A Survey of Security Attacks in M2M Communication

[1.] Sunita Godara, [2.] Mr. Narendra Kumar
Department of Computer Science and Engineering,
JIET, Jodhpur (Raj.), India

Abstract:- It has been estimated that by the end of 2020 there will be 50 billion connected devices world-wide [10]. The number of interconnected machines will very soon exceed the overall population count. Therefore it is of vital importance to be able to understand M2M interactions. M2M is a new business concept originating from the telemetry technology, used for automatic transmission and measurement of data from remote sources by wire, radio or other means [10]. M2M offers various opportunities as well as unique challenges. These devices vary from highly-mobile vehicles communicating in real-time, to immobile meter-reading appliances that send small amounts of data sporadically.M2M devices would typically operate unmanned and unguarded by humans and thus are subject to increased levels of security threats, such as physical tampering, hacking, unauthorized monitoring, etc. Terminal devices may also get geographically dispersed over time. Such M2M devices should therefore provide adequate security to detect and resist attacks. Devices may also need to support remote management including firmware updates to correct faults or recover from malicious attacks. M2Mes are typically deployed in the field for many years, and after deployment, tend to require remote management of their functionality. It is likely that M2M devices will be deployed in very large quantities, and many of them will also be mobile, making it unrealistic or impossible for operators or subscribers to send personnel to manage or service them. These requirements introduce a number of unique security vulnerabilities for the M2M devices and the wireless communication networks over which they communicate.
In this paper main focus is on giving a short overview of M2M communication principles, basic architecture, various applications and its security attacks.

Keywords: M2M, MTC, Security threat, ETSI.

I. INTRODUCTION

Machine-to-machine(M2M)communications have emerged as a cutting edge technology for next-generation communications, and are undergoing rapid development and inspiring numerous applications[3].**Machine to machine (M2M)** refers to technologies that allow both wireless and wired systems to communicate with other devices of the same ability.M2M uses a *device* (such as a sensor or meter) to capture an *event* (such as temperature, inventory level, etc.), which is relayed through a *network* (wireless, wired or hybrid) to an *application* (software program), that translates the captured event into *meaningful information*.

1.1 Components of M2M

1.1.1 Collection of Data

- The M2M communication process begins with collecting data out of a machine so that it can be sent over a network. In an electronic device, we simply connect to the equipment's serial port and request for the data.
- The main aim of M2M hardware device is to introduce the intelligence in the machine with the communication network.
- M2M device is a wireless modem performing two functions of loading data and then give instructions for transmitting data to network.
- Wireless data module are physically integrated with the machine and programmed to understand the rules how to send and receive data.
- If we take example of application electric utility stations, in which it is necessary to send real time data of state of machine or various process taking place.

1.1.2 Transmission of data through a communication network

- If we want to transmit the data there are many options like telephone wires, cellular networks and satellites.
- Satellites are expensive but they are best solution for monitoring of equipment's in remote areas.
- Difficulty of Installation and cost are limitations for telephone lines.
- If we go for the third solution that is cellular networks in which M2M communication, GSM and GPRS are suitable method. Among these methods M2M is drawing attention now a day.
- For such type of M2M networks they require Gateways.
- Gateways collect the data from networks, convert and sent them over internet and perform security features like authentication and access control.

1.1.3 Assessment of the data

- Data can be collected from two places first from software application and second from some systems designed for M2M network.
- Assessment of data in M2M communication network can be defined as analyzing the data and integrating it with operational data.

1.1.4 Response to the available information The M2M technology enables sending the right data to the right place in the right way depending on the circumstances. They also present data to individual users based on their specific function in the business process.

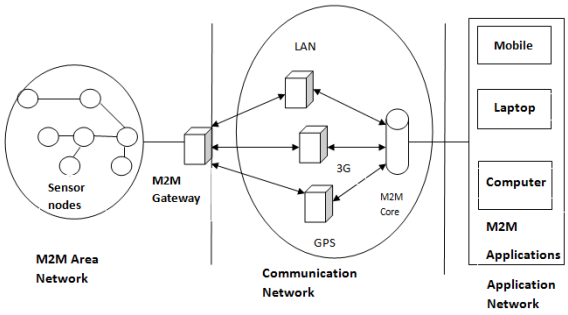
- The new element that M2M brings is that now companies have new data to work with, data that is central to the way they operate and the value they provide.

II. HOW M2M WORKS

Making a machine-to-machine communications system work is a step-by-step process. The main elements involved are sensors, a wireless network and a computer connected to the Internet.

