J. Parallel Distrib. Comput. 109 (2017) 142–154

Contents lists available at ScienceDirect

J. Parallel Distrib. Comput.

journal homepage: www.elsevier.com/locate/jpdc

A survey on information security threats and solutions for Machine to Machine (M2M) communications

Gurkan Tuna [a,*], Dimitrios G. Kogias [b], V. Cagri Gungor [c], Cengiz Gezer [d], Erhan Taşkın [d], Erman Ayday [e]

[a] Department of Computer Programming, Trakya University, Edirne, Turkey
[b] Department of Electronics Engineering, Piraeus University of Applied Sciences (T.E.I. of Piraeus), Greece
[c] Department of Computer Engineering, Abdullah Gul University, Kayseri, Turkey
[d] NETAŞ Telekomunikasyon A.S., Istanbul, Turkey
[e] Department of Computer Engineering, Bilkent University, Ankara, Turkey

HIGHLIGHTS

- A detailed review of information security threats and solutions for M2M communications.
- Research challenges and open research issues in M2M communications.
- A review of oneM2M standard.

ARTICLE INFO

Article history:
Received 15 June 2016
Received in revised form 2 February 2017
Accepted 28 May 2017
Available online 28 June 2017

Keywords:
Machine to Machine (M2M) communications
Security threats
Countermeasures
OneM2M standard

ABSTRACT

Although Machine to Machine (M2M) networks allow the development of new promising applications, the restricted resources of machines and devices in the M2M networks bring several constraints including energy, bandwidth, storage, and computation. Such constraints pose several challenges in the design of M2M networks. Furthermore, some elements that contributed to the rise of M2M applications have caused several new security threats and risks, typically due to the advancements in technology, increasing computing power, declining hardware costs, and freely available software tools. Due to the restricted capabilities of M2M devices, most of the recent research efforts on M2M have focused on computing, resource management, sensing, congestion control and controlling technologies. However, there are few studies on security aspects and there is a need to introduce the threats existing in M2M systems and corresponding solutions. Accordingly, in this paper, after presenting an overview of potential M2M applications, we present a survey of security threats against M2M networks and solutions to prevent or reduce their impact. Then, we investigate security-related challenges and open research issues in M2M networks to provide an insight for future research opportunities. Moreover, we discuss the oneM2M standard, one of the prominent standard initiatives for more secure and smoother M2M networks and the Internet of Things.

1. Introduction

Machine to Machine (M2M) is a term used when talking about devices, machines, and equipment which can communicate between each other through wired or wireless links. M2M communications enable the exchange of data between typically low-power and low-cost devices, in an autonomous way without human intervention [16]. An M2M communications system consists of sensors, a wireless network, and a computer connected to the Internet [16,36,62]. M2M networks consist of a number of devices and a gateway responsible for the connection among devices and between the M2M network and other networks. The term M2M is often used interchangeably with the term IoT (the Internet of Things). In recent years, M2M has found a large number of applications across many industries, including telematics, industrial automation, remote monitoring, intelligent transportation, healthcare, security, consumer electronics, fleet management, point of sale, smart metering, smart homes, utilities, and smart grid [32,62]. Although, it has been used in many industries, the

* Corresponding author. Fax: +90 284 224 02 87.
E-mail addresses: gurkantuna@trakya.edu.tr (G. Tuna), dimikog@teipir.gr (D.G. Kogias), cagri.gungor@agu.edu.tr (V.C. Gungor), cgezer@netas.com.tr (C. Gezer), etaskin@netas.com.tr (E. Taşkın), erman@cs.bilkent.edu.tr (E. Ayday).

http://dx.doi.org/10.1016/j.jpdc.2017.05.021
0743-7315/

practical constraint for the wide deployment of M2M and IoT devices is the limited IPv4 address pool, which necessitates the use of IPv6 addresses to increase the deployment scale of such devices.

Various communications technologies, including cellular communications, such as GSM/GPRS/EDGE, WCDMA/HSPA, and CDMA, RFID, Wi-Fi, ZigBee, WiMAX, xDSL and fiber to the x (FTTx) can be found in M2M networks [30,32,62,69]. In M2M networks, much of the information is delivered in the form of sparse data. Different from traditional computer networks, data can come from sensors and other non-IT devices and is mostly only a few kilobytes. Typically, data generated by single M2M devices is not meaningful alone, but all generated data (by all deployed devices) can create a complete picture of the application. Therefore, M2M applications should not only enable M2M devices to talk to each other, but they should also collect all generated data and interpret it.

Since M2M is an emerging research area, there is a need to clearly identify the issues and approaches in addressing security of M2M networks. Along with the wide deployments of M2M networks, the types of attacks that are experienced by the service providers and businesses are likely to change. For instance, one of the new challenges is the need to consider physical attacks on devices. The main M2M information security risks rarely originate from the network. In spite of the progress made in the security of traditional distributed systems, securing such pervasive computing systems poses new challenges because of the dynamic nature of such systems [56]. M2M security requirements are often dependent on dynamically changing contexts such as available resources, location, user activity, and nearby people. However, most common threats are due to unprotected device hardware and weak application design, as most M2M applications developed by the industry lack for information and communications technology expertise. Therefore, telecommunications operators and network vendors play a key role in assisting their customers for securing their M2M applications by means of a number of services. Such services include monitoring connections using keep-alive messages, correlating location data with GPS tracking, leveraging on existing trust provisioning chain to deploy applicative security credentials, enabling applications to leverage on deployed authentication and identification infrastructures, and using over the air programming for remote management for secure deployment of applications and for firmware upgrades.

In this paper, a survey of information security threats against M2M networks is provided. This paper mainly presents common information security threats and vulnerabilities in M2M networks and investigates potential solutions against these threats and vulnerabilities. Moreover, the challenges in meeting the security requirements of both existing and emerging M2M applications are also presented. Finally, a brief introduction to the oneM2M protocol is presented. OneM2M is a global organization formed in 2012 to create an interoperable and scalable standard for communications of services and devices used in M2M and IoT. The specifications developed by oneM2M provide a framework to support services and applications such as public safety, health, home automation, smart grid, and connected car.

The rest of this paper is as follows. Section 2 reviews potential M2M applications. A survey of security requirements for M2M communications is presented in Section 3. Section 4 presents potential M2M security threats and solutions to those threats. Security related challenges of M2M are investigated in Section 5. Current research status is given in Section 6. Discussion on oneM2M and open research issues are given in Section 7. Finally the paper is concluded in Section 8.

2. Potential M2M applications

In M2M communications, remote sensors gather data and send it wirelessly to a network, where it is next routed, often through a public network such as the Internet, to a server. Then, data is analyzed and acted upon according to the software application running on the server. In the past, telemetry technology was used for the same purpose. However, different from the telemetry communications, M2M communications uses existing networks to transmit data. In addition to this, M2M communications represents various improvements over telemetry systems, such as increased sensitivity and accuracy offered by remote sensor technology, fast computers, and software. Due to better sensors, the explosive growth of public wireless networks, and increased computing capability, M2M communications has so many applications in many fields. Instead of deploying high-cost dedicated networks for communications, M2M generally uses existing wireless networks to transmit telemetry for the following reason. Different from older telemetry system which do not always rely on radio signals and sometimes use dedicated phone lines, M2M devices do not need high-power radio signals since cellular towers are typically spread over a large area to provide coverage. For M2M devices, appropriate standardized radio technology is determined based on the application requirements.

Regardless of its application areas, the core concept behind M2M is to enable real-time data communications between central management applications and remote machines/devices to enhance the value of the remote devices for their users. While there are many wired and wireless communications options for M2M applications, M2M technology has become more mobile and even smarter since the trend lies within embedded cellular M2M via 3GPP technologies such as GSM/GPRS, UMTS/HSPA(+), and LTE networks [1]. Because, as a transport solution, 3GPP cellular networks offer significant advantages to M2M providers especially in terms of deployment aspects such as global reachability and low cost embedded modems by System on Chip (SoC). Recently, 3GPP has completed a study on optimizing LTE for machine-type communications (MTC) in order to provide devices that are cost competitive with existing 2G equipment [2]. However, similar to wireless networks, 3GPP cellular networks are vulnerable against some information security threats such as false network attacks and tamper attacks [40].

Considering the available communications options, the number of innovative devices and applications which can leverage the M2M technology is endless. In recent years, M2M technology has rapidly spread throughout a wide range of application areas, as more reliable data can be generated and transmitted faster by M2M networks, and energy consumption of M2M devices is low. While the application areas of M2M technology are numerous, most common use cases of M2M technology are found in logistics, automotive, transportation, utilities, health, security, safety, payment, and consumer market [36,62].

3. Security requirements for M2M communications and how to address them

In modern M2M communications networks, as in classic WSNs, for end-to-end communications between sensors, there is a need for assurance regarding the *confidentiality, identity, integrity, authentication, access control* and *non-repudiation* of the data that are transmitted in the network. These requirements can be met either by the functionality of the communications protocol (e.g., use of encryption techniques) or by external mechanisms (e.g., firewall). The exposure of the communications to the Internet introduced new security requirements, like *availability* and *resilience against attacks* from external entities that should be addressed by applications in these environments. Further security requirements

Table 1
Major security requirements for M2M communications.

