International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp. 175-184
http://dx.doi.org/10.14257/ijsia.2014.8.3.19

Cooperative Architecture for Secure M2M Communication in Distributed Sensor Networking

Sungmo Jung, Donghyun Kim and Seoksoo Kim[1]

Department of Multimedia, Hannam University, 306-791 Daejeon, Korea
sungmoj@gmail.com, donghyunk1986@gmail.com, sskim0123@naver.com

Abstract

Machine to machine (M2M) technology has emerged as a rapidly developing technology for large-scale networking of devices without dependence on human interaction. The new form of machine interconnectivity integrates with cloud computing infrastructure through the Internet however, M2M communication poses unique security challenges as the Internet grow steadily and rapidly. The large number connected devices enable attackers to compromise the network nodes through automated and self-propagating malwares such as distributed denial of service attacks (DDoS). This paper presents a cooperative architecture for M2M system security to enable M2M nodes to interface with intelligent devices sensing real-world conditions and control physical devices. We also present performance results of our cooperative architecture that shows that our security scheme is capable of reliably handling concurrent events generated by different types of M2M devices to achieve a high degree of security.

Keywords: *Machine-to-Machine, Distributed Sensor Network, Secure Communication, Cooperative Architecture, Network Security*

1. Introduction

The emergence of cloud computing provided the ease of use, on-demand self service, location independent resource pooling, dynamic provisioning capabilities, scalability, performance, reliability, virtualization, and pay per use services. Cloud computing applications led to the reduction of the costs associated with the management of hardware and software resources in the network [1]. With the recent convergence of Internet and wireless communications for cloud computing, machine (M2M) technology has become the focus of machine-based communications. M2M communications involves the automated transfer of information and commands between two machines without human intervention at either end of the system [2]. M2M involves low-cost, scalable and reliable inter-machine interaction via wireless communication standards like GSM, GPRS, WLAN, Bluetooth, and Zigbee technology [3, 4]. With M2M technology still at its early stage, wireless service is one of the many important links in a machine to machine deployment chain.

M2M technology is capable of building wireless M2M ecosystems covering a wide range of applications for a professional and personal everyday life. With increased processing power, it would enable to jointly deliver federated cloud services to users that fully leverage the power of cloud. With its capability of capturing and analyzing the massive amount of data available in all kinds of smart devices, M2M is a business concept used for automatic

[1] Corresponding Author

ISSN: 1738-9976 IJSIA

transmission of data from remote sources by wired, wireless, radio, and other transmission technologies.

Despite the technology existing in its various forms, deployment of M2M technologies by M2M innovators is hounded by challenging privacy and security issues. The large number connected devices enable attackers to compromise the network nodes through automated and self-propagating malwares such as distributed denial of service attacks (DDoS). Additionally, without the use of passwords or PIN codes, it poses security challenges when deploying M2M technologies as it has less possibility to control changes compared to a more traditional human to machine (H2M) technologies. Also, if the data traffic over GPRS from M2M devices becomes too large there is a risk of blocking out other data services and even normal phone calls as it can be susceptible to attacks by malicious hackers. Security is a requirement for a reliable and secure M2M communication.

In this paper, we present a security mechanism for M2M technologies with cloud computing to address security issues. Our goal is to devise new cooperation schemes that allow network nodes to be notified of possible attacks before being targeted by them, thus enabling the deployment of preventive defenses. Specifically, we define a cooperative architecture for service delivery, data acquisition, and transmission of data in cloud computing. The secure service delivery aids in providing massive amounts of M2M information exchange through cloud computing environment.

2. Related Works

M2M is a promising technology, although still in its early phase. The high technological advancement in the field of communication and computation fueled by wireless mobile networks and sensor networks have allowed the development of a new technology called machine-to-machine communications [5, 6] which has recently received considerable attention.

There have been previous surveys on the characteristics, applications, and communication protocols in WSNs [7, 8] which addressed several design and security issues and techniques for WSNs describing the physical constraints on sensor nodes, applications, architectural characteristics, and the protocols proposed in all layers of the network stack. For instance, a large number of compromised machines are used by attackers to build large networks of bots that are used to carry out malicious activities. Particularly, botnet infrastructures are responsible for the vast majority of distributed denial of service attacks. Some estimates [9] show that botnets created through a worm that reached the size of two million machines. Other recent data concerning worm spread can be obtained from the website [10]. Many M2M applications pose complex design and software challenges and therefore demand a pre-integrated and well-tested software solution [11]. However, not much research has been done to address security challenges in M2M systems.

