A Review on Security and Scalability in M2M

Simranjit Singh, Pavan Kumar Verma

Department of Electronics and Communication Engineering, Dr. B.R. Ambedkar National Institute of Technology Jalandhar, India

*Corresponding author

doi: https://doi.org/10.21467/proceedings.114.25

Abstract

In this paper, we review the scalability and security issues in machine-to-machine(M2M) communications and their proposed solutions. Numerous methods and protocols are available for addressing the issue of security and scalability in M2M communications. Security aspect of the M2M communication should be addressed from the beginning itself so that the implementation of various applications become feasible. All the requirements for interconnection of thousands of devices, M2M networks should have huge scalability for low-cost connectivity according to the need. With the help of a scalable M2M network, cost efficiency becomes higher and consumption of power also decreases.

Keywords: Machine-to-Machine(M2M), Scalability, Security

1 Introduction

In the present scenario of forward-looking research in the field of communication, much work has been done to date. We live in the age of machine communication where the machine works more intelligently than man and therefore the world is more intelligent. As far as automatic communication between machines is concerned, the machine must be intelligent and machine makes its decision without direct human interference in order to improve cost-effectiveness and time management. When we talk about the word automatic then in the spirit first name comes, that is, SCADA (supervisory control and data acquisition systems). In this sensor and embedded systems are connected by a certain network and driving by computer for industrial use.Connection of M2M can be established by using a computer with internet access, wireless connection and various sensors. The M2M network included information about the device as well as information by connecting the devices to the gateway to connect the device's network. M2M has huge scope in industries, automation in industries, monitoring from distance, advanced transportation, telematics, medical services, security, electronics, managing the fleet, advanced metering, advanced homes and smart grid. When we talk about M2M communication growth, we're seeing lower costs and greater connectivity. We are already accustomed to cheap, broadband and commercial Internet access. To the current worldwide scenario concerning the LTE and 5G communication network providing speed access at a competitive price that have almost the same speed access. M2M has also implemented IP-based connecting devices to move the world at various stages such as monitors, actuators and sensor devices, in house and industrial works. To have progress through latest interconnection and interoperable service that have the capacities renovate our everyday lives. To obtain the updated information, M2M provides many applications such as IoT (Internet of Things). Requirements as key characteristics of M2M communications, the variety and diversity of applications, device functionality and market must be considered. Finally, we think and learn about to flexibility of M2M design and application on how to useful for technology increment for future purpose of enabling interoperate machine. how do we preserve the identity and confidentiality of information without limiting potentially beneficial applications; how do we ensure the actual capacity of these systems when we are becoming more and more accustomed to them; One person or organization is not able to provide all of these solutions.

Proceedings DOI: 10.21467/proceedings.114; Series: AIJR Proceedings; ISSN: 2582-3922; ISBN: 978-81-947843-8-8

2 Scalability

Herstad et. al. [9] purposed the exhibition platform to support adaptability functionality, technology, fast development, scalability and independence on the device. Where Distributed processing of items for hot connection in runtime configuration and competition for parallel behavior management have also been supported by the platform. For the point-to-point distribution of messaging service was implemented by the queue. Various routing algorithms are supported by COOS (Connected Objects Operating System).Its configurability can be enhanced using various filters and transports. Modularity of the message bus supports distributed processing. It facilitates distribution between carrier network, locations, Java platforms and technologies. High availability M2M system needs hot plugging and run time configuration. Decoupled modules can be reconfigured and installed during run time because of modularity. The metrics are not providing the comparison and evaluation with other designs.

Singh and Huang [17] discussed architecture developing the network of M2M network practically deployment scenario. A universal method for effective and efficient monitoring and maintenance of monitoring that are deployed in several M2M devices, tracking and monitoring was discussed. In this method, performance (together withno M2M bridge) was assessed using the simulator written in C. The achievement was showed for better scalability of M2M gateway at expected proposed architecture. Control signalling was reduced significantly with this. It is suitable for delay-tolerant applications. To effectively deploy M2M systems, the requirement of the M2M device model must be generalized.