Requirement	Description
Confidentiality	It prevents unauthorized disclosure of sensory data in transmission from passive attackers to ensure that only authorized entities can read these data in an M2M communications system.
Integrity	It must be ensured so that illegal alteration of the sensory data can be detected. In an M2M communications system, meeting the integrity requirement is critical since illegal alteration may result in serious consequences, especially in mission-critical M2M application domains [43].
Authentication	It is a prerequisite for secure M2M communications since it allows the back-end server in the M2M application domain to corroborate the sensory data of the M2M nodes in the M2M domain.
Access control	It is the ability to limit and control access to the back-end server in the M2M application domain. By access control, only authorized M2M application systems are allowed to gain access to the back-end server.
Non-repudiation	It guarantees that M2M nodes cannot deny the transmission after sending data,
Availability	It ensures that whenever M2M application systems access the back-end server, the back-end server is always available.
Privacy	It is highly important in some privacy-sensitive M2M communications systems. If sensitive information is improperly used or illegally disclosed, undesirable negative effects can be faced with.
Freshness secrecy	It is important that an M2M node should not be able to read any previously transmitted messages when it joins the network and any future messages after it leaves the network [25].

include *privacy, trust, liability,* and *anonymity* that are demanded for the social acceptance of the (future) applications regarding M2M networks and communications. Finally, *authorization* and *data integrity* are also key requirements. Table 1 lists security requirements for M2M communications environment.

To address the security requirements listed in Table 1 and establish a secure M2M communications environment by defending against possible security threats, a suite of security mechanisms are needed. Generally, the security requirements in M2M communications can be achieved by cryptographic techniques. For instance, symmetric or asymmetric encryption primitives can be used to achieve confidentiality, and digital signature and message authentication code techniques can be used achieve the others. Nevertheless, most security mechanisms only efficiently defend against external attacks. If M2M nodes are compromised and launch some internal attacks, more sophisticated security mechanisms are needed [43]. In the following, proposed solutions and promising approaches that deal with the security requirements listed in Table 1 are given.

- *Identity, Authentication, Confidentiality and Integrity:* It is very important to find a way to authenticate the identity of an entity in a heterogeneous M2M network. In centralized approaches, the identification and authentication might take place by the central entities in various points (to serve scalability requirements) while in distributed approaches each node will be responsible for such actions. In [39], the first two-way, fully implemented authentication security scheme for IoT is presented. This scheme is based on existing Internet standards and RSA encryption and is designed for use on *Ipv6 over Low power Wireless Personal Area Networks (6LoWPANs)* [47]. In [63], a transmission model that manages to address the security requirements for anonymity and confidentiality in IoT is proposed, with the use of a signature and encryption scheme. Regarding confidentiality and integrity, in [50] the authors describe how existing key management systems could be applied for serving modern M2M communications, while the authors in [33] state that no current solution can guarantee confidentiality. Recent solutions try to address questions regarding the adaptability of the WSNs to the environment of M2M communications by presenting a light-weight encryption method for privacy protection in the form of an authentication protocol [41]. Finally, in [60], a user authentication and key agreement scheme is proposed, for WSNs and M2M communications that enable the secure negotiation for a session key among sensor nodes in the network. Even though several recent solutions manage to partially address the difficulties of the integration of WSNs with IoT and M2M communications, the need for creation of a solution that will be used as a standard still remains open.
- *Access Control and Data Integrity:* Access control is about gaining permission to the content or services that is allocated or provided by entities in the network. In centralized approaches various nodes/ entities might easily identify a central node, and then safely communicate with it since all access permissions will be stored there. In distributed approaches, the dynamic and heterogeneous environment that is created in modern M2M communications amplifies the difficulties that have to be dealt by each node. However, once each node can control who has access to its data, then the overall network performance will increase. To address these difficulties, in [47], the identification of two distinct subjects is presented: the data holders and the data collectors. The former have to be able to provide specific data to the latter which, in turn should be able to authenticate that the origin of the data is from a legitimate data holder. The main difficulty here lies on the fact that identification of legitimate users, in order to provide the desired access control, is a difficult computational procedure that requires many resources and power from the user node. To deal with this problem, in [44], a hierarchical access control scheme for the layer that is responsible for the collection of information is proposed. This scheme actually takes under consideration the limited resources and computational capacity of the nodes creating only a single key for each user/node. In [37], an identity based system for emergency situations is introduced that includes registration, user authentications, and policies that determine the level of emergency and authorize the access to the provided information by legitimate

users, in time of need. Finally, in [18], a security architecture that uses a prototype query processing engine for data streams is developed that addresses data integrity and confidentiality issues. In summary, it can be stated that an overall solution has not been found yet, but all the proposed solutions manage to address certain security requirements. At the same time, they all present one common drawback: the need to reach a trusting entity before moving on to request or deliver data to other network entities.

- *Privacy and Anonymity:* The increased number of applications that take advantage of the advanced sensor capabilities and the development of WSNs (e.g. applications for health monitoring, sport activities or civil protection) generate and propagate personal data and information, increasing the need to efficiently protect those sensitive transmitted data. Distributed approaches manage to perform better regarding privacy and data management issues, because of better control that each entity possesses on the data it generates and processes. In these approaches, more information is received by those with the respective credentials, since they allow creating specific access control policies and provide only requested data. As an example, a node in a distributed strategy might give information about its location to certified users, allowing more detailed information (i.e., exact location instead of just announcing vastly the geographic area where it resides) based on the user's credentials. On the other hand, on centralized approaches, the (central) data provider can select to share or not certain information streams, while the type of services that can be provided will be limited by the variety and amount of received data. Hybrid approaches, that combine central entities which use distributed strategies, may allow for a negotiation of a set of secret keys in order to increase the overall security, anonymity and privacy but the central entity may no longer be able to process the data just to store them.

Proposed solutions to increase privacy and anonymity on an M2M communications include a technique derived from Information Control Theory [31], that is proposed to tag the data, providing several privacy properties. But, the data tagging, unfortunately, is a heavy processing action that should be carefully integrated for successful M2M communications. In [23], a cluster based scheme named CASTLE (Continuously Anonymizing STreaming data via adaptive cLustEring) is presented which ensures anonymity, freshness and deals with the delay constraints on the delivery of information flaws. Another approach is presented in [67], where a division of the traditional strategies is proposed into two different categories: the *Discretionary Access* category, where the minimum privacy risks that should be met in order to prevent any data disclosure or theft are described, and the *Limited Access* category that provides the limits for any security access to prevent or avoid any malicious attacks. In [61], an enhanced Domain Name System (DNS) for smart devices is proposed in order to deal with the privacy/security risks that arise when an IoT node receives a static domain name. In [17], a decentralized protocol for privacy-preserving IoT applications is described. The proposed protocol uses a multi credential system that does not allow to the different showing of the same credential to be linked, therefore manages to avoid the discovery of the different keys. Like before, the users are proposed to be divided in data origins and data collectors. In [48], to increase privacy a mutual authentication protocol with key exchange characteristics for WSNs and RFIDs is presented that uses a random generator on the reader's tag and creates a unique hash function to increase security while providing for key refresh and key backup to reduce the risks. Finally, in [55], an assessment of the privacy requirements for data is delivered with the introduction of a layered architecture in IoT that estimates data availability and quality along with the levels of security and anonymity.

To summarize, regarding privacy and anonymity, it can be stated that the proposed solutions manage to deal partially with the peculiarities of M2M or IoT communications environment and open issues are still need to be efficiently addressed to achieve an efficient and secure integration.

- *Trust and Governance*: Trust is very difficult to define. For our study, trust will be divided in two dimensions: (i) trust in interaction between the involved entities and (ii) trust in the system by the active users. For the first definition of trust, in centralized approaches, the uncertainty stems from the interaction with the data providers and deals with the freshness of information and its reliability. Furthermore, even though central entities might hold critical information regarding the local characteristics of the network, the cooperation between such entities demands a level of trust between them to exchange the data in order to be able to update or fix any inconsistencies in values or knowledge. While on distributed approaches, it is more difficult to find a way to estimate trust between two entities or verify reputation metrics. At the same time, second hand information regarding those metrics can be easily disseminated from one entity to the other, taking advantage of the network's functionality.

The second definition is closely related to the knowledge of the network's internal state, for M2M communications around the node. In centralized approaches, all the information is not given freely but can become available by searching storing records or by sending queries. On distributed approaches, more time is needed to be able to discover and query relevant data holders. But distributed approaches manage to perform better, regarding governance rules, since each node can place the desired rules and build each own access permissions, excluding unwanted participants from the communications network. Centralized approaches do not impose such advantage since the servers might, as well, be placed on foreign ground where they operate.

These problems are addressed, up until now, by solutions as in [19,20], where trust level assessment of IoT entities is delivered by studying human guided Smart Objects, connected wirelessly with heterogeneous characteristics and showing cooperation capabilities. The social relationships that are created at these Smart Objects are based on characteristics like *friendship, ownership* and *community*, while the malicious users try to damage the IoT functionality of the communications by trust related attacks, like self-promotion and bad or good mouthing. In [19], especially, a dynamic, distributed trust management protocol is proposed: when two nodes meet and complete a transaction (of any kind), then they can rate the quality of their cooperation and, at the same time, can exchange their views regarding other nodes that have been seen by each other. The latter can be considered as a kind of recommendation. Similarly, in [46] social networking concepts are introduced in IoT, since entities in IoT can establish social relationships, thus creating Social IoT (SIOT). The challenge in SIOT is the building of a reputation-based trust mechanism that deals with certain type of malicious behavior that aims at misleading the other entities, regarding the node's trust levels. In [38,42,52,64,68], models regarding the management of trustworthiness are presented with basis on various P2P solutions.

