NEW SECURITY CHALLENGES IN M2M NETWORKS

Aleksandar Obradović, Bojana Jakovljević, Gorica Nikolić, Nemanja Ognjanović
Telekom Srbija a.d.

Abstract - *Machine to machine (M2M) technology is bringing benefits to humans, as well as the new market opportunities for M2M device manufacturers, service providers, and Telco operators. On the other hand, the deployment of M2M technologies is raising numerous challenges, in the first place those in security, which are not encountered in traditional communication networks, and therefore not answered yet. Due to the low cost and mass deployment nature of M2M devices and infrastructure developed so far for their support, security issues are not fully addressed by the existing wireless devices and standard cellular networks. An overview of new security challenges for M2M networks is given in this paper.*

Keywords- M2M; security; cost; scale; unattended devices; trust; network complexity; aplication layer complexity;

1. INTRODUCTION

M2M implies the use of a device in order to capture a certain event (temperature, humidity, velocity, blood pressure etc) and represent it in a form of transferable information. This information is then transferred over the communication network (wired or wireless) towards an application (software program) where the event is processed.

Due to a large number of deployed M2M devices, global security policy enforcement for all devices is not the best solution because it would lead to inefficiency and increased costs. M2M networks accepted the global trend by which some of the enforcements are delegated to trusted entity. A trusted entity is an entity whose behaviour is predictable. This model of delegation is considered as suitable for M2M networks and it involves balancing between the trust and enforcement.

M2M devices are typically deployed to operate without human intervention and, after deployment, M2M devices rely on remote management of their functionality as well as on subscription management.

There is a number of possible attacks against either M2M device (attack against unattended devices may include physical, protocol, configuration or cloning attacks etc) or M2M infrastructure (attacks on the core network). In order to understand possible treats this paper gives an overview of the most important issues regarding emerging security challenges in M2M communication.

2. LOW ENERGY/LOW OVERHEAD

Having in mind that in M2M networks, the majority of M2M devices may be unattended for a long period of time, it is justified to assume that those M2M devices would be highly constrained regarding energy consumption. For such devices, crucial issue is how to provide reliable and long lasting power supply. The possible solutions are the use of longer lifespan batteries, or use and storage of energy from natural environment (for example solar energy). In terms of "low security overhead", the overhead of energy consumption is minimized for the purpose of security. It is possible to establish relation between the energy consumption minimization and different kinds of overhead decrease.

It is also possible to investigate security in terms of energy consumption [1]. The power consumption can be considered as a function of the running cryptographic algorithms within device, data overhead for security and infrastructure parameters like time between re-authorization and the number of layers defined for security.

A. Computing cryphtocraphic alghoritms

There are three factors that fully define security in almost every cryptographic system, and those are: **randomness**, **unpredictability** and **secrecy** of the key [2]. Some of the cryptographic protocols used require a random generator, but in general real randomness is hard to achieve. For example, pseudo-randomness is requiring a lot of computing and the presence of a non-volatile memory. In order to minimize the cost overload it is possible to use the same cryptographic primitive both for generation of the pseudo-random number and for the protection of the data confidentiality or authentication/integrity [3]. It is expected that lightweight hash functions are going to be standardized in near future.

B. Data overhead

The main challenge is the protection of the confidentiality when short plaintext messages are transmitted from the low power M2M devices. Stream-ciphers and block-ciphers are recommended for the use in M2M networks because public-key encryption is not suitable due to bad impact on the size of the ciphered text.

Significant overheads are expected from message headers as well as inability of further compression of the already encrypted data. For example, it is not possible to compress IP packets if the IPsec is used. As a consequence, an entire IP packet is sometimes used to transmit a single bit of data. That is the reason why it is necessary to keep the encryption process at the lowest layer possible and to enable data and header encryption before data encryption.

C. Infrastructure parameters

Scenarios in which M2M device is working within existing network infrastructure are those where the biggest overhead is expected. Moreover, these scenarios imply that the device must interwork with protocols inherited from LTE, 3G or GSM networks, also on a layered IP or even use HTTPS for communication process with M2M service provider, thus requiring HTTP stack and the support of TCP. On the other hand, it is possible to have more complex security issues in case

of binding to an unacknowledged protocol (UDP) such as CoAP (Constrained Application Protocol).

Regarding power consumption, special attention should be paid in case of several layers of encryption and integrity. In this case overheads are being created in all aforementioned ways. This raises the question of possible omitting or collapsing of layers.