2.1 Architecture of M2M

An M2M network as standardized by ETSI is composed of five key elements [3]:



•The M2M component usually embedded in a smart electrical device, replies to requests or transmits data.
•The M2M gateway enables connectivity between the M2M components and the communication network.
• The M2M server works as a middleware layer to pass data through various application services.
• The M2M area network provides connectivity between M2M components and M2M gateways.
• The M2M communication network provides connection between M2M gateways and M2M servers.
These five elements constitute the three domains of M2M system specified by ETSI [12]: the M2M component working in the device domain, the M2M area network and gateway in the network domain, and the M2M server and communication network in the application domain.

III APPLICATIONS OF M2M COMMUNICATIONS

The advances of wireless technologies enable mobility and eliminate the need of cable installation for M2M components have pushed the development of wireless M2M communications [11]. Machine-to-machine communications have so many applications. With better sensors, wireless networks and increased computing capability, M2M can be deployed for the following applications [10]:

3.1 Traffic control

It is a typical application of M2M system in which sensors monitor traffic volume and speed. The sensors send this information to computers using specialized software that controls traffic-control devices, like lights and variable informational signs. By using this concept traffic control devices are used for maximizing flow of traffic.

3.2 Utility companies

This is another M2M communications, in which we can control oil and gas consumptions and in billing customers. In the field, remote sensors can detect important parameters at an oil drill site. The sensors can send information wirelessly to a computer with specific details about pressure, flow rates and temperatures or even fuel levels in on-site equipment. The computer can automatically adjust on-site equipment to maximize efficiency.

3.3 Telemedicine

Telemedicine offers another use. For instance, some heart patients wear special monitors that gather information about the way their heart is working. The data is sent to implanted devices that deliver a shock to correct an errant rhythm.

3.4 Business

Business also can use M2M communications for tracking inventory and security. By using M2M communications we can track all the equipment working as well as their quantity and provide them some security features so that unauthorized persons cannot use them.

3.5 Security

Security includes different surveillance applications, alarms, object/human tracking, etc.

3.6 Transportation

This includes Fleet management, emission control, toll payment, road safety, etc.; remarkably interwoven with Intelligent Transport Systems (ITS) concepts.

3.7 e-Health

This includes remote patient monitoring, Mobile Health, telecare.

3.8 Manufacturing
This includes production chain monitoring and automation.

3.9 Industrial supply and provisioning
This application includes freight supply and distribution monitoring, vending machines, etc.

3.10 facility management
Facility management includes information and automation of various homes, building or any campus.

IV OPEN RESEARCH ISSUES

There are many technical challenges for M2M communications and following are important research issues [3]:

4.1 Standardization
Machine to machine communication is a new technique which includes both local and wide area network concept. There is very little standardization for M2M. So they require to be developed for applications, architecture and various enabling technologies of M2M communications for e.g., ZIGBEE, RFID, UWB, Wi-Fi and Bluetooth needs to be specified [1].

4.2 Traffic Characterization
Characteristics of traffic exchanged among M2M components have not been well studied so far. M2M traffic will be different from that of human-based network due to the special functions (e.g., data collection and monitoring) and requirements (e.g., hard real-time traffic). Traffic characterization is the fundamental to the design and optimization of network infrastructures. M2M traffic characterization is also required to provide quality of service (QoS) support for M2M applications.

4.3 Protocol Re-design
The transmission protocols of Internet like TCP/IP is not efficient for M2M traffic due to some reasons of energy wastage when we transmit less data. So new protocols specially designed for wireless M2M communication should be designed.

4.4 Spectrum Management
Spectrum management is an important design issue because there is limited bandwidth and wireless M2M technologies need to efficiently transmit signal over the frequency channels. Traditional spectrum allocation was static and it was not an optimal management technique as the demand and supply for wireless M2M network changes. Thus, for well-functioning of spectrum and its efficient use number of challenges are studied in detail.

4.5 Optimal Network Design
Optimal network design is an important issue in M2M communication as it consists of number of devices connected to various systems. The network design has to minimize cost of M2M communications including its hardware devices, maintenance, and use of radio resource while meeting QoS requirements of the traffic and applications.

4.6 Security
Security for M2M communication is an essential requirement in order to ensure that the whole system functions smoothly and safe from any sorts of attack and intrusion. This covers a wide range of solutions targeting threats such as denial-of-service, eavesdropping on transmission, routing attacks, flooding, and data center security and access control [4].

V M2M SECURITY

5.1 Threats

5.1.1 Physical attacks

Physical attacks include the insertion of valid authentication tokens into a manipulated device, inserting and/or booting with fraudulent or modified software (re-flashing), and environmental/side-channel attacks, both before and after in-field deployment

5.1.2 Compromise of credentials
They include brute force attacks on tokens and (weak) authentication algorithms, physical intrusion, or side-channel attacks, as well as malicious cloning of authentication tokens residing on the machine communication identity module (MCIM)

5.1.3 Configuration attacks
Configuration attacks such as fraudulent software update/configuration changes; misconfiguration by the owner, subscriber, or user; and misconfiguration or compromise of the access control lists.