3. Cooperative M2M Systems

M2M systems consist of wireless sensor networks connected to the outside world through the Internet. Devices are equipped with heterogeneous wireless sensors that can monitor behavior, conditions and can interface with virtually any type of mechanical, electrical or electronic system for an unlimited number of specific applications, which include access control and security, vehicle tracking systems, home automation systems, automotive systems, robotics, and medical systems. A wireless sensor network is composed of the sensors and their local interconnections, the gateway to the external world, a transport network and a service platform that handles the data and supports applications and users [12]. M2M

technology is primarily a combination of various technologies such as wireless sensors, Internet, personal computers, and software technologies. In M2M, a field node or a group of field nodes gather data and send it wirelessly through a network where it is routed, often over the Internet, to a server or cloud of servers.

Due to M2M systems' limitation in terms of security, a cooperative mechanism enables deployment of preventive defenses. A cooperative architecture [13] is characterized by a hierarchical topology. Its main innovation is the ability to gather alerts and malware specimens from a wide network space, thus allowing for early detection of emerging threats. Moreover, all the networks involved in the cooperative intrusion detection effort can be alerted about new threats as soon as they are detected.

In M2M systems, a cooperative sensor is defined as a component that relays the generated alerts to a cooperative intrusion detection architecture. We define a cooperative network as a network in which at least a cooperative sensor is deployed. Theoretically, any machine connected to the Internet has the same chance of being targeted by a worm, however the presence of firewalls has the effect of slowing the infection because some protocols are blocked for inbound connections. With the aid of IDS sensors and honeypots throughout a large number of heterogeneous and geographically distributed networks, administrators can thoroughly monitor both malware spread and attack trends. A typical cooperative M2M technology for cloud computing which comprises the following basic components [14, 15] is shown in Figure 1.

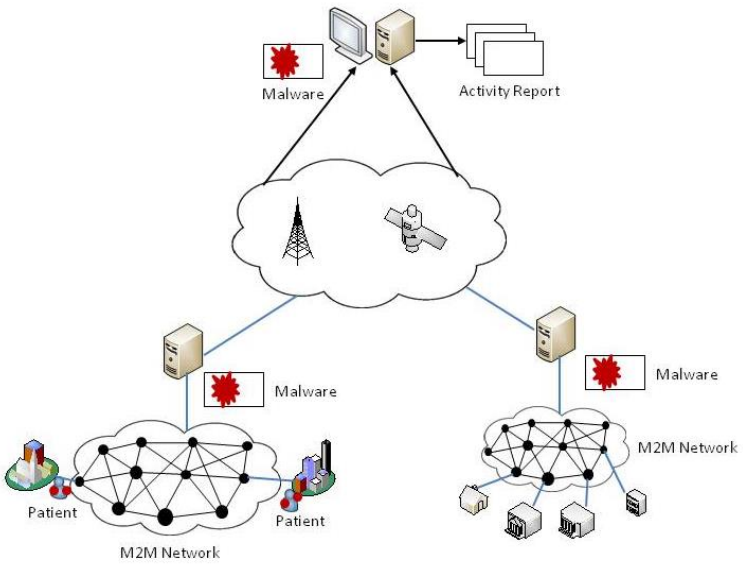

Figure 1. Cooperative M2M Architecture

M2M allows a wide variety of machines to become nodes of personal wireless networks, global Internet which provides to develop monitoring and remote control applications. This will decrease costs for involved human resources and will make machines more intelligent and autonomous. Wireless M2M technology brings in new direction the state of development of the systems for data acquisition and control. The systems are not only passive data collecting modules which delivers sensed data to some central machine for analysis and data processing in some proprietary network, something more systems getting more and more autonomous in decision making for control and in machine to machine coordination. The

need to manage diverse M2M facilities motivates several requirements such as maintenance, inventory management, access control, location tracking, and remote monitoring for which an M2M solution would be useful.

M2M system for data acquisition and control belongs to the class of distributed, heterogeneous, network systems for data collecting, data processing and process control. It provides following features for remote data monitoring and control of subsystems, communication and control interfaces to industrial microcontrollers integrated into machine network system, building data acquisition tracking systems, cooperative task processing and evaluations between subsystems, building of heterogeneous networks based on wireless and wired communication technologies, and service of different type of embedded devices using wireless and wired interfaces.

3.1. Load Balancing

M2M systems are susceptible for malicious attacks due to lack of security mechanisms. Consider a realistic scenario in which a network participating to a cooperative architecture of an M2M system is targeted by an attacker, while the other participating networks are not. This scenario is represented in Figure 2. Uneven load distribution is effectively mitigated by the distributed alert aggregation and correlation approach. Lacking a single, centralized aggregator to which all the alerts have to be transmitted, there is no single path through which all the alerts generated by a sensor.