3. COST&SCALE

A. Cost

At this moment, M2M device price trend is 4-5 Euros per device. This price is close to the price of a SIM card with a secure element. The question already raised is if it is possible to decrease the cost of a secure element. By now, the costs linked both with conventional SIM cards, as well as with the soft SIM (the case where both network residency and Home Location Register (HLR) costs are present) are extremely high.

This section is presenting an estimate of the total cost for the support of a single M2M device within the cellular network. Calculation is based upon assumptions for the LTE M2M networks [4], using data inputs from existing 2G and 3G Telekom Srbija's mobile network.
It is important to underline the assumption that each M2M end device will have initial network cost as well as a capacity cost. The capacity cost is included in total cost calculation even when the device is used, but not generating any data.

The cost estimate is done by simplifying the SIM distribution process. In this calculation it is assumed that SIM cards are already delivered from SIM vendors to the M2M providers. The distribution in reality can be much longer: from SIM vendor, to the MNO after which SIM cards are resold to the end customer. Such channels of SIM distribution include much higher expenses.

Table 1 shows relevant factors with cost estimates taken into account for cost prediction for individual M2M device. A particular M2M device cost will include a network cost in a range of 2-3 Euros, and for each SIM attached over GPRS with active session an extra fee of 2-3 Euros.

TABLE I. COST ESTIMATE FOR M2M DEVICE DEPLOYMENT

Cost element	***Costs produced by***	***Cost estimate***
SIM card (hardware itself)	Requisition and purchase of SIM cards and their delivery to device manufacturer. (M2M SIM may need extended temperature range and non-removable fitting)	€1-€2 (per each SIM)
Allocation of IMSI and MSISDN	Each SIM will have unique IMSI and MSISDN allocated from MNO ranges	negligible e.g. there may be no MSISDN
HSS/AuC capacity	Every SIM must have matching HSS & AUC entry (even if never subsequently used)	€0.25 (per each SIM)
MME/VLR Capacity	Every IMSI-attached SIM will need space in an MME/VLR even if it generates no mobility or user plane traffic. Most M2M devices are to be permanently IMSI attached and if so then wake up messages can be delivered.	€1 (per each SIM)
SGSN (VLR) Capacity	Every GPRS-attached SIM will need space in an SGSN even if it generates no mobility or user plane traffic. This ensures that the majority of M2M devices will GPRS attach only when required and detach when finished.	Applicable in 2G/3G networks. For LTE it is merged with MME costs.
SGW SAU Licence capacity	For each Simultaneously Attached User (SAU) it is required licensed capacity on SGSN. This allows GPRS sessions to be deterred from being left established and as well to activate PDP-Contexts only briefly, when data transfer is required.	€1 (per SAU) It may disappear under future licensing models
PGW SAU Licence capacity	If SGW is combined with PGW then this is a shared cost.	€1 (per SAU)
IT element costs (e.g. account management costs & possible SIM distribution model)	Provisioning System, Billing Systems, CUR etc.	Highly variable, should be minimized for M2M

Almost every revenue model is traffic based. However, in M2M networks such model is not correct, due to the fact that M2M devices are generating low rate data traffic. This could be overcome at some level by signing commercial agreement with the customers (inside the home network). However, the problem of data roaming costs (national and international roaming) remains because signed roaming agreements are valid no matter what kind of devices are attached and what amount of data they are generating. It is clear that in such situations costs are in disproportion to the generated revenue.

Although it seems there is nothing to be done, it is possible to protect the operators from some unwanted end device behaviour by introducing some kind of compensation, such as cost penalty or by introducing core element which would be able to restrict the resource usage.

B. Scale

According to Wireless World Research Forum (WWRF) view [5], it is possible that there would be trillions of M2M connected devices in the future. Such a large number of M2M devices will be used in various use cases and scenarios defined for M2M communication. As a consequence, the requirements for M2M devices are different. Even with a projection of smaller number of deployed M2M devices, the price per

individual device for management of the device itself and its associated account is crucial.

The term account management in cellular networks is used for the process of association of encryption Key and IMSI with a dedicated subscriber, as well as for the process of assignment of dedicated identifiers for the user (such as an MSISDN). This process includes generating and keeping different subscriber records in various network entities, like HSS (HLR in 2G/3G), the MME (SGSN in 2G/3G) and the Serving Gateway/PDN Gateway (GGSN in 2G/3G). Some of these nodes together with their associated records cause typical cost impacts on M2M device deployment.

Account management function, which is one of the core network functions, is very important in the M2M management chain. It is in charge of Call Data Record (CDR) generating process, CDRs collecting process and forwarding them towards either mediation/billing or prepaid systems. This is further reflected on other customer management systems (like SubAdmin, online billing, prepaid top-up and customer care).