In [45], the authors conclude that current traditional access control models are not suitable for dynamic, decentralized M2M communications scenarios. In [19,46] a fuzzy approach to Trusted Based Access Control (FTBAC) is proposed. In this approach, trust is measured by factors like experience, knowledge and recommendations. These scores are then mapped to permissions and access

requests are mapped to credentials which are used to determine whether access to certain data will be permitted or not. Primary simulation results have shown that the proposed approach is flexible, energy efficient and scalable. In general, it is believed that solutions based on cryptographic protection can achieve efficient access control by increasing the trust levels. The price that these solutions have to pay is an increase of the overhead in time and the amount of energy consumption. In [59], the authors point out that the current mechanisms for trust and reputation do not manage to offer flexible mechanisms that can adapt easily and seamlessly to the surrounding environment. In [34], a layered architecture is presented for trust management, consisting of three layers (sensor, core and application layer respectively), where each layer is controlled by a separate trust management that is based on self-organization, routing and multi-service. To summarize, the available solutions regarding trust and governance utilize many different techniques. And, even though many techniques for trust management are mature enough, a fully distributed and dynamic approach has not yet been introduced. Especially one that could address the inherent characteristics of M2M communications in an IoT environment, as stated in [66] as well.

4. Security threats in M2M networks and countermeasures against the security threats

M2M networks consist of a number of devices with limited resources and, possibly depending on the architecture, a more powerful, integrated device called gateway which is responsible for the connection among the devices and the connection between the M2M network and external networks. An M2M network is potentially formed by many M2M nodes and a M2M gateway. Each M2M node is a smart and flexible device equipped with some specific sensing technology for real-time monitoring. As soon as monitoring data are sensed, M2M nodes are expected to make decision and transmit the sensory data packets to the M2M gateway in single-hop or multi-hop patterns. After receiving the packets from the M2M nodes, the M2M gateway manages the packets and provides efficient paths for forwarding these packets to the remote back-end server via wired/wireless networks.

Thanks to M2M and the expansion of wireless networks, now remote monitoring, data acquisition and control is available to a larger audience than previously possible. Therefore, security is one of the most important challenges that need to be addressed for the smooth integration of M2M networks and the Internet of Things (IoT) in real-life scenarios. In IoT, a large number of devices interconnect forming heterogeneous networks to transfer, usually over the Internet, data and information. In M2M communications, which is a special case of an IoT implementation, such devices are low-power sensors that generate personal and sensitive data, whose integrity and privacy is crucial and has to be firmly guarded [70].

The integration of modern, low-power, cheap but extremely powerful sensors with Wireless Sensor Networks' (WSN) applications and the use of the Internet for the dissemination of the generated information has introduced the system to new, advanced security threats. The reason is that, besides the threats that are inherent to low power WSN environment characteristics and constraints (e.g., depletion of energy, small memory capacity, limited processing power), in M2M networks, there are also external or Internet originated hazards. The integration of the Internet has exposed the network's communications (both for the devices and applications) to newly introduced security threats, depending on the applied mechanism used for the integration between the technologies (i.e., the use of centralized IoT architectures or distributed ones) [33,51,54]. Those threats are mainly motivated by the wireless nature of the communications and the physical exposure of the communicating entity (sensor). In this section, we will first classify the attackers and describe the common security threats that can be detected in M2M communications. Then, we will focus on the specific security and privacy threats that can be found in M2M systems and describe how the communications system architecture can be affected by these attacks. Finally, the security requirements for an efficient and robust M2M communications system are presented followed by descriptions on how to address them.

4.1. Classification of attacks and common security threats

Before going into the details of the specific threats in M2M communications, we will first classify the attackers as *internal* or *external* [33]. *Internal* attackers are those who manage to take control of a network node and then, participate on the communications that take place legitimately. Such attackers can easily send/receive messages to/from the other networks' nodes because access to any encryption keys that are demanded for the network's communications is open to the attacker as the node's new owner. On the other hand, *external* attackers mainly "listen" to the (wireless) communications, try to understand the network's functionality, and discover any possible vulnerability. External attackers are easier to defend, since they do not hold any crucial information (e.g., cryptographic keys for the communications) that may damage the M2M communications.

In addition to the aforementioned classification of the attackers, a similar classification of the types of potential attacks can be also done as *passive* and *active* attacks [33]. In a *passive* attack the attacker has no intention of generating any interaction with a network entity. Instead, the attacker only tries to understand the network's functionality by observing the communications and search for a way to break into the system silently, without been noticed. In an *active* attack, on the other hand, the attacker uses all of its resources to break into the system and disrupt its communications and functionality without been worried about getting noticed.

Considering the above types of attacks and the behaviors of the attackers, Table 2 lists and describes threats relevant to the security domains.

The way each of the aforementioned threats may damage the network's communications and functionality does not only depend on the nature of the attack or the attacker but, as it has been mentioned earlier, might also depend on the approach for the integration of the M2M communications [51,54].

4.2. Security vulnerabilities & threats specific to M2M networks and countermeasures

Since most M2M applications generate and transmit sensitive data between communicating entities/nodes, they need to be able to provide required security services such as mutual authentication between the communicating entities/nodes, access control, high availability, confidentiality, and protection against data manipulation. In M2M applications, security related operations must be provided with a number of approaches and mechanisms such as secure storage of sensitive data, sensitive functions, such as cryptographic algorithms, key derivation functions and hash functions, performing operations on sensitive data, and secure connection to allow the secure transmission of sensitive data with an appropriate level of confidence in order to implement security features and countermeasures against potential threats [3,58]. Regardless of where the provision of security services is realized, the ability to establish security associations (SAs) between corresponding M2M nodes is required [3].

Table 2
Summary of common threats related to security domains.

Attack	Classification	Definition / Description
Eavesdropping	Passive, external	A passive and external attack in which the attacker targets various diverse communications channels (e.g., wireless networks, Internet) and listens to the disseminating data, even recording or cloning it, in an effort to learn things about the network and possibly manages to find a way inside it (becoming therefore an internal attacker when access is achieved). The probability of this network attack has increased due to the Internet-based communications in a M2M communications network.
Man in the Middle	Active, external	An active and external attack, where the attacker first uses eavesdropping to learn about the communications keys used by two peers and, then, impersonates one part to the other by manipulating messages and their flow, controlling fully the conducted communications. Man in the Middle (MITM) attack is a common network attack that is influenced by the Internet-based communications.
Node Capture	Active, external	Instead of intercepting the communications or trying to find a hole on the network security, an active external attacker might try to (manually) take control of a device and then extract any information from it, instead of destroying it.
Spoofing	Active, internal/external	An active internal or external attack, in which the attacker impersonates a legitimate user or network node in order to gain access and launch other attacks against critical nodes in the network such as spreading malware by bypassing access controls, and hence damaging the network's functionality.
Denial of Service (DoS)	Active, external/internal	DoS attacks target the network operation and aim to decrease network's functionality or even shut it down for a small time period. When a DoS attack takes place, a malicious user aims to exhaust the network's resources by continuously keeping the network traffic high and, eventually, preventing legitimate users from using the network. This is a very common and dangerous attack in the M2M environment, where exhaustion of the sensors' energy is crucial for the network's survival. The physical compromise and destruction of a node can also be considered as a DoS attack, since the results remains the same: the destruction of the network's operation. The following attacks can be categorized under DoS attacks. • *Distributed Denial of Service (DDoS):* In a DDoS attack, continuous flooding for requests from multiple malicious nodes damages the network's operation and disrupts any communications. Such flooding requests might be targeting different layers of the protocol stack, creating a different kind of attack that needs to be carefully addressed. For example, the DDoS attack that disrupts the wireless communications by jamming the signal via sending bogus data and requests is considered as an attack at the physical layer. At the MAC (Medium Access Control) layer, a DDoS attack involves the malicious nodes sending packets at the same time as a legitimate node, resulting in packet collisions and decreased network performance [33]. • *Fuzzing:* In this attack, the attacker's goal is to cause a device or application to fail by using randomly generated or manipulated messages. Attackers can insert specific exploits into messages including buffer overflows, special format characters or invalid input data to find implementation errors on a device application or service.
Routing Protocol Attacks	Active, external	They affect the routing decisions on the communications path and can target all the modern routing protocols. Examples of such attacks include: • *Sybil attacks*: In Sybil attacks, a node manages to create many fake identities and affect the communications performance. • *Wormhole attacks*: In wormhole attacks, the attacker records packets transmitted somewhere on the network and then tunnels them in a different area where they are retransmitted.
Injection	Active, internal/external	This attack relies on injecting malicious data into an application through its communications interfaces in order to execute, interpret, or parse in an unexpected manner. When untrusted data is sent to an interpreter as part of a SQL, LDAP, XPath or OS command/query, this data can cause executing unintended commands or gaining access to unauthorized data.