Allalouf et. al. [3] Introduce the re-routing protocol for a different cross layer. The path that maximizes data reduction is chosen by the protocol. The issue of smart grid congestion due to the generation of large amounts of data from smart meters is addressed. Two types of overload control and congestion avoidance mechanisms for MTC devices are proposed by Taleb and Kunz [18]. One is the soft mechanism and the other one is the rigid mechanism. In soft mechanism, for minimizing the frequency from measuring on soft level by attempting the MTC devices are taken by mobile operator without strangling them. In rigid mechanism, rigid measures are taken for disallowing the concerned MTC devices from executing indeed procedures and connecting to the network by the mobile operator. MTC devices are grouped with mobility with low features. (Corici et. al.) [7] and assigning each TCM device gives time for assigning and subscribing sound in HSS, where small data has been transmitted via online/offline access mode and low priority. LTE-A (Chen, 2010) [6] can be used to solve signalling overhead and complexity issues in M2M communications.

Lien et. al. [13] proposed ACB (Cooperative AccessClass Barring) for access load sharing and global standardization in M2M communications. It eliminated defects in ordinary ACB. This facilitated device escaping from continuous congestions and improved access delays.In this author was to find the idea of a problem with the mathematical type pattern in which the selection of the BS strategy for each MTC device, the co-operative access class was validated with the exception of three pre-positions. A simulation considered 3 Pico and 7 macro cells, two metrics i.e. averaging the throughput and delay, and worst throughput and worst delay for validation of solution. According to the results of the simulation, the proposedCooperative ACB achieved 30 percent improvement as compared simple ACB (both in worst case and delay).

Pawan et. al. (2018) [19] in their paper discussed the necessity of a medium access control protocol which is scalable and energy efficient. Such a protocol would have anadvantage as it could expedite a great deal of M2M devices to facilitate the assessment of the channel. To achieve this, anew hybrid-MAC protocol was put forward, that mainlycontains a Data Transmission Interval (DTI) and also a Contention Interval (CI). In this setup, all the devices make use of a MAC with multiple beam antenna array, i.e. the MBAA-MAC protocol. The protocol discussed here is able to provide a high value of throughput as a result of multiple

Proceedings DOI: 10.21467/proceedings.114
ISBN: 978-81-947843-8-8

Series: AIJR Proceedings
ISSN: 2582-3922

transmissions at the same time. In random grid topology's case, with the increase in the number of transmission pairs, we can see an overall increase in the throughput of thenetwork. Also, in random topology's case, the increase inthe number of flows aids the increase in throughput. At last, in cluster topology's case, the results obtained fromsimulation depicted that during DTI, the MBAA-MAC protocol would perform a lot better than IEEE 802.11 DCF protocol per time slot and hence the overall throughput ofthe network rose up to a value of 110%. Another observation obtained from simulation results was that the enabling of MBAA-MAC protocol would improve the energy consumption in M2M devices.

Zhang et. al. (2020) [20] tried the optimization of the throughput of massive random access of M2M with a guarantee of delay in the industrial IOT. At the entry stage of network, the random access collision is a censorious issuein case of massive M2M communications. To reduce the channel contention at the stage of network access need the back off parameters from base station, the calculation of whose proper values is a problematic affair. This paper studies a novel technique of distributive estimation of the proper value of back off parameters. With the use of observed values of total and successful transmissions ofaccess results by each machine type device, an estimation can be obtained for the optimal value of back off parameters. As it turns out, the performance of the proposed scheme is determined by the estimation interval. By proper selection of the estimation interval value, we can work towards maximizing the throughput where the number of MTDs is fixed in the given network. The scheme suggested can be applied to heterogeneous as well as homogeneous scenarios. The other advantage of the scheme proposed inthe paper is that it is capable of achieving same performancebut with a considerable amount of low s signalling overheadand it also lays out a design method for traditional M2M communication which has practical access.

Althumali et. al. (2020) [1] Suggest how to select the best coverage zone and spectrum efficiency for M2M infrastructure where a large number of devices are used to network resources at same time. Random Access Channel (RACH) design in the massive access to verify and obtain ofachieve for collision and congestion due to that degraded system performance. When considering the above issue, propose collision resolution schemes using a backup indicator (BI) that describes how many standby devices are available for resource use. This scheme has three integrated access techniques: Standard Random Access (SRA), Static Access Class (ACB) and Dynamic Access Class (DAB). The optimized BI value that achieves approximate access success is computed for the 3 different regimes. after analyzing, the RP is indicated, reaching the access rate of around 99% [1], A certain tolerance to delay is overlooked, it is also necessary for an increase in mass arrivals scenarios.