Aforementioned charging systems, along with special customer management systems, have specific customization for the particular country, or for the each operator based on a regulatory requirements or tariff terms. While interoperability is a must, and certain common features are implied (the exchange of CDRs for roaming subscribers), it is basically up to the each Mobile Network Operator (MNO) how they would cope and organize their billing arrangements.

It is possible to predict that high number of M2M devices will require access to wide-area mobile networks. A single M2M device can only require sporadic authentication and it also can be equipped with some standard equipment which would allow a connection to at least one access network when the connection is needed. Having in mind that the constant need for authenticating each M2M device can be demanding, it also may reduce the benefits gained from certain M2M services, especially those based on a low cost machine/service ratio.

Taking into account the fact that standard provisioning of mobile telephones and data cards/modems with SIMs can be time-consuming and complicated process, it is clear that SIM provisioning of M2M devices will only increase problems due to a large number of devices and their degree of use (low and sporadic frequency of use). Therefore, it is expected that as the number of M2M applications is increasing, so will the number of the unused or infrequently used SIMs. Additional costs linked with provisioning or quarantining (keeping minimally active) will only make M2M devices more expensive. This can lead into situations where mobile M2M service does not satisfy low cost demand.

The practise and common sense have shown that authentication keys should be stored in hardware, since hardware environment is more secure and certified [6]. Such hardware can enable non-exportability of private content (crypto keys). In theory, devices may have a “soft SIM”, which means that they have a SIM module in software or hardware. However, such solution would represent a major security risk, and it would produce high costs for operators, since it would require the use of core network elements, in the first place HLR and authentication centre (AuC), and it would require a provisioning of a subscription per particular device.

Some new form of authentication is possible, but requires major network redesigning. Also, new solutions could jeopardize existing connections to 3G or GSM networks.

The conclusion is that the cost is the leading factor to be taken into account when deploying M2M devices which are provisioned and secured. Further traffic optimization for M2M use cases is expected. One of the possibilities for traffic optimization, from the operator point of view might be the use of a single bill which would match the consolidated number of devices.

4. UNATTENDED M2M DEVICES

In large number of M2M use cases, M2M devices are forming multiple capillary networks by connecting between themselves over PAN or LAN networks (they can use ZigBee, WiFi or Bluetooth). One of the possible architectures for this study is the one used in EXALTED, namely LTE-M (“LTE for Machines”) [7]. The goal of capillary network is either to provide connectivity for M2M end devices to communicate outside the capillary network through M2M gateways or simply to enable connectivity between M2M devices forming a capillary network itself.

M2M applications generally run on M2M devices without human intervention, and devices are pre-configured to run basic processes prior to their deployment in the network. In particular cases human intervention is possible but should be minimized. Furthermore, some M2M devices may be deployed in places where human intervention is not physically possible and these devices are called **unattended**. Unattended devices can be configured remotely after device bootstrap procedure that is automated by infrastructure entity. Such infrastructure entity must be AAA based, in order to support security requirements. Similar to initial device configuration, other processes can be done remotely, e.g. software updates, re-configurations etc.

A. Device chalenges

As M2M device becomes fully operable, which means that it can send and receive data from other nodes and networks, **remote authorization** must be provided. This is necessary because during application running, accessing devices to AAA must be provisioned with credentials which are satisfying the security requirements in terms of the protection of the transmitting/receiving data (confidentiality, integrity etc).

Lowering the communication overhead is the main challenge recognized from M2M device side. The process of overhead decrease is linked with remote procedures and it is carried out

by M2M devices which are resource-constrained oriented. The difference between the manual remote procedures and automated procedures is that automated require communication resources. Those resources are provided by the communication device itself, but in particular situations where messages are relayed trough intermediary devices the communication resources are provided within the network itself. The second big issue is the **stable connectivity**. Unreliable communication is known for its multiple retransmissions of the sent messages and that process is very expensive for M2M devices. Further on, M2M device should have the right to access the service infrastructure in following scenarios: each time when a device moves within the same network or each time when it moves from one network to another. Moreover, some M2M devices should be configured in a way that they could relay messages from other devices. That would enable the access to the network for a particular device trough other devices inside the network. In addition to this, M2M devices may have the possibility to support network access even trough network entities (such as gateways) and which are inside different administrative domains.