The results of an attack on the communications might highly depend on the architecture of the system since the vulnerabilities will highly vary. To this end, the results of an attack on a *centralized* architecture, that uses application platforms located somewhere in the *cloud* to gather data from various scattered entities, will be different from when a similar attack is launched against a *distributed* architecture, where all the entities have the ability to retrieve, provide, and process information and data. Variations on the deployment strategies, the flaw of information, and the availability of services are the main reasons for this difference on the expected results. On centralized approaches, the attacker will aim for the target that cause the largest damage to the network

and any central entity falls into this category. Such entities will be heavily guarded but, in the case where the attack succeeds, the network will be seriously damaged. On distributed approaches, the information is generated and processed in many different entities, and hence the attacker will have to increase its efforts in order to cause the same damage as the one caused by breaching into a central entity, increasing the difficulty for the success of the attack. On the other hand, on distributed approaches the entities will not be as heavily guarded as a central entity would, making it easier to fall under a malicious attack. Furthermore, if the attacker selectively gains control of certain entities that possess a specific piece of information, then the result can be very devastating for the network's performance. Another aspect of an attack on a centralized approach is the flow of information. On such approaches, information flows from every 'thing' to the central entity, following a relatively hierarchical route. On distributed approaches, the information flow takes place inconsistently, when it is needed, resembling the functionality of a peer-to-peer (P2P) system. Therefore, the capture of the flow will not reveal any comprehensive data regarding the structure or operation of the network but, at the same time, the attacker will have processed information and not raw data. Finally, regarding the connectivity of the network, approaches that use super nodes or central entities would require that the addresses of these entities are well-known in the network and that they can accept external connections making them susceptible to any malicious attacks. Those strategies would need further security solutions and protection mechanisms to be able to control those incoming connections, such as additional middleware layers and firewalls. Regarding the suitability of an approach to defend against a security threat in M2M communications, no single solution stands out. Centralized approaches provide better defense at the central entity but, if successful, the attack can deeply wound the network's functionality. On the other hand, a successful attack on a distributed approach has smaller effect, but entities are scattered at various locations increasing the number of probable attacks that might have to deal with (e.g., node capture or DoS attack).

In general, an attacker will aim to take under control information that relates to authentication and encryption of the data that is transmitted in M2M communications either to read and/or modify this information and to jam the communications and/or to allow the impersonation of a legal network party in the M2M communications network. Common techniques that are used to achieve these results are hacking of a legal user or eavesdropping of the communications. Table 3 lists the potential threats and proposes countermeasures in an effort to address them.

In summary, although M2M networks share the same classic threats existing in other technologies or networks, in M2M networks, most of the threats are a combination of security risks originated by the inherent characteristics of low power devices and applications, augmented by the risks that are originated from their integration with external communications and the Internet. The heterogeneity of the networks that are combined to create a M2M network and the huge number of interconnected devices amplifies the dangers and the needs to propose novel secure mechanisms for the communications in an effort to increase the resiliency and efficiency in the system's communications performance.

5. Research challenges

Autonomous operation is highly desirable in almost all environments. Then, the more the machines can operate autonomously, the more work they can do without human intervention. On the other hand, possibly in the future, humans will still need to be in the chain to oversee the different operational processes, but they will act as direct supervisors. Therefore, the humans will only be responsible for taking a step if a machine reports a problem. So the humans will be "the weakest link in the chain". Therefore, novel management frameworks are needed to reduce the complexity of managing a huge number of M2M devices, especially in the industry [22].

Telemetry systems installed in the past were not designed information security in mind. Because the designers did not expect that those systems will be connected to a public access network like the Internet. Similarly, traditional M2M applications have been typically focused and used specific edge devices, a single network and custom platform. Therefore, securing them to the acceptable level has been relatively easy for information security professionals. However, the transition to M2M was quick and the designers again generally failed to address information-security related concerns. In addition, although some M2M devices do not support IP protocol for communications, most M2M devices inherently support IP and run embedded and highly vulnerable operating systems. Therefore, in addition to guaranteeing the integrity of data received from the M2M devices, firmware upgrades must be authenticated to ensure no malware is introduced to the embedded operating systems [33].

M2M designers always should keep in mind that the key in information security is to prevent threats and vulnerabilities not to cure them. It is expected that number of attacks on M2M systems will increase. Hence, M2M device suppliers should offer their customers simple and cost effective measures to enable them have secure M2M designs and accordingly M2M application owners should use proper consulting to secure their M2M networks and devices [33,54]. In fact, every part of the M2M chain must be protected, including protection of the M2M networks and M2M devices themselves, the securing of physical and logical access credentials, protection of the communications among the M2M devices, and securing of the M2M applications themselves and of the portals used for access.

Although standards bodies all around the world develop new information security standards, most of the standards generally are either too strong, and hence hard to adopt, or too weak, and hence incomplete. Whether the standards are strong or weak, the key point is implementation. In addition, it is well-known that there has never been a security standard which has obviated all information security concerns. Even if there such a theory exists, its efficiency will still be questionable since what works in theory is not always practical to implement. Therefore, the designers should see the whole picture in order to successfully satisfy the risk requirements of their potential customers [4].

Most information security architects use data encryption to protect sensitive digital information and comply with legislative mandates and regulatory standards related to data privacy protection. In addition, in terms of implementation, there may be country-specific regulatory guidelines to be addressed. For instance, in the US, the National Institute for Science and Technology (NIST) has been creating rules by which M2M must play [5]. Although the use of data encryption is an effective means of enforcing security policies governing the confidentiality of sensitive data, encrypting information is a processor-intensive task and thus M2M devices may need to be selective as to what they encrypt as they have to minimize power usage. Battery lifetime is one of the main challenges and if an M2M device deals with encryption activity all the time, soon it will not have any power to do anything.

Most of commercial M2M platforms are scalable and comprehensive in features, but they come with high licensing fee and high total cost of ownership. Therefore, commercial M2M platforms involve significant risks for enterprises and telecommunications operators who wish to invest in M2M and are unsuitable for innovation and early stage exploratory activities in which novel M2M

Table 3
Security threats in M2M networks and countermeasures/solutions [3,43,58].

Description of threats	Possible consequences	Countermeasures/solutions
Hacking of Long-Term Service-Layer (LTSL) keys stored in M2M devices/gateways.	M2M devices/gateways may be impersonated using the LTSL keys.	• To address this treat, one of the solutions is to store M2M LTSL keys in a Hardware Security Module (HSM), typically certified for being tamper-resistance, which resides within the M2M device/gateway, and this way makes it impossible for attackers to discover the values of LTSL keys. • Session keys with a predetermined limited lifetime set by an M2M security policy can be used.
Hacking and modification of LTSL keys stored in M2M devices/gateways.	A DoS attack may be realized to prevent proper operation of the M2M solution.	• To address this treat, one of the solutions is to store M2M LTSL keys in a HSM, typically certified for being tamper-resistance, which resides within the M2M device/gateway, and this way makes it impossible for attackers to discover the values of LTSL keys. • Allowing the modification of stored sensitive data and LTSL keys is done after a strong cryptographic authentication and authorization.
Hacking and replacement of LTSL keys stored in M2M devices/gateways.	The M2M solution may be operated illegitimately and users cannot be made accountable for realized activities.	• To address this treat, one of the solutions is to store M2M LTSL keys in a HSM, typically certified for being tamper-resistance, which resides within the M2M device/gateway, and this way makes it impossible for attackers to discover the values of LTSL keys. • Allowing the access and modification of stored sensitive data and LTSL keys is done after a strong cryptographic authentication and authorization.
Hacking of LTSL keys stored in M2M infrastructure equipment, such as security server or equipment holding network Common Service Entity (CSE), are discovered by means of various techniques including the reading the contents of memory locations, monitoring of internal processes and illegal/unauthorized use of management interfaces used for illegal/unauthorized purposes.	The LTSL keys may be used to impersonate M2M infrastructure equipment.	• M2M LTSL keys can be stored in a tamper-resistance certified HSM, which resides within the M2M infrastructure equipment to make it impossible for attackers to discover the value of LTSL keys. To make the M2M system even more secure, HSM/server-HSM are configured not to reveal the values of the stored keys to the M2M management system and M2M system operators. • Session keys with a predetermined limited lifetime set by an M2M security policy can be used.
Deletion of LTSL keys stored in the M2M infrastructure equipment by means of management commands.	Proper operation of the M2M solution may be prevented and a DoS attack may be realized.	• M2M LTSL keys can be stored in a tamper-resistance certified HSM, which resides within the M2M infrastructure equipment to make it impossible for the attacker to discover the value of LTSL keys. • Allowing the access and modification of stored sensitive data and LTSL keys is done after a strong cryptographic authentication and authorization.
Sniffing of sensitive data while used during the execution of sensitive functions in M2M devices/gateways.	Copied sensitive data may be used to compromise security of the M2M solution.	• Executing sensitive functions which may be executed within an HSM prevents LTSL keys from being exposed outside the HSM.
Eavesdropping of M2M Service Layer (SL) messaging between entities.	Privacy of the users may be lost and the M2M Service Provider (SP) can be blamed.	• Use of secure communications link and SA between communicating entities/nodes by means of modern cryptographic algorithms.
Modifications of M2M SL messaging between entities.	Loss of revenue may happen as the attacker may defraud the M2M SP and a large-scale attack can be realized.	• An SA is established between the communicating M2M entities to provide mutual authentication, confidentiality, and integrity. The SA relies on protocols proven to resist MITM attacks. • Session keys with a predetermined limited lifetime set by an M2M security policy can be used.
M2M SL messaging between entities is replayed.	Loss of revenue may happen as the attacker may defraud the M2M SP and a large-scale attack can be realized.	• To detect whether a part or all of a message is an unauthorized repeat of a part or all of earlier message functionality can be provided by the protocol suite. • Session keys with a predetermined limited lifetime set by an M2M security policy can be used. • Use of secure communications link and SA between communicating entities/nodes by means of modern cryptographic algorithms.
Hacking and installation of unauthorized or corrupted M2M SL software in M2M devices/gateways by an attacker.	This type of attacks may be used to commit fraud, cause a breach of privacy, reveal sensitive data, and prevent operation of the M2M devices/gateways.	• Verification of the integrity of executable files and functions in M2M devices/gateways should be done. This way if a file or function fails the integrity verification test, its use can be prevented by means of policy-based actions.
Possible interdependence of underlying M2M systems and resources	Although M2M gateways and M2M endpoints are typically dedicated to specific services, M2M systems frequently share resources with a number of other unrelated systems and applications. Hence, such attacks may cause threats for many interdependent services.	• Inventory of the assets of an M2M solution should be prepared and shared M2M assets should be identified. In addition, sensitivity assessment of shared M2M assets can be carried out for management review. Based on the asset inventory and sensitivity assessment, a risk assessment should be carried out to make recommendations for the management to treat, transfer or accept risks related to interdependency.
Lack of context awareness solutions for M2M and this may exhaust available resources and trigger M2M service impacts or outages.	Although the level of security is sufficient on the context of the M2M operation, its static management may result in inefficient usage of available system resources.	• Inventory of the different operational contexts of an M2M solution should be prepared and assessment for sensitivity to confidentiality, integrity, and availability requirements should be carried out. Based on the operational context inventory and sensitivity assessment, a risk assessment should be carried out to determine if risks differ across the operational contexts.

