slices of the network.

The threat of IMSI catching, where rogue radio network equipment requests mobile devices to reveal their identity, was discussed during the 3G and 4G standardization process. However, no protection mechanism was introduced at that time, as the predictable threats did not seem to justify the cost or complexity involved. It is not clear whether this risk analysis is still valid, and enhanced IMSI protection deserves consideration for 5G.

5G radio network security

Due to the evolved threat landscape and new technology that provides users with low-cost alternatives to program their own devices (even at radio access level), the attack resistance of radio networks should be a more clearly outspoken design consideration in 5G, analyzing threats such as Denial of Service from potentially misbehaving devices, and adding mitigation measures to radio protocol design.

Although LTE radio access has excellent cryptographic protection against eavesdropping, there is no protection against modifying or injecting user plane traffic. With 5G radio access as a building block in, for example, industrial automation, the potential benefits of adding integrity protection seem worthy of investigation.

Flexible and scalable security architecture

With virtualization and more dynamic configurations entering the picture for 5G, it seems logical to consider a more dynamic and flexible security architecture for it. Security for synchronous aspects like RAN signaling could be located close to the access with a higher degree of independence from asynchronous security aspects, such as those related to the user plane, than today. This would allow for more efficient security handling, and limit threats to sensitive user data at the same time.

New security designs with higher flexibility could also better address unnecessary conflicts between usability and security. For example, new network APIs could allow the network to perform service chaining, such as traffic optimizations, while still allowing data to be encrypted end-to-end.

Energy-efficient security

While security services such as encryption come with a cost, the expense is no longer an issue for mobile phones and similar devices. The energy cost of encrypting one bit is one or two orders of magnitude less than transmitting one bit [2]. However, for the most constrained, battery-dependent devices with a long target life time, there may be a need to consider even more lightweight solutions, as every micro joule consumed could be of importance.

Cloud security

Cloud security is already an extremely hot topic, and it will be added to the list of 5G concerns. Entire books have been written on this subject, so there follows just a brief list of priorities for cloud security in a 5G context, motivated by the discussions above.

- Develop hypervisors and network virtualization with high assurance on isolation. As mentioned, investments in this area could pay off, as this would greatly simplify the handling of diverse security requirements in the same infrastructure.
- Build useful ecosystems and architectures from existing trusted computing tools and concepts for remote attestation, for example.
- Provide more efficient solutions for cloud-friendly data encryption (homomorphic encryption, allowing operations on encrypted data).
- Develop easy-to-use, trusted management of cloud systems and the applications that run there.

Some of these continue to represent essential academic research topics.

CONCLUSION

Revisiting the questions posed in the introduction, here are the conclusions drawn from the discussion above.

Are there fundamentally new security requirements, and if so, how should they be identified?
Three of the four drivers for 5G security (new service delivery models, evolved threat landscape, and increased focus on privacy) involve new requirements. The fourth driver, new trust models, requires an analytical approach to identifying the requirements. Here, it should be reemphasized that a good security solution is not defined by the number of security requirements.

Can 5G security be a carbon copy of 4G security?
If 5G had only been about bitrates, for example, the answer would likely be yes. However, as 5G will act as a pillar for the Networked Society, additional aspects need to be considered.

Are previous design approaches still valid?
Many of them are still valid. For example, the 3GPP's approaches for 3G and 4G – which brought the industry highly secure radio and core network protocols, subscriber authentication and more – are largely still valid. However, there must also be new considerations for 5G security design. Most notably, trust models must be revisited, and new aspects such as potentially misbehaving entities and devices should be catered for. Greater emphasis also needs to be placed on the assurance side, and it is important to account for completely new stakeholders and the extent to which they and their businesses will be dependent on 5G security design.

5G can, and will, be a cornerstone in realizing the vision of the Networked Society, in which everything that can benefit from a connection will be connected. But instead of tackling 5G security by trying to implement all imaginable security mechanisms, there needs to be a systematic and analytical multi-stakeholder approach, anchored in a new trust model for 5G networks. This will deliver an evolved 5G security architecture that will be able to provide a trustworthy platform for this vision. A few specific evolutionary technical topics have also been identified in this paper: identity management, radio network security, flexible and scalable security architecture, energy efficient security and cloud security,

From a security point of view, however, it is important to note two things. First, the Networked Society vision does not unconditionally state that everything will be connected – only those things that benefit from being connected. Secondly, although the vision includes a connection, this connection does not necessarily have to be to one and the same global 5G system. The benefits of being connected must outweigh the risks of being potentially "reachable" from more or less anywhere on the globe.

The threat landscape in which mobile networks operate has gradually changed since 2G was designed. Through evolved security solutions, successive generations of 3GPP mobile networks have stayed trustworthy and remain a highly secure and convenient way to access services and information. Although 5G faces far more dramatic cyber-security challenges, by using the right design approach, 5G networks will be able to meet growing demands for security and privacy.

GLOSSARY

API	application programming interface
ETSI	European Telecommunications Standards Institute
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
ISO	International Organization for Standardization
SECAM	Security Assurance Methodology
SLA	Service Level Agreement
USIM	universal SIM

REFERENCES

1. Ericsson, Ericsson Mobility Report, June 2015, available at: http://www.ericsson.com/ericsson-mobility-report
2. C. Margi, B. Trevizan, G. de Sousa, M. Simplicio, P. Barreto, T. Carvalho, M. Näslund, R. Gold, “Impact of Operating Systems on Wireless Sensor Networks (Security) Applications and Testbeds”, Proceedings of ICCCN 2010, pp. 1-6, 2010.