3 Security

Latest M2M standards and architecture were presented by Jiang, & ShiWei [11] with a focus on communication issues and security. According to the author heterogeneous devices are one of the most prominent problems in M2M communication. This makes determiningthe way to identify devices uniquely and enabling a secure communication through them the main research challenge. For the first problem, the authors proposed an identifying scheme, which allows the identification of devices independently of the technology used. With respect to the second issue the authors discuss the basic processes, the current M2M architecture and standards used for a secure connection.

The different characteristics and limiting resources of M2M systems in case of H2H systems also present challenges in design of suitable security mechanisms that allow M2M systems to control heterogeneous sensing. In addition, because there may be a condition where users mayrequire systems that will make it easier to control the amountof personal information that is made available. In addition, certain other

requests may require a fixed amount of availability of personal information (Cha et. al. [5]). Therefore, the security and privacy of M2M systems become important considerations.

In the M2M domain, Some M2M nodes may toggle into sleep mode for power saving and not monitored (Lu et. al. [14]). Since hackers can easily attack the unsupervised M2M devices (Saedy and Mojtahed [16]) which increases the vulnerability of these nodes (which are not being monitored) to get injected by fake data reports (Hongsong et. al. [10]; Kitagami et al., 2012 [12]). To avoid this vulnerability of M2M communications, secure communication is required. (Bartoli et. al. [4]), appropriate monitoring needs to be improved and security techniques to detect suspicious events, like changing thelocation of the device, damage to device (Fu et al., 2011) [8] etc. Various other privacy and security problems in M2M communication which need immediate attention include physical and configuration attacks, protocol attacks as well as core network attacks, attacks on the identity and data of the user and unsupervised M2M system being prone to security issues (Hongsong et. al. [10]).

TABLE I. ADVANTAGES AND APPLICATIONS OF M2M TECHNIQUES

Technique	Description	Advantages	Applications
Build an M2M service platform	Demonstrate solutions to issues by setting a service platform architecture to connect objects	supports quick growth, competition, responsiveness, adaptive management, scalability	Provides platforms for the service provider for service development.
Effective Integration of Capillary	A method to efficiently manage and monitor M2M devices deployed for various applications	reduces the overall signaling of monitoring	delay-tolerant applications
Data Quality Aware Volume Reduction	Study data traffic for the intelligent network by advanced measurement within a limited bandwidth	manages congestion by intelligently reducing the volume of conscious quality flows offline	Smart grid networks
Un-peer2peer Protocol Stack	Offers improved support of M2M communication with less complexity and development costs.	less complexity and development cost	fleet management remote control security applications
Adaptive hybrid mac protocol for high volume M2M networks	The protocol provides high throughput through several concurrent transmissions.	Increases overall network throughput.	real-time applications, namely smart grid, remote e-healthcare, home automation
Dynamic Backoff Collision Resolution	Adjusts the Backoff Indicator (BI) to match the number of devices on hold and the resources available	Collision Rate is reduced, Improve energy efficiency, Reduce access delay	Security And management of resources
Cooperative Access Class Barring(ACB) for M2M	for overall stabilization and sharing of access load to eliminate significant defects in the standard ACB.	Improving access delays	Smart access stabilization of ACB

Lu et. al. [14] Offer the security technique in M2M node detection for efficient bandwidth, cooperative authentication (BECAN) and compromise the fake data torque filter respectively. In this technique, the detection is compromised by the nodes surrounding the coupling mode.Used by the BECAN schema where the attacker injected data that is wrong and this work is done internally And it detects, filters by en route nodes using this route filtering probability (EFP) and filter report (FR). Simulate the route of the filtration probability and the length of the route indicating the EFP increase as the number of knots increases. The long polling communication method for M2Mremote monitoring services is efficient as a communication protocol that simultaneously meets the security and immediacy requirements.

Kitagami et al. (2012) [12] provided an Stand-alone control method for balancing and grading using only devicesand servers, without the use of a multimedia server. The efficacy of a particular method is determined by a simulationusing two parameters, namely elapsed time and load index. Simulation results indicate that the proposed approach is effective.