(*continued on next page*)

Table 3 (*continued*)

Eavesdropping of sensitive information at the Transport layer.	This type of attacks may cause numerous threats to the M2M solution.	• This type of attacks typically depends on exploiting the lack of security protection during data transmission or vulnerabilities in the protocol protecting the communications channel. • Use of secure communications link and SA between communicating entities/nodes by means of modern cryptographic algorithms.
Unauthorized possession of viable keys and credentials is gained and the keys and credentials are removed from the legitimate M2M device by an attacker.	The removed keys and credentials are used in unauthorized M2M devices so that the legitimate M2M user is charged. In addition, a service request of the legitimate user may be denied while the unauthorized device is online.	• M2M LTSL keys can be stored in a tamper-resistance certified HSM bounded to the M2M device/gateway to make it impossible for the attacker to discover the value of LTSL keys.
Buffer overflows are present when the use of non-type safe Application Programming Interface (API)'s are exposed and they are special cases of the violation of memory safety.	Buffer overflows are indicated by the return code which jumps to a random location, and hence incorrect code is executed and this may change local data.	• Implementing secure coding practices which enforce strict input data validation in M2M system, services, and applications.
Untrusted data sent to a query interpreter can cause injection flaws which are often found in program arguments, OS commands, SQL queries, LDAP queries, and XPath queries.	The attacker sends inappropriate queries to the application-level server and by exploiting security vulnerabilities of the query interpreter gains unauthorized access to the server.	• Untrusted data should be kept separate from queries and commands. • Parameterized APIs should be preferred and specific escape syntax should be used for the interpreter. • Examination of vulnerable code makes it easy to discover and resolve injection flaws.
Custom authentication and session schemes often have flaws which can be used by attackers and malicious users.	By exploiting flaws or leaks in the authentication or session management functions, the attacker impersonates legitimate M2M users.	• Strong session management and security controls should be in place. • Implementing secure coding practices which enforce strict input data validation in M2M system, services, and applications.
Due to security misconfiguration, attackers gain unauthorized access to or knowledge of the M2M system by accessing default user accounts, unpatched flaws, unprotected files and directories, and unused pages.	The attackers and malicious M2M users may compromise the M2M System.	• Good separation and high security between M2M application components should be provided.
Not encrypting sensitive data is one of the most important flaws. Even encryption is employed; other flaws such as weak algorithms, unsafe key generation and storage, weak hashes to protect passwords, and not rotating keys can be used by attackers and malicious users.	Since their limited access, attackers have difficulty in detecting the flaws; hence they generally exploit other flaws and tools, such as finding keys, getting clear text copies of data, or accessing data via channels automatically decrypting, to gain the needed access.	• Appropriate strong algorithms and strong keys should be used, and key management protocols should be in place.
Invalid input data by means of injecting specific exploits, SQL injection attacks, buffer overflows, and cross-site scripting can be used to gain control over vulnerable machines.	The attacker may access unintended functionality, execute remote code, steal data, escalate privileges, bypass authentication, and realize a DoS attack.	• Input data validation should be used to ensure that the content provided to an M2M application does not allow accessing to unintended functionalities or privilege escalation. • Least-privileges should be implemented to minimize M2M service privileges and reduce associated risks.
Code is injected into Web pages generated by a vulnerable Web application.	This attack is called cross-site scripting and takes advantage of Web servers which return dynamically generated pages or allow their users to post viewable content to run HTML, ActiveX, JavaScript and VBScript on remote machines browsing the sites within the context of client–server sessions.	• Positive input validation which decodes any input to validate its length, characters and format before accepting it should be in place to protect against cross scripting attacks.
Outdated software that could not be upgraded.	The system is vulnerable to external attacks that can take advantage of the outdated code to provide access to a node and, then, the whole system.	• The sensors are deployed in hazardous location where their replacement or upgrade is not possible. • Replace these sensors with updated solutions.

ideas and applications need to be quickly prototyped, field tested for technical and business feasibility.

Although the philosophy behind M2M is not something completely new for those familiar with embedded control and monitoring, when potential M2M use cases have been taken into consideration, M2M offers significant market potential [62]. On the other hand, different from the requirements of existing M2M solutions, it is expected that M2M plug and play (PNP) capability will be essential for the success and overall acceptance of M2M technologies for future M2M solutions. In addition, the designers may need to design their products so as to enable them to support a mixture of new and legacy devices and services [62]. In this respect, M2M gateways and aggregation points are expected to play key roles by providing interworking with different wireless technologies and bringing the sensors with short-range radios online.

6. Current research status

After discussing the research challenges in M2M communications networks, a discussion about the current research status will take place focusing on how the solutions that are under consideration and examination, try to deal with the security requirements in M2M communications.

As described above, the heterogeneity of the devices that communicate in an IoT environment plays a very important role in the M2M communications, mainly due to the variation in the available computation capabilities of the included sensors along with limitations in the lifetime due to energy depletion. Lately, in order to address those problems, several solutions that propose energy harvesting have been examined [53] taking advantage of renewable energy resources (e.g., sun, wind) in an effort to extend the lifetime of a sensor. When these solutions are combined with

efforts in introducing new lightweight protocols for symmetric and asymmetric encryption [28,65], an increased security performance of the system can be achieved. Identification, authorization and trust are, also, consider as important security requirements in M2M communications, as stated in Section 3, and current research status in this area aims to provide the required conditions for two different devices to build a trust relationship and enhance all the existing identification and authorization solutions. To this end, the design of a secure identifier is examined in [21] where the use of IEEE 802.1AR [35] or other cryptographically generated identifiers [6,49,57] is proposed and examined. At the same time, the use of a secure boot for local trust validation will be of great importance on establishing a trusted environment from where various trust validation processes can begin. For example, autonomous validation with the use of smart cards that possess authentication secrets is examined but an important disadvantage is the need to create costly replacements for the existing solutions. On the other hand, the use of remote validation inherits many problems from M2M environments showing scalability and complexity limitations due to the heterogeneity of M2M communications, while semiautonomous validation [24] is currently under study to test whether it can address the limitations of the others. Semiautonomous validation combines local and remote validation techniques in an effort to establish communications in situations of danger or necessity. The use of distributed mechanisms for semiautonomous validation is under study to test whether they can increase the system's performance.

Anonymity and liability are two other topics that will, not only, highly influence the security of a M2M communications system, but will also influence the societal acceptance of such a system. Very frequently, in modern M2M or IoT networks the data that are transmitted through the mobile phones or the sensors are personal and sensitive to be overseen by others. Therefore, techniques that propose data transformation or randomization are under study, in an effort to anonymize the content for a possible intruder. Especially, models like k-anonymity [57] are examined as to how efficient they can be proved for anonymizing the data in M2M communications. Liability affects security when third-parties demand access to data that have been gathered by sensors to analyze and process. Techniques that ensure that an explicit statement about the use of these data is issued along with assurance that they will not be disseminated to others need to be examined and tested. Finally, the lack of standards has been already pointed out as a possible security hole for M2M communications. To this end, Internet Engineering Task Force (IETF) organized a group to work on 6LoWPAN [47] and emphasize on proposing new standards for communications in low-energy area networks, where most M2M communications do belong. In addition, different working groups have been formed, like Routing Over Low power and Lossy networks (ROLL) [7] and Constrained RESTful Environments (CoRE) [15] which are such examples in an effort to provide the needed standards that will enhance the communications between two devices that will take place autonomously and efficiently. Finally, in [21] a novel architecture is described that can highly increase the efficiency of the M2M communications, while allowing a better control of their security by providing M2M service bootstrap and key hierarchy for authentication and authorization, along with mutual agreement for the key of the communications.