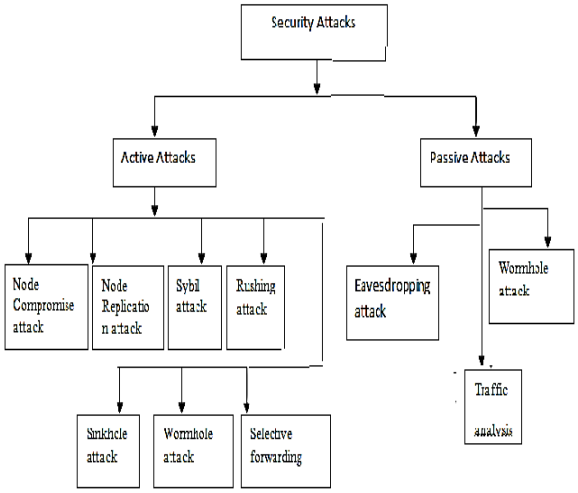
5.1.4 Protocol attacks
Protocol attacks are directed against the device, which include man-in-the-middle attacks upon first network access, denial-of-service (DOS) attacks, compromising a device by exploiting weaknesses of active network services, and attacks on over-the-air management (OAM) and its traffic.

5.1.5 Attacks on the core network
The main threats to the mobile network operator (MNO), include impersonation of devices; traffic tunneling between impersonated devices; misconfiguration of the firewall in the modem, router, or gateways; DOS attacks against the core network; also changing the device's authorized physical location in an unauthorized fashion or attacks on the network, using a rogue device

5.1.6 User data and identity privacy attacks
They include eavesdropping user's or device's data sent over the access network; masquerading as another

user/subscriber's device; revealing user's network ID or other confidential data to unauthorized parties.

5.2 General Classification of Security attacks



Different security attacks are classified[8] as shown in figure. In an *external attack*, the attacking node does not belong to a community of authorized nodes in a network. It does not have key materials for communication inside the network. By compromising the node the attacker can perform internal attacks. In an *internal attack* the attacker possesses a node with key materials. Internal attacks cause more serious damage to M2M networks than external attacks. Internal attacks are harder to detect and prevent in comparison to external attacks.

In *passive attacks* the adversary monitors the traffic between two or more communicating nodes to collect and discover valuable information. This is an easy task, since wireless communication is open radio transmission. This kind of attack does not disrupt a M2M communication. In contrast, an *active attack* attempts to deliberately modify communication in M2M network. Security holes in the network are exploited to launch various attacks like packet modification, injection, or replaying. Passive attacks are very difficult to detect and prevent, but they cause less damage. Active attacks are, on the other hand, easier to detect, but damage is far bigger. Passive attacks usually lead to active attacks.

5.2.1 Eavesdropping attacks

Wireless communication broadcasts all data to be communicated into surrounding aerial space. Anyone with a good receiver can eavesdrop and intercept transmitted messages. The attacker could extract information like location of node, message IDs, node IDs, timestamps, application specific information and others. This is the most common attack to privacy. By snooping to the data, the attacker could easily track the communication contents. When the traffic conveys the control information about the sensor network configuration, which contains potentially more detailed information than accessible through the location server, the eavesdropping can act effectively against the privacy protection [8].

5.2.2 Node Compromise attacks

In this type of attack the attacker can control physically over one or more nodes of the network. In other words the attacker is capturing the node's private key, stealing the node's identity, and can send messages signed on behalf of that node. When node's keying material is extracted, attacker has everything needed to enter the network and perform internal attacks. The term compromised node designates such a trusted node that has been taken over by the attacker. Compromised nodes can be used to monitor and analyze network traffic with aim to prepare more destructive attacks.

5.2.3 Node Replication attacks

Node Replication attack is basically application independent and mostly found in wireless sensor networks. In this type of attack the attacker makes his own sensor nodes by doing replication of real nodes, he collects all secret information's of nodes like key and identity and place these nodes as real nodes in the network. This type of attack affects routing, resource allocation, misbehavior detection and data aggregation mechanisms by injecting false data. Node replication attacks are similar to Sybil attack.

5.2.4 Selective Forwarding attacks

In M2M network there are a number of nodes and the task of each node is to forward packets. Selective forwarding attacks are type of black hole attacks, in which the malicious node forwards only the selected packets and discard others [13]. This type of attacks decreases network efficiency.