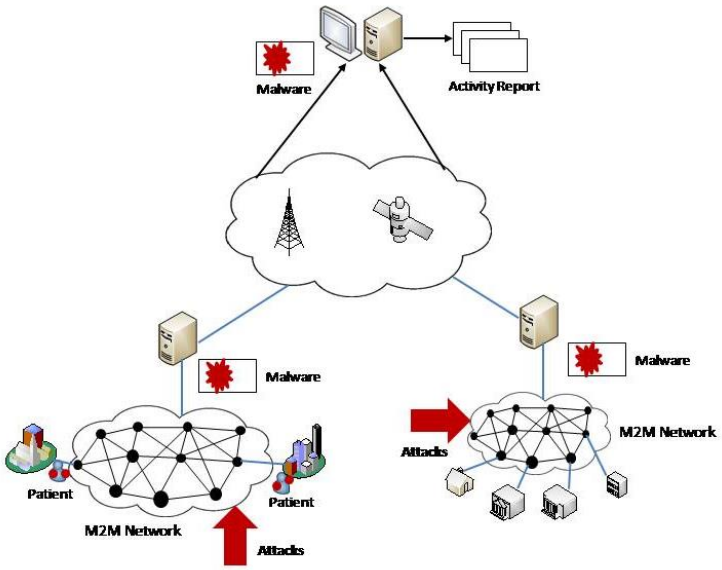

Figure 2. Load Balancing

3.2. M2M Network Activity Reporting

M2M systems implements several design strategies such as push strategy, pull strategy, and hybrid strategy. This paper will consider the push strategy where intelligent devices initiate the communications and sends data through an M2M domain over the cloud to a remote user. In this operation, the device recognizes predefined conditions and triggers itself to send alarms, alerts, e-mails, data and commands to an M2M domain. Subsequently, the gateway connects over the network through the Internet to send data to the remote users.

The ability to generate and disseminate timely and detailed information on the M2M network-based attacks and malware spreading through the Internet represents the main purpose of the cooperative architectures requiring one or more cooperative sensors.

This scenario enables network activity reports to be sent to all the cooperating networks, even to those not yet reached by the malware. In this way, all the participating parties receive the information needed for deploying defensive countermeasures, such as blocking certain network connections, closing ports or patching some software applications. The exchange of information between the cooperating networks is the most effective measure against the spread of malware. Furthermore, the knowledge about the infection vector may be shared very early with the vendor of the targeted software, which can start correcting the problem when only few machines have already been attacked.

3.3. M2M Secure Service Delivery

When delivering an M2M service, there are concerns towards the efficiency and reliability. In dealing with M2M computing, one can assume that almost all services consist of wireless sensor communication. Some services might utilize other elements than sensors such as more hardware-oriented communication methods, but sensor networks will be the basic object for most services. Because of this there will be a need for a module that is responsible for handling the communication with the wireless sensors.

Table 1. M2M Communication Attacks

M2M attacks	Encryption Policies	Secrecy	Privacy
Cipher-text attack	M2M service encryption using private keys	Yes	No
Chosen plaintext attack	M2M service encryption using permanent keys	Yes	No
Known plaintext attack	M2M service encryption using temporary keys	Yes	No
Man-in-the-middle attack	M2M service without encryption	No	No

Issues and challenges in M2M communications revolve around the areas of security, privacy, reliability, robustness, latency, cost-effectiveness, software development and standardization. Security is one of the most important considerations while designing an M2M system, as the users do not want the hackers to break into M2M applications designed to control, for example, building security, environmental monitoring, vehicle tracking, etc. In order to prevent possible security violations, the most appropriate communication techniques must be used, because different types of communication techniques present different encryption and security features. For instance, Ethernet technology does not provide encryption and, it can provide only limited security with the use of a firewall. Thus, shown in Table 1 are the possible attacks and vulnerabilities in M2M service delivery using Ethernet technology. Cellular operators, on the other hand, provide encryption and access authorization to data sent over the network. Reliability is another important issue. The intelligent devices used in an M2M network should be reliable by means of availability. Energy-efficient sensors and techniques must be developed to allow these devices to communicate over short distances using less power, or over long distances using line-powered bridges so that the battery energy is utilized more efficiently, for longer continuous operation without maintenance. Latency is also a concern in many M2M applications. For example, in the case of intruder detection, an

alarm that cannot be sent on time can be useless since the intruder can leave the vicinity of event by the time that the alarm is received.