7. Open research issues and discussion on oneM2M

While, in recent years, considerable research efforts have been directed to M2M communications, there are many open issues that need to be addressed. In this section we focus on the open research issues on security threats in M2M networks and discuss oneM2M standards initiative.

7.1. Open research issues

In future M2M applications, wireless communications will be fundamental as sensing and actuating devices are expected to be able to autonomously communicate without any human intervention. Because M2M devices with wireless communications capabilities allow the users of M2M applications to transparently interact with their physical surroundings. However, interoperability issues between M2M devices following different standards from different vendors create significant challenges for the developers of M2M applications. Therefore, novel approaches are necessary to define how M2M devices and applications with heterogeneous characteristics communicate autonomously at the various protocol layers and how information security can be enabled for wireless communications. Besides them, a flexible and scalable M2M middleware can be used to integrate a wide variety of M2M devices following diverse protocols and standards.

It is expected that the model for M2M in the future will eliminate the use of a central hub which accepts wired and/or wired signals from connected M2M devices, and instead will have devices which communicate with each other and work out problems on their own. However, such decentralization will lead to situations where highly resource-constrained M2M nodes will have to connect and send data to powerful remote servers in addition to playing an active role in providing information security. In this respect, due to the technological gap between these classes of devices, collaborative management approaches are essential.

Different from traditional telemetry systems, due to the tremendous increase in data volume from a large number of M2M devices, network traffic and load on the M2M infrastructure has increased severely. Accordingly, storage space and throughput on the M2M infrastructure and network have increased. This makes it necessary to develop strategies for scalable M2M infrastructures and networks. On the other hand, the use of intelligent gateway devices can help in addressing the issues of M2M network traffic and data volumes up to a level.

In the future, it is expected that M2M devices will play a key role in security-critical applications. However, most M2M devices are seriously constrained in terms of energy, memory, and computational capability. Hence, these limitations must be considered for the security of M2M wireless communications and existing security mechanisms may not be appropriate for M2M wireless communications. In fact, the heterogeneity and the particular characteristics of M2M devices are currently motivating the design of a set of communications protocols at the various communications layers.

7.2. oneM2M

OneM2M is a standards initiative to address the need for a common M2M service layer (SL) which can be embedded within hardware and software, and relied upon to connect a large number of devices in the field with M2M application servers by developing technical specifications [8,9]. The key objective of oneM2M is to involve organizations from M2M-related business domains and then prepare, approve and maintain the necessary set of technical specifications. OneM2M is developed to define a number of requirements and specifications including the followings [29,58]:

1. The requirements and use cases for a common set of SL capabilities;
2. SL aspects with high-level and detailed service architecture;
3. SL and communications functions;
4. Identification and naming of applications and devices;
5. Open interfaces and protocols;
6. Security and privacy aspects;

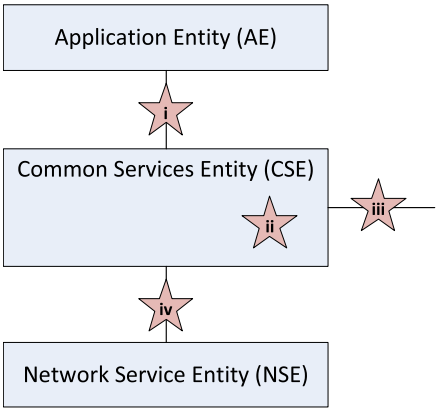


Fig. 1. Overview of the oneM2M security context [3].

7. Discovery and reachability of applications;
8. Interoperability standards;
9. Information models and data management;
10. Collection of data for billing and statistical purposes.

It is expected that framework developments and their adaption processes should be in accordance with the ETSI M2M and oneM2M architecture recommendations. In [27] the integration of a user centric IoT application with the standardized referenced architectures is shown. Due to the limitations and application related constraints, it may be necessary to efficiently manage both smart and legacy devices, an important feature for IoT ecosystems. In this respect, utilization of CoRE Link [10] can settle the heterogeneity of the managed devices and promote interoperability [26].

Basically, from information security point of view, oneM2M is a good step to face the challenges of M2M security and privacy and will be the key to the sustainable development of both M2M and IoT applications. Because the security architecture of oneM2M is based on the following components and features [11]:

- Identification and Authentication;
- Authorization;
- Identity Management;
- Security Association;
- Sensitive Data Handling;
- Security Administration.

In oneM2M security context, three entities are described [3] (see Fig. 1). The first, Network Service Entity (NSE) can be consist of several different kinds of communications infrastructure such as GSM/GPRS/EDGE, WCDMA/HSPA and CDMA, RFID, Wi-Fi, ZigBee, 6LowPAN, WiMAX, xDSL and FTTx. On the top of NSE, Common Service Functions (CSFs) reside in the entity called Common Services Entity (CSE). CSFs handle the fundamental roles such as communications, data, and device management, security, service charging, subscriptions and notifications, etc. In oneM2M specifications, CSEs are located in three types of nodes (i.e. Middle Node, Application Service Node, and Infrastructure Node) each having one and only CSE [14]. CSEs collaborate in a distributed fashion for the system-wide operation. These services are used by the Application Entities (AEs) [10].

Related with these entities four security domains can be identified; (i) Application Domain Security is responsible for the secure exchange of messages between applications; (ii) Intra Common Services Domain Security is the set of security measures for the secure communications between CSFs located in CSE; (iii) Inter Common Services Domain Security is the set of features that enable secure exchange of messages between CSEs in different nodes; and finally, (iv) Underlying Network Security Domain concerns securely exchange of messages between underlying network and common services.

Regarding (iv), before any oneM2M CSFs can take place, connectivity has to be established in the underlying network, which may involve independent provisioning and service registration procedures. For the security concerns at (iii) service layer security provisioning and association establishment procedures results in a TLS or DTLS session which protects messages being exchanged between adjacent AEs and CSEs [12]. Furthermore, AEs that need special privacy requirements against untrusted intermediate nodes may form a secure link through provisioning and association in order to encrypt the application related content. The internal functionality of CSE can also cause security gaps as a part of intra common services domain security (ii) for instance, possession of a set of viable keys and credentials can allow an unauthorized M2M device to cause denial of service attacks, buffer overflows, man-in-the-middle attacks or consume service rights of a legitimate M2M User.

Security services of oneM2M is organized into six different functions namely; identification and authentication, authorization, identity management, security association, sensitive data handling, security administration. Identification step can be described as the process of checking if the identity required to authenticate is valid or not. After that, authentication process can take place which validates if the identity has a trustworthy credential. In the specifications, provisioned symmetric key or certificated-based methods can be used as the authentication procedure. Furthermore it is allowed to use a centralized key distribution server which can be hosted by a 3rd party or by M2M Service Provider. Devices in the field domain can access this key distribution server using a symmetric key (M2M Authentication Function Security Association Establishment Framework). Authorization regulates the accesses to the services and data. Access control can be done by using a control list or role/attribute based methods. For the role based access control, a token based framework called OAuth has been mentioned in the specifications as an example [13]. Role or attribute based access is more scalable than user-based control lists and can greatly reduce the cost and administrative overhead. For the purpose of anonymity, identity management functionality of security services in oneM2M, provides pseudonyms which serve as temporary identifiers that cannot be linked to the true identity [14]. Security association can only be performed after successful identification and mutual authentication of the corresponding M2M entities. Association provides security services to the communicating entities, such as confidentiality and/or integrity of information exchange though the use of derived keys as a result of this procedure. In the security architecture of oneM2M, isolated secure environments can be created. Inside these secure environments sensitive functions and data can be stored. Secure environment abstraction layer provides physical or logical connectivity to the secure environments in order to store/retrieve data such as credentials, subscriptions, personal information or functions including security algorithms. In such a way different applications/functions can concurrently operate inside a node in a securely isolated manner. Finally security administration can be described as the set of functions to manage the security functions, resources, attributes and the resources provided by the secure environment.

8. Conclusion

Although M2M offers many benefits to many types of industrial or non-industrial applications, the devices' limited resources bring several constraints and hence create design-related challenges. Moreover, although the underlying principle of M2M is not new and a similar technology has been used for a long time for supervisory control and data acquisition purposes, neither the technology itself nor most of M2M devices were designed with security in mind as the designers did not expect that the M2M devices would be connected to a public access network such as Internet. However, different from the designer's original assumption, most M2M devices are not now behind a secure network.