Renuka et al. (2019) [22] proposed it allowed Cyber-PhysicalSystems in the authentication scheme in an M2M network tobecome more effective and secure in authentication. It enables any pair of entities in M2M to authenticate oneanother and accept a session with a unique key for secure communication. This process has not intercepted the M2M service provider and it removes the burden of large-scale devices for authentication. With the help of a mobile secret key user, browse at random and authenticate any M2M domain network. This authenticated bridge makes it possiblefor the mobile user to authenticate with any sensor node in the field. Authentication is achieved through the use of invocation and symmetrical key encryption. This system is adapted to environmental sensors that have limited resources(calculation, storage, energy, etc.).

Castilho et al. (2020) [21] introducing Middleware Security, This promised to ensure the safety of the network controller and the Internet connection in the industrial network as well as homely. The Raspberry Pi Gateway Access Point (RGAP) with Linux- Xenomai operating system delivers an AP to OPC on an IEEE 802.11 in wireless network for the purpose of security in WPA2. In this work corresponding to the data and encrypted the command subsequently unable to access the information from the control system. Testing the proposed model using Constrained Application Protocol (CoAP) and the Message Queue Telemetry Transport (MQTT) protocol, provide opportunity to avoid the risk from which Internet-connected devices are exposed normally. By the implementing the RGAP for OPC authentication improves the authentication security. It assures and gets the security athigh level mainly focuses on MQTT. Using this model for both home and industry that control networks that get healthyperformance and synchronize time for challenging tasks through RTOS SO in real time.

References

[1] ALTHUMALI, H. D., & OTHMAN, M. (2020). Dynamic Backoff Collision Resolution for Massive M2M Random Access in Cellular IoT Networks.

[2] D.Castilho, S., & Godoy, E. P. (2020). Implementing Security and Trust in IoT/M2M using Middleware.

[3] Allalouf, M., & Gershinsky, G. (2011). Data-Quality-Aware Volume Reduction in Smart Grid Networks., (p. 6).

[4] Bartoli, & Serrano. (2010). Secure lossless aggregation for smart grid M2M networks.

[5] Cha, & shah. (2009). Trust in M2M Communication.

[6] Chen, Y., & Wang, W. (2010). Machine-to-Machine communication in LTE-A.

[7] corici, & Fiedler. (2011). Evolution of the resource reservation mechanisms for machine type communication over mobile broadbandevolved packet core architecture.

[8] Fu, & jing. (2011). Application-based identity management in M2M system.

[9] Herstad, A., & Nersveen, E. (2009). Connected Objects: Building a Service Platform for M2M., (p. 15).

[10] Hongsong, & Zhongchuan. (2011). Security and trust research inM2M system.

[11] Jiang, & ShiWei. (2010). A study of information security for M2M ofIoT.

[12] Kitagami, & kaneko. (2012). Method of autonomic load balancing forlong polling in M2M service system.

[13] Lien, S.-Y., & Liau, T.-H. (2012). Cooperative Access Class Barring for Machine-to-Machine Communications.

[14] Lu, & Li. (2011). the green, reliability, and security of emerging machine-to-machine communications.
[15] Renuka, K., & Kumari, S. (2019). Design of a Secure Password-basedAuthentication Scheme for M2M Networks in IoT enabled Cyber- Physical systems.
[16] Saedy, & Mojtahed. (2011). Ad hoc M2M communications and security based on 4G cellular system.
[17] Singh, S., & Huang, K.-L. (2011). A Robust M2M Gateway forEffective Integration of Capillary and 3GPP Networks ., (p. 3).
[18] Taleb, T., & Kunz, A. (2012). Machine Type Communications in 3GPP Networks: Potential, Challenges, and Solutions., (p. 7).
[19] Verma, P. K., Verma, R., & Alrayes, M. M. (2018). A novel energy efficient and scalable hybrid-mac protocol for massive M2M networks.
[20] Zhang, C., & Sun, X. (2020). Distributive Throughput Optimization for Massive Random Access of M2M Communications in LTE Networks.
[21] D.Castilho, S., & P. Godoy, E. (2020). Implementing Security and Trust in IoT/M2M using Middleware.
[22] Renuka, K., & Kumari, S. (2019). Design of a Secure Password-based Authentication Scheme for M2M Networks in IoT enabled Cyber-Physical systems.

Proceedings DOI: 10.21467/proceedings.114
ISBN: 978-81-947843-8-8

Series: AIJR Proceedings
ISSN: 2582-3922