B. Infrastructure chalenges

M2M devices are relatively small physical devices (mostly battery operated), capable for exchange of information in real time with any other device via a local network. Such devices consist of a CPU, memory, low-power wireless interface and a lightweight operating system and they are deployed in a large numbers. Since the number of the deployed M2M devices is huge, the biggest issue is **how the infrastructure will manage that number of M2M devices.** It is not easy to answer to this question; however some of the security mechanisms (related to management) can be delegated to some other network entities (gateways, other M2M devices etc). This delegation process evidently leads to infrastructure offload. The real challenge is how to ensure delegation of services in a secure way down even to the end devices but without large changes in already deployed infrastructure. If this process is successful at the end than some frequent security operations (such as authorization, re-authentication) can be delegated easily and successfully.

Another important issue is the **communication process** between the M2M device and the management infrastructure. Communication path includes various entities (routers, gateways etc). Therefore, end-to-end security mechanisms are required from the remote management infrastructure as well as the support for inter-domain security procedures in situations where network entities reside in different administrative domains.

5. NETWORK AND APPLICATION LAYER COMPLEXITY

A. Network Complexity chalenges

1) Device mobility

Mobility of network devices became the common requirement in modern technologies. Devices are often integrated with moving machines, or they are carried by people. Also, edge routers and gateways can be mobile, so in both cases the access point to the Internet is constantly changing [8]. Since M2M networks support frequent topology changes (mesh, star topology, ad-hoc networks) certain degree of node mobility (frequent node join and leave) is possible. Further on, mobility based communication can increase communication between nodes and clusters within M2M networks.

Each time a mobile device is moving from an entity (gateway) where it has been authenticated at the beginning it has to repeat the authentication procedure on the new gateway in order to be allowed access to the network. The raising challenge **is how to allow a device authentication process while a device communicates simultaneously**. Possible solution to this problem is to use proactive approach, in which the gateway that is in charge of authentication procedure will send keys to all other possible gateways before the device does, or as a less proactive solution, it is possible that the new gateway will interrogate the old gateway in order to obtain the key material. The interrogation process in the second scenario is leading to speeding up the authentication procedure. **Therefore, it is of crucial interest for the authentication infrastructure to keep track of M2M device location and its mobility behaviour.**

Depending on the nature of the M2M network structure, M2M devices can move either separately or jointly in a bulk. Emerging problem with the bulk moving M2M devices is the re-authentication procedure, because it will lead to a large communication overhead at the network access domain. The real problem that should be solved here is to develop and propose re-authentication and network access control mechanisms which would be able to cope with this large overhead peak. One of the reasonable and cheap solutions is organizing the bulk devices into groups. Moreover, the movement of the bulk of devices can be coupled with the movement of the gateway itself. This would be helpful in a way that delegation mechanisms will be able to support handling re-authentication procedures of the bulk M2M devices.

2) Network topology and communication range

Since M2M networks are multi-domain networks, it is possible that M2M device can not directly communicate with the network of its administrative domain. Therefore, it is possible that M2M device will use other networks in which some of the domains have business relationship with its own administrative domain for the connection. Network access must be protected and the protection must be based on authentication procedures but within the existing multi-domain infrastructure.

The other problem that can emerge in M2M networks is limited communication range of M2M devices therefore they might not be able to reach the gateways directly, without hoping. In this particular case, M2M device depends on other devices which can relay request messages from initial M2M device towards the gateway. Example of the request message that needs to be relayed is an authentication request message. Intermediary devices relay authentication messages from M2M devices towards gateway. After successful authentication, all

cryptographic keying material which is needed for secure packet relaying will be provided to M2M devices in order to establish link-layer security associations.

B. Application Layer Complexity

Since the deployment of M2M networks is taking place now, it is reasonable to expect that various M2M service providers are already offering their services in order to enable the deployment of M2M applications. At the same time, the most important standardization bodies, like ETSI or 3GPP are shaping their proposals of the M2M network architecture which should support a wide range of M2M applications.

The challenges rise with the increased number of applications. In a recognition to the idea of a new world, in which objects are talking with other objects, applications or servers it is always important to have in mind that the idea "Internet of Things" is setting new standards regarding security and communication requirements.

M2M service provider must improve the existing and develop new security models in order to protect the data. Since M2M networks are based upon an open architecture, M2M service providers must be interoperable, which means that a M2M device from one M2M service provider can communicate with other M2M device which is in the other M2M service provider network (similar to already existing interoperability between mobile phones between two different operators).

Important need in M2M networks is notification mechanism. Various authorized parties can subscribe to the data stream of a single device, and they can be notified each time when some new data is available. Notification can be provided by using broadcasting mechanisms such as MBMS [9], OMA BAST [10] etc. For example, OMA BCAST in its structure has the Notification Function dedicated to providing information's to the terminal or a group of terminals about events regarding Broadcast Service. Moreover, mentioned parties must be provided with the security keys in order to decipher the data they have received.