In this paper, we first present typical network security threats in M2M networks and potential solutions to reduce their effects or prevent them. Then, we investigate the challenges and open research issues in M2M security. As given in the paper, the identification and application of appropriate security measures must be taken into consideration at the beginning of design and development phases. If M2M designers consider an overall integrated security approach, they can ensure end-to-end security in M2M implementations. Importantly, in addition to playing a key role in the sustainable development of M2M applications, oneM2M handles security. As confidence in the security and privacy of data will be a key factor in the successful take-up of M2M and IoT services, oneM2M specifications should be integrated into M2M development lifecycles.

Acknowledgment

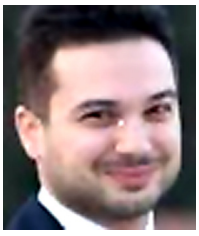
This work was supported by the Turkish Scientific and Technical Research Council (TUBITAK) under Grant no. 3140911.

References

[1] 3GPP TR 33.868, Security aspects of Machine-Type communications, July 2011.
[2] http://www.3gpp.org/news-events/3gpp-news/1714-lc_mtc.
[3] OneM2MPartners, oneM2M-TR-0008-Security-V1.0.0 , 2014-April-10.
[4] https://docbox.etsi.org/workshop/2013/201301_securityworkshop/04_m2mandsmartsecurity/gemalto_ennesser.pdf.
[5] http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm.
[6] Trusted Computing Group, www.trustedcomputinggroup.org, visited on March 30, 2014.
[7] Routing Over Low power and Lossy networks, http://datatracker.ietf.org/wg/roll/charter, visited on November, 2016.
[8] http://www.onem2m.org/news-events/news/53-the-rise-of-the-machines-world-s-first-global-standards-for-m2m-deployment.
[9] ETSI, Functional Architecture, TS 118 101.
[10] https://tools.ietforglhtmllrfc6690.
[11] http://onem2m.org/images/files/deliverables/TS-0003-Security_Solutions-V-2014-08.pdf.
[12] OneM2MPartners, Security Solutions, TS-0003-V101, 2015-January-30.
[13] Online: http://oauth.net/, 16-October-2015.
[14] OneM2MPartners, OneM2M Technical Specifications, 2015-January-30.
[15] Constrained RESTful Environments, https://datatracker.ietf.org/wg/core/charter/, Visited on November, 2016.
[16] J.N. Al-Karaki, K.-C. Chen, G. Morabito, J. de Olieveira, From M2M communications to the Internet of Things: Opportunities and challenges, Ad Hoc Netw. 18 (2014) 1–2.
[17] A. Alcaide, E. Palomar, J. Montero-Castillo, A. Ribagorda, Anonymous authentication for privacy-preserving IoT target driven applications, Comput. Secur. 37 (2013) 111–123.
[18] M. Ali, M. ElTabakh, C. Nita-Rotaru, FT-RC4: A Robust Security Mechanism for Data Stream Systems, Tech. Rep. TR-05-024, Purdue University (November 2005).
[19] F. Bao, I. Chen, Dynamic trust management for internet of things applications, in: Proceedings of the 2012 International Workshop on Self-Aware Internet of Things, Self-IoT '12, USA, San Jose, 2012, pp. 1–6.
[20] F. Bao, I. Chen, Trust management for the internet of things and its application to service composition, in: 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WoWMoM 2012, San Francisco, CA, United States, 2012, pp. 1–6.
[21] I. Bojic, J. Granjal, E. Monteiro, D. Katusic, P. Skocir, M. Kusek, G. Jezic, Communication and security in machine-to-machine systems, in: Wireless Networking for Moving Objects, Protocols, Architectures, Tools, Services and Applications, Springer, 2014, pp. 255–281. http://dx.doi.org/10.1007/978-3-319-10834-6_14.
[22] David Boswarthick, Omar Elloumi, Olivier Hersent (Eds.), M2M Communications: A Systems Approach, Wiley, West Sussex, UK, 2012.
[23] J. Cao, B. Carminati, E. Ferrari, K.L. Tan, CASTLE: continuously anonymizing data streams, IEEE Trans. Depend. Secure Comput. 8 (3) (2011) 337–352.
[24] I. Cha, Y. Shah, A.U. Schmidt, A. Leicher, M.V. Meyerstein, Trust in M2M communication, IEEE Trans. Veh. Technol. 4 (3) (2009) 69–75.
[25] Dong Chen, Guiran Chang, A survey on security issues of M2M communications in cyber-physical systems, KSII Trans. Int. Inf. Syst. 6 (1) (2012) 24–45.
[26] Soumya Kanti Datta, Christiannti Bonnet, A lightweight framework for efficient M2M device management in oneM2M architecture, in: Proceedings of 2015 International Conference on Recent Advances in Internet of Things (RIoT), IEEE, 2015.
[27] Soumya Kanti Datta, Amelie Gyrard, Christian Bonnet, Karima Boudaoud, oneM2M architecture based user centric IoT application development, in: Proceedings of 2015 3rd International Conference on Future Internet of Things and Cloud (FiCloud), IEEE, 2015.
[28] O. Delgado-Mohatar, A. Fuster-Sabater, J.M. Sierra, A light-weight authentication scheme for wireless sensor networks, Ad Hoc Netw. 9 (5) (2011) 727–735.
[29] Asma Elmangoush, Adel Al-Hezmi, Thomas Magedanz, The development of M2M standards for ubiquitous sensing service layer, Global Communications Conference, GLOBECOM, 2014, pp. 624–629.
[30] ETSI, Machine To Machine Communications, TS, 102 689.
[31] D. Evans, D. Eyers, Efficient data tagging for managing privacy in the internet of things, in: Proceedings–2012 IEEE Int. Conf. on Green Computing and Communications, GreenCom 2012, Conf. onInternet of Things, iThings 2012 and Conf. on Cyber, Physical andSocial Computing, CPSCom 2012, Besancon, France, 2012, pp. 244–248.
[32] Zubair Md. Fadlullah, Mostafa M. Fouda, Nei Kato, Akira Takeuchi, Noboru Iwasaki, Yousuke Nozaki, Toward intelligent machine-to-machine, Commun. Smart Grid 49 (4) (2011) 60–65.
[33] J. Granjal, E. Monteiro, J. Sá Silva, Security in the integration of low-power Wireless Sensor Networks with the Internet: A survey, Ad Hoc Netw. 24 (2015) 264–287.
[34] L. Gu, J. Wang, B.b. Sun, Trust management mechanism for Internet of Things, China Commun. 11 (2) (2014) 148–156.
[35] T. Heer, S. Varjonen, Host Identity Protocol Certificates, 2011.
[36] Jan Holler, Vlasios Tsiatsis, Catherine Mulligan, Stefan Avesand, Stamatis Karnouskos, David Boyle, From Machine-To-Machine to the Internet of Things: Introduction to a New Age of Intelligence, Academic Press, MA, USA, 2014.
[37] C. Hu, J. Zhang, Q. Wen, An identity-based personal location system with protected privacy in IoT, in: Proceedings - 2011 4th IEEE International Conference on Broadband Network and Multimedia Technology, IC-BNMT 2011, Shenzhen, China, 2011, pp. 192–195.
[38] S.D. Kamvar, M.T. Schlosser, H. Garcia-Molina, The eigen-trust algorithm for reputation management in p2p networks, in: Proc.WWW'03, New York, USA, 2003, pp. 640–651.
[39] T. Kothmayr, C. Schmitt, W. Hu, M. Brunig, G. Carle, Dtls based security and two-way authentication for the Internet of Things, Ad Hoc Netw. 11 (8) (2013) 2710–2723.
[40] Chengzhe Lai, Hui Li, Yueyu Zhang, Jin Cao, Security issues on machine to machine communications, KSII Trans. Int. Inf. Syst. 6 (2) (2012) 498–514.
[41] J.-Y. Lee, W.-C. Lin, Y.-H. Huang, A lightweight authentication protocol for internet of things, in: 2014 International Symposium on Next-Generation Electronics, ISNE 2014, Kwei-Shan, 2014, pp. 1–2.
[42] Z. Liang, W. Shi, Enforcing cooperative resource sharing in untrusted P2P computing environments, Mob. Netw. Appl. 10 (2005) 251–258.
[43] Rongxing Lu, Xu Li, Xiaohui Liang, Xuemin (Sherman) Shen, Xiaodong Lin, GRS: The green, reliability, and security of emerging machine to machine communications, IEEE Commun. Mag. 49 (4) (2011) 28–35.
[44] J. Ma, Y. Guo, J. Ma, J. Xiong, T. Zhang, A hierarchical access control scheme for perceptual layer of IoT, Jisuanji Yanjiuyu Fazhan/Comput. Res. Dev. 50 (6) (2013) 1267–1275.
[45] P.N. Mahalle, P.A. Thakre, N.R. Prasad, R. Prasad, A fuzzy approach to trust based access control in Internet of Things, in: 2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems, VITAE, NJ, Atlantic City, 2013, pp. 1–5.
[46] M. Nitti, R. Girau, L. Atzori, A. Iera, G. Morabito, A subjective model for trustworthiness evaluation in the social internet of things, in: 2012 IEEE 23rd International Symposium on Personal Indoor and Mobile Radio Communications, PIMRC, Australia, Sydney, 2012, pp. 18–23.
[47] M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the internet of (important) things, IEEE Commun. Surv. Tutor. 15 (3) (2013) 1389–1406.