4. M2M Vulnerabilities

Knowing the vulnerabilities that affect the machines of the protected network enables one to highlight the attacks exploiting the system vulnerabilities. Among all the security alerts received by cooperating nodes, only a few of them represent a real threat. In M2M system security, a system failure is classified according to the threat they pose to the system. The threat T of a system failure is defined as the consequence C such that a system failure will be multiplied by the probability of occurrence P of the system failure for a specific component i.

$$Ti(x) = Ci \times Pi \quad (1)$$

Here the probability P of the entire M2M system failing with the probability Pi for a component i failure. Assessing the security of a system is defined by the security of the individual components, so increasing security can often be done by introducing redundancy into the system. It is, however, not as trivial as it seems to utilize redundancy in order to improve the security of a system. Redundant components are an extra cost that needs to be justified in some way. There may not be sufficient will to invest in redundant resources, if the expense incurred by a failure is less than the cost of preventing it. A thing to note is that the failure rate of the individual components should be considered when introducing redundancy in a system.

4.1. Security

The level of dependability of a system is in the end a trade-off between cost and how reliable the service needs to be. In defining the security features of the M2M system, reliability is a requirement. The reliability of a system has to with the quality of its measurement in providing uninterrupted service [16]. The reliability function R(t) of a system is defined as:

$$Ri(x) = P(Ti > t) = 1 - F(t) \quad (2)$$

4.2. Scalability

Scalability is also another requirement as it provides desirable attribute of the M2M system. The concept connotes the ability of a system to accommodate an increasing number of elements or objects, to process growing volumes of work gracefully, and/or to be susceptible to enlargement [17].

In this security framework, we consider the hardware devices as wireless sensors, mobile devices, access network, and service platform for the reliability. Other components are assumed to be fault-free. The wireless sensors have a failure rate of fws, the access network has a failure rate of fan and the service platform have a failure rate of fsp. The security function can be defined in the following:

$$Si(x) = Ri(x) - e^{-(fws+ fan + fsp)} \quad (3)$$

The security function for the M2M system is defined by the reliability and the failure of network devices. Important to notice is that this implies that a component with a very large failure rate will be dominating the security of a system. If we assume that the failure rates of the sensors are several orders of magnitude larger than those of the access network, it will in essence be useless to introduce a redundant solution for the access network if the devices continuously fail.

5. Implementation

To illustrate the scenario of M2M communication, we implement the use of using wireless sensors and mobile devices to provide IP connection to the M2M smart application where the patient's prescription bottle can send updates on when the medicine has been consumed and also provides alerts to the patient and the monitoring physician. The monitoring of patients will request very high reliability from any service. This means that the service availability have a high value. Table shows details of some aspects of patient monitoring application. It is noteworthy that the worst-case availability offered by the M2M platform per device is actually lower than the stated requirement for the monitoring of patients. In addition, we also need to take into consideration network elements that may fail and consequently lower the availability of services. 96% might be achievable service availability on average, but not per network devices. If this system is to use the public GPRS network in competition with mobile phone users and other M2M services the problems might be even worse. One way of solving this is by using for instance a fixed connection from the house. This will however lead to problems when the patient wants to get out of the house. These are aspects that need to be addressed if such a service is to be launched. Some way of enhancing the reliability for such services is needed to provide reliability as well as security.

Table 2. Monitoring Details

Service Reliability	97.5%
Service Availability	96%
Response Time Average	5 seconds
Number of patients	150
Message Interval	1 minute
Transmission Capacity	4 MB

In Table 3 we report the results of simulations aiming to assess how the replication factor k influences the probability of losing a message. It is possible to configure a replication factor so that each message is sent to the k cooperative alert aggregators whose node is nearest to the message key. In this series of simulation we used a constant network size of 1,000 cooperative nodes and varied both the concurrent failure rate and the replication factor. For each combination of fault rate and replication factor we run 1,000 simulations, and we measure the packet loss probability as the percentage of simulations in which at least one message have been lost.

Table 3. Message Loss Probability (k=4)

Fault rate	500 nodes	1000 nodes
1	0	0
2	0	0
3	0	1
4	1	2
5	2	6
6	5	10
7	7	13
8	12	24
9	25	52
10	38	78

6. Conclusion

Machine-to-machine communication is associated with the automated connectivity of remote machines through the Internet. Successful adoption of M2M technology requires a strategic approach to ensure that the technical solution is balanced with the business case to demonstrate an early return on investment. Simple solutions work best where the technology can be proven quickly and the benefits easily understood. There are many challenges in the successful adoption of M2M technology. In this paper, we provided an understanding of M2M, discussed the security issues, and propose a cooperative architecture for a secure and successful deployment of a resilient M2M solution.