In order to enable M2M data communication there are two possible types of enablers. The first group of enablers is related with routing, distribution and advertising M2M transmitted data and the second group of enablers is related to data security. Again, OMA BCAST is based on enablers and as such it may be adopted to be use in M2M networks for broadcast distribution.

When selecting M2M service provider for an application, it is necessary to have in mind the following factors, such as: price, coverage extension, reliability etc. However, it is noticeable that those parameters are independent of security and trust that are linked with a particular M2M service provider. In these cases, it is possible that M2M service provider will not have the required level of security and trust in order to handle some sensitive data. It is possible that even M2M service provider refuses to deal with confidential data in such cases.

Taking into account all of the above mentioned facts, certain mechanisms are developed which would enable end to end data encryption. In those mechanisms M2M service provider does not know the relevant decryption keys and this is opposite to hop based protection. Hop based protection model has the following path: from the source of the data towards M2M service provider No#1, then trough M2M service provider No#2 and finally to the destination of the data. With end to end data encryption M2M service provider can handle data streams that are secured by using secrets which are distributed from a third party business entity.

6. CONCLUSION

Further development of M2M security mechanisms has a huge impact on M2M technology advancement. Improved encryption algorithms, along with data overhead minimization and network infrastructure optimization can provide better conditions for variety of use cases and scenarios. By reducing power consumption and data usage, M2M devices can achieve longer integrity and stand-alone working in environments where human intervention is not desirable or even possible.

Main challenge for M2M security is cost reduction. Security mechanisms are adding up to devices and network complexity. There are some elements that can be considered for further studies in order to reduce cost. First of all, it is possible to reduce SIM cost in the provisioning process by improving scalability, efficiency and by reducing the distribution costs. As a good solution, the use of embedded SIM is proposed. It is also possible to reuse SIM cards together with the level of security provided for various M2M devices inside the capillary network. Further on, it is possible to reduce network costs by improving network elements (the use of LDAP and UDC as a database in HSS, MME; defining a different licensing model for MME where the processing power becomes the limiting factor instead of a capacity; decreasing the processing load by cutting down the number of attached/detached M2M devices).

Stable device connectivity and scalable infrastructure for M2M communication must be provided in order to achieve end to end security for all M2M use cases. Device mobility is a must for variety of M2M use cases, and majority of the principles inherited form mobile networks can be applied in M2M solutions.

The next generation security model for M2M is based on a mix of device-centric trust and a traditional enforcement. Sharing trust and enforcement tasks between a device and a network will lead to creation of a new scalable concept which can easily fit into already existing models.

ACKNOWLEDGMENT

This work has been performed in the framework the ICT project ICT-5-258512 EXALTED, which is partly funded by the European Union. The authors would like to acknowledge

the contributions of their colleagues from the EXALTED project.

REFERENCES

[1] FP7 EXALTED: “D3.2 - Study of Commonalities and Synergies between LTE-M and the Heterogeneous Network,” project report, August 2011

[2] William Stallings, “Cryptography and Network Security: Principles and Practice, 5/E,” January 2010

[3] “ISO/IEC 29192:2012 Information technology – Security techniques – Lightweight cryptography,” International Organization for Standardization, Tech.Rep., 2012

[4] FP7 EXALTED: “D2.2 - Impact of Use Cases in Business Models,” project report, August 2011

[5] Jesús Alonso-Zárate, Mischa Dohler, Thomas Watteyne, “Machine-to-Machine – An Emerging Communication Paradigm,” Wireless World Research Forum (WWRF), November 2010

[6] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C.Vikkelsoe, “PRESENT: An Ultra-Lightweight Block Cipher,” In Proceedings of Workshop on Cryptographic Hardware and Embedded Systems — CHES 2007, Lecture Notes in Computer Science, volume 4727

[7] FP7 EXALTED: “D2.3 - The EXALTED system architecture,” project report, August 2012

[8] C. Perkins, Ed., D. Johnson, J. Arkko, "RFC6275: Mobility Support in IPv6" , July 2011

[9] Frank Hartung, Uwe Horn, Jörg Huschke, Markus Kampmann, and Thorsten Lohmar, “IP Multicast/Broadcast in 3G Networks,” International Journal of Digital Multimedia Broadcasting Volume 2009 (2009), Article ID 597848, December 2009

[10] “OMA-AD-BCAST-V1_1-20100914-C: Mobile Broadcast Services Architecture,” Open Mobile Alliance, September 2010