[48] L.b. Peng, W.b. Ru-chuan, S. Xiao-yu, C. Long, Privacy protection based on key-changed mutual authentication protocol in internet of things, Commun. Comput. Inf. Sci. 418 (2014) 345–355.
[49] G. Piro, G. Boggia, L.A. Grieco, A standard compliant security framework for IEEE 802154 networks, in: Proc. of IEEE WorldForum on Internet of Things (WF-IoT), Seoul, South Korea, 2014, pp. 27–30.
[50] R. Roman, C. Alcaraz, J. Lopez, N. Sklavos, Key management systems for sensor networks in the context of the internet of things, Comput. Electr. Eng. 37 (2) (2011) 147–159.
[51] R. Roman, J. Zhou, J. Lopez, On the features and challenges of security and privacy in distributed internet of things, Comput. Netw. 57 (10) (2013) 2266–2279.
[52] A.A. Selcuk, E. Uzun, M.R. Pariente, A reputation-based trust management system for P2P networks, in: Proc. of CCGRID 2004, Washington, DC, USA, 2004, pp. 251–258.
[53] F.K. Shaikh, S. Zeadally, Energy harvesting in wireless sensor networks: A comprehensive review, in: Renewable and Sustainable Energy Reviews, vol. 55, Elsevier, 2016, pp. 1041–1054.
[54] S. Sicari, A. Rizzardi, L. Alfredo Grieco, A. Coen-Porisini, Security, privacy and trust in internet of things: The road ahead, Comput. Netw. 76 (2015) 146–164.
[55] S. Sicari, C. Cappiello, F.D. Pellegrini, D. Miorandi, A. Coen-Porisini, A security- and quality-aware system architecture for Internet of Things, Inf. Syst. Front. 18 (4) (2016) 665–677.
[56] François Siewe, Towards the modelling of secure pervasive computing systems, J. Parallel Distrib. Comput. 87(C) (2016) 121–144.
[57] L. Sweeney, k-Anonymity: A model for Protecting Privacy, Internat. J. Uncertain. Fuzziness Knowledge-Based Systems 10 (5) (2002) 555–570.
[58] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, J. Song, Toward a standardized common M2M service layer platform: Introduction to oneM2M, IEEE Wirel. Commun. 21 (3) (2014) 20–26.
[59] G.D. Tormo, F.G. Marmol, G.M. Perez, Dynamic and flexible selection of a reputation mechanism for heterogeneous environments, Future Gener. Comput. Syst. 49 (2015) 113–124.
[60] M. Turkanovi, B. Brumen, M. Hlbl, A novel user authentication and key agreement scheme for heterogeneous ad hoc wireless sensor networks, based on the internet of things notion, Ad Hoc Netw. 20 (2014) 96–112.
[61] Y. Wang, Q. Wen, A privacy enhanced dns scheme for the internet of things, in: IET International Conference on CommunicationTechnology and Application, ICCTA 2011, Beijing, China, 2011, pp. 699–702.
[62] Geng Wu, Shilpa Talwar, Kerstin Johnsson, Nageen Himayat, Kevin D. Johnson, M2M: From mobile to embedded internet, IEEE Commun. Mag. 49 (4) (2011) 36–43.
[63] Z.Q. Wu, Y.W. Zhou, J.-F. Ma, A security transmission model for internet of things, Jisuanji Xuebao/Chin. J. Comput. 34 (8) (2011) 1351–1364.
[64] L. Xiong, L. Liu, Peertrust: supporting reputation-based trust for peer-to-peer electronic communities, IEEE Trans. Knowl. Data Eng. 16 (2004) 843–857.
[65] X. Xiong, D.S. Wong, X. Deng, TinyPairing: A fast and lightweight pairing-based cryptographic library for wireless sensor networks, in: Proceedings of the IEEW Wireless Communications and Networking Conference, 2010, pp. 1–6.
[66] Z. Yan, P. Zhang, A.V. Vasilakos, A survey on trust management for Internet of Things, J. Netw. Comput. Appl. 42 (2014) 120–134.
[67] J. Yang, B. Fang, Security model and key technologies for the internet of things, J. China Univ. Posts Telecommun. 8 (2) (2011) 109–112.
[68] B. Yu, M.P. Singh, K. Sycara, Developing trust in large-scale Peer-to-Peer systems, in: Proc. of First IEEE Symposium on Multi-Agent Security and Survivability, 2004, pp. 1–10.
[69] Yan Zhang, Rong Yu, Shengli Xie, Wenqing Yao, Yang Xiao, M. Guizani, Home M2M networks: Architectures, standards, and QoS improvement, IEEE Commun. Mag. 49 (4) (2011) 44–52.
[70] Kai Zhao, Lina Ge, A survey on the internet of things security, in: Proceedings of 2013 9th International Conference on Computational Intelligence and Security, CIS, 2013, pp. 663–667.

Gurkan Tuna serves as an Assoc. Prof. at Edirne Vocational School of Technical Sciences, Trakya University, Turkey. He received his B.S. degree in computer engineering from Yildiz Technical University, Istanbul, Turkey, in 1999, and his M.S. degree in computer engineering from Trakya University, Edirne, Turkey, in 2008. He received his Ph.D. degree in electrical engineering from Yildiz Technical University, Istanbul, Turkey, in 2012. Tuna has authored several papers in international conference proceedings and refereed journals. He has been serving as a reviewer for international journals and conferences. His current research interests include smart grid, the Internet of Things, ad hoc and sensor networks, and robotic sensor networks.



Dimitrios G. Kogias is an Adjunct Lecturer and a Senior Researcher at the Dept of Electronics Engineering of Piraeus University of Applied Sciences (PUAS). He has participated in National and European projects while he has, also, taken part to international conferences. His work has been published in international Journals and he has co-authored two book chapters. His current research issues are in IoT device communication and privacy, cloud computing and security.

Vehbi Cagri Gungor received his B.S. and M.S. degrees in Electrical and Electronics Engineering from Middle East Technical University, Ankara, Turkey, in 2001 and 2003, respectively. He received his Ph.D. degree in electrical and computer engineering from the Broadband and Wireless Networking Laboratory, Georgia Institute of Technology, Atlanta, GA, USA, in 2007 under the supervision of Prof. Ian F. Akyildiz. He was an Associate Professor and the Graduate Programs (Ph.D. and M.S.) Coordinator at the Department of Computer Engineering, Bahcesehir University, Istanbul, Turkey. He is now associate professor at Abdullah Gul University (Turkey). His current research interests are in smart grid communications, machine-to-machine communications, next-generation wireless networks, wireless ad hoc and sensor networks, cognitive radio networks, and IP networks. Dr. Gungor has authored several papers in refereed journals and international conference proceedings, and has been serving as an Editor, and program committee member to numerous journals and conferences in these areas. He is also the recipient of the IEEE Transactions on Industrial Informatics 2012 Best Paper Award, the IEEE ISCN 2006 Best Paper Award, the European Union FP7 Marie Curie IRG Award in 2009, Turk Telekom Research Grant Awards in 2010 and 2012, and the San-Tez Project Awards supported by Alcatel-Lucent, and the Turkish Ministry of Science, Industry and Technology in 2010.

Cengiz Gezer is currently working for Netaş Telecommunications Inc., Istanbul, Turkey. He received his B.S. degree (2005) in electrical and electronics engineering from Osmangazi University, Eskişehir, Turkey, his M.S. degree (2008) in telecommunication engineering from Istanbul Technical University, Istanbul, Turkey and his Ph.D degree (2012) in telecommunication engineering from University of Bologna. His research interests include machine type communications, wireless sensor networks and security.

Erhan Taşkın is currently working for Netaş Telecommunications Inc., Istanbul, Turkey. He received his B.S. (2002) and M.S. (2005) degrees in computer engineering from Canakkale Onsekiz Mart University, Canakkale, Turkey and his Ph.D degree (2013) in computer engineering from Trakya University, Edirne, Turkey. His research interests include digital image and video processing, machine type communications, next generation networks and security.

Erman Ayday is an Assistant Professor of Computer Science at Bilkent University, Ankara, Turkey. Before that he was a Post-Doctoral Researcher at Ecole Polytechnique Fédérale de Lausanne (EPFL), Switzerland, in the Laboratory for Communications and Applications 1 (LCA1) led by Prof. Jean-Pierre Hubaux. He received his M.S. and Ph.D. degrees from Georgia Tech Information Processing, Communications and Security Research Lab (IPCAS) in the School of Electrical and Computer Engineering (ECE), Georgia Institute of Technology, Atlanta, GA, in 2007 and 2011, respectively under the supervision of Dr. Faramarz Fekri. He received his B.S. degree in Electrical and Electronics Engineering from the Middle East Technical University, Ankara, Turkey, in 2005. Erman's research interests include privacy-enhancing technologies (including big data and genomic privacy), wireless network security, game theory for wireless networks, trust and reputation management, and recommender systems. Erman Ayday is the recipient of Distinguished Student Paper Award at IEEE S&P 2015, 2010 Outstanding Research Award from the Center of Signal and Image Processing (CSIP) at Georgia Tech, and 2011 ECE Graduate Research Assistant (GRA) Excellence Award from Georgia Tech. He is a member of the IEEE and the ACM.