5.2.5 Sybil attacks

Sybil attack is a harmful attack in which a malicious node illegitimately acquires multiple identities and consequently presents itself as a group of nodes. This node is called a Sybil node. This type of nodes pretends to be other nodes or they claim for false identities. Sybil attack can severely impact many mechanisms and protocols in M2M network like routing protocols, data aggregation, distributed storage and misbehavior detection.

5.2.6 Rushing attacks

Rushing attacks are directed against on-demand routing protocols and the attacker hurries route request packet to the next node to increase the probability of being included in a route. Rushing attack, which results in denial-of-service when used against all previously published on-demand ad hoc network routing protocols. Specifically, the rushing attack prevents previously published secure on-demand routing protocols to find routes longer than two-hops (one intermediate node between the initiator and target).

5.2.7 Sinkhole attacks

Sinkhole attack is one of the severe attacks in M2M network. Attracting traffic to a specific node is called sinkhole attack. In this attack, the adversary's goal is to attract nearly all the traffic from a particular area through a malicious node. Sinkhole attacks typically work by making a malicious node attractive to surrounding nodes.

5.2.8 Wormhole attacks

The wormhole attack is a severe threat against packet routing in sensor networks that is particularly challenging to detect and prevent. In this attack, an adversary receives packets at one location in the network and tunnels them to another location in the network, where the packets are resent into the network. An instance of a wormhole attack would involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. Thus a false route would be established which would shorten the hop distance between any two non-malicious nodes.

CONCLUSIONS AND FUTURE WORK

Conclusion: M2M communication is described exclusively in detail. The architecture, the application areas, research issues and possible security attacks are also described. It is observed that M2M communication is emerged as a cutting edge technology for next-generation communications, and are undergoing rapid development and inspiring numerous applications. Also, the amount of work done on M2M communication and its security issues is very limited and specific.

The previous techniques for security in M2M were expensive and non-scalable. M2M communication applications and scenarios are growing and lead the way to new use and business cases. Due to the nature of M2M scenarios, which involve un-guarded, distributed devices, new security threats have emerged. Therefore, efficient and practical security algorithms are required.

Future work: In this paper a survey of various security attacks in M2M communication is discussed along with the architecture and basic principles of M2M. In future research work can be done for finding the solutions for various types of security attacks so that M2M communication is not affected.

REFERENCES

[1] Y.Zhang, R. Yu, S. Xie, Y. Xiao, and M. Guizani, "**Home M2M Networks: Architectures, Standards, and QoS Improvement,**" IEEE Communications Magazine, vol. 49, no. 4, pp. 44-52, 2011.

[2] D.Niyato, L. Xiao, and P. Wang, "**Machine-to-machine communications for home energy management system in smart grid,**" IEEE Communications Magazine, vol. 49, no. 4, pp. 53–59, 2011.

[3] Chen Hongsong," **Security and Trust research for M2M Communications,**" Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference , pp. 286 - 290,10-12 July 2011.

[4] R. X. Lu, X. Li, X. H. Liang, *et al*. "**GRS: The green, reliability, and security of emerging machine to machine communications,**" IEEE Communications Magazine, vol.49, no.4, pp.28-35, Apr.2011.

[5] C. Inhyok, Y. Shah, A. U. Schmidt, et al., "Security and trust for M2M Communications," Vehicular Technology Magazine, IEEE, vol. 4, no. 3, pp. 69-75, Sep. 2009.

[6] M. Dohler, T. Watteyne and J. Alonso-Zárate, "**Machine-to-machine: an emerging communication paradigm,**" *Presentation Report*, Dec.2010.

[7] Dr. G. Padmavathi and Mrs. D. Shanmugapriya," **A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks**", (IJCSIS) International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, 2009.

[8] Dong Chen; Guiran Chang "A Survey on Security Issues of M2M Communications in Cyber-Physical Systems," KSII Transactions on Internet & Information Systems; Vol. 6 Issue 1, p24, January 2012.

[9] V.Galetic,"**Basic Principles of Machine to Machine communication and its impact on telecommunication industry,**" IEEE Communications Magazine, pp.380-385, May 2011.

[10] Ritesh Maheshwari, Jie Gao, Samir R Das, "**Detecting Wormhole Attacks in Wireless Networks using Connectivity Information**", IEEE INFOCOM 2007, Alaska.

[11] Zubair Md. Fadlullah, Mostafa M. Fouda, "**Towards Intelligent Machine-to-Machine Communications in Smart Grid**," IEEE Communications Magazine, vol.49, no.4, pp.60-65, April 2011.

[12] ETSITS 182 690: M2M **Functional Architecture**

[13] Leela Krishna Bysan and Ashok Kumar Turuk, "**A Survey on Selective Forwarding Attack in Wireless Sensor Networks**," ICDeCom, 24-25 feb 2011.