The suggested system architecture gives possibilities for building more intelligent and autonomous wireless M2M system. It resolves the security issues in communication and control problems between different in technical characteristics machines that make them part of global Internet network. The secure software framework allows systems to function in different application domain. Providing reliable services is complicated by the fact that different parts of the network are provided by different entities in the cloud.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2013R1A1A2006026).

References

[1] B. Hayes, “Cloud Computing”, Communications of the ACM, vol. 51, **(2008)**, pp. 9-11.
[2] A. Brown and J. Moroney, “A Brave New World in Mobile Machine to Machine (M2M) Communications”, Strategy Analytics, Forecast and Outlook Snapshot, **(2008)**.
[3] ZigBee Alliance, “ZigBee Overview”, http://www.zigbee.org/documents/ ZigBeeOverview4.pdf.
[4] S. Milanov, “Bluetooth Interface”, www.comexgroup.com/communications/bluetooth.htm.
[5] G. Lawton, “Machine-to-Machine Technology Gears Up for Growth”, Computer, vol. 37, **(2004)**, pp. 12-15.
[6] J. Brazell, L. Donoho, J. Dexheimer, R. Hanneman and G. Langdon, “M2M: The Wireless Revolution”, Texas State Technical College Publishing, **(2005)**.
[7] I. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, “Wireless Sensor Networks: A Survey”, Computer Networks, vol. 38, **(2002)**, pp. 393-422.
[8] S. Tilak, N. Abu-ghazaleh and W. Heinzelman, “A Taxonomy of Wireless Micro-Sensor Network Models”, ACM Mobile Computing and Communications Review, vol. 6, **(2002)**, pp. 28-36.
[9] S. Gaudin, “Storm Worm Botnet More Powerful than Top Supercomputers”, Information Week.

[10] Shadowserver foundation homepage, http://www.shadowserver.org.
[11] S. Gilani, "The Promise of M2M: How Pervasive Connected Machines are Fueling the Next Wireless Revolution", White Paper, Mentor Graphics, **(2009)**.
[12] J. Ferreira, R. Roque, C. Roadknight, J. Foley, P. Ytterstad and B. Thorstensen, "Sensor Telcos - New Business Opportunities", Technical Report, Eurescom, **(2006)**.
[13] M. Colajanni, D. Gozzi and M. Marchetti, "Collaborative Architecture for Malware Detection and Analysis", In Proceedings of The IFIP 23rd International Information Security, **(2008)**.
[14] M. Huff, "M2M Device Networking: Components & Strategies", Technical Report, MSI Tec, Inc., **(2007)**.
[15] D. Boswarthick and U. Mulligan, "M2M Activities in ETSI", SCS Conference – Sophia, **(2009)**.
[16] G. Wei, "Reliability Evaluation Method of Tactical Communication Network", Acta Electronica Sinica, vol. 1, **(2000)**.
[17] A. Bondi, "Characteristics of Scalability and Their Impact on Performance", Proceedings of the 2nd international workshop on Software and performance, **(2000)**, pp. 195-203.

Authors

Sungmo Jung, he received the B.S. degree in Department of Multimedia Engineering from Hannam University, Daejoen, Korea in 2008, and the M.S. degree in Department of Multimedia Engineering from Hannam University, Daejeon, Korea in 2010. Now, he completed in course of the Ph.D's degree in Multimedia Engineering from Hannam University. He is a member of IEEE and IEEE Communication Society. He has the international license CEH(Certified Ethical Hacker) for network penetration test. His research interests include Machine-to-Machine Architecture, Multimedia Communications, and Network Security.

Donghyun Kim, he received the B.S degree in Departmant of Multimedia Engineering from Hannam University, Daejeon, Korea in 2012, and currently, he is working on the M.S. degree in Department of Multimedia from Hannam University. His research interests include Image Processing, Augmented reality, and Network Security

Seoksoo Kim, he received a B.S. degree in Computer Engineering from Kyungnam University, Korea, 1989 and M.S. degree in Information Engineering from Sungkyun-kwan University, Korea, 1991 and Ph.D. degree in Information Engineering from Sungkyun-kwan University, Korea, 2002. In 2003, he joined the faculty of Hannam University, Korea, where he is currently a professor in the Department of Multimedia Engineering. His research interests include multimedia communication systems, distance learning, multimedia authoring, telemedicine, multimedia programming, computer networking, and information security. He is a member of KCA, KICS, KIMICS, KIPS, KMS, and DCS. He is editor-in-chief of IJMUE.