ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

A Survey Using Security and Privacy in Machine-to-Machine Communications

J.Pavithra
Department of Computer Science and Application
D.K.M College for Women(Autonomous)
Vellore,Tamilnadu,India
pavithrajmani@gmail.com

B.Arulmozhi
Head of the Department,
Department of Computer Science and Application
D.K.M College for Women(Autonomous)
Vellore,Tamilnadu,India
arulsenthil2014@gmail.com

***Abstract*—Machine-to-Machine Communication is one of the most attractive technology used in both industrial and education sectors and that is predicted to grow within the next few years. It refers to direct communication between devices using any communication channels. It provides a way of communication between connected devices. Very important obstacles which will cut down Communication growth and even hold back the large roll-out of sure applications are security and privacy. The limitations in the architecture of communication networks make the system extremely vulnerable to malicious attacks. In this paper, we discuss the related solutions to design a cost effective security scheme to support large number of devices. Machine to machine wireless network can serve to improve the production and efficiency of machine, to enhance the reliability.**

Keywords*— *machine-to-machine architecture; security; privacy

I. INTRODUCTION

Machine-to-Machine (M2M) communications, additionally referred to as MTC for Machine-Type-Communication by the Third Generation Partnership Project (3GPP) visit communications between little and cheap devices wherever no or very little human intervention is needed. During the communications between these devices, the watching of some events and also the remote directions of sure actions is hence forward doable. The monitored events are relayed through wireless or wired links towards a server or a superintendence station so as to be processed and in step with the results, some actions is also performed. Thereby, M2M covers many applications from health applications, wherever sensors monitor important signs and transmit them to a tending skilled, to police work solutions exploitation police work cameras to stay a watchful eye on the users pet, home or workplace so forth.

II. M2M COMMUNICATION DESIGN

The M2M design will be divided into three interlinked domains namely, device domain ,network domain and application domain. The following figure illustrates the architecture of M2M networks.

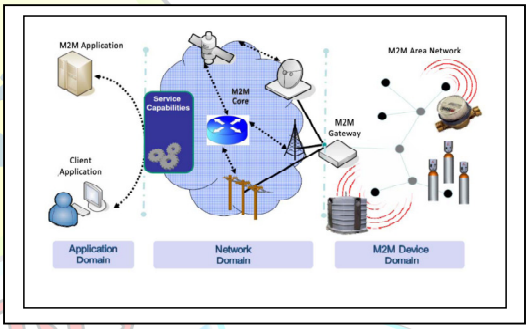

Fig 1: M2M Architecture

Device domain: It consists of the set of devices concerned in running M2M applications. A number of these devices are equipped with specific sensing technology because it is that the case with body sensors whereas different devices simply record current values. Once the mandatory knowledge is gathered, the M2M device forwards it through the network domain to the remote server. Note that this domain is additionally brought up as M2M domain.

Network domain: It consists of a group of heterogeneous access networks sanctioning the device domain and also the application domain to exchange information.

Application domain: It includes the servers wherever knowledge collected by the M2M devices or different network nodes is hold on. These time period knowledge is created out there to legitimate users through a range of M2M applications sanctioning remote watching and forwarding of the M2M devices and also the network is either direct or through a entrance exploitation the M2M space network. In fact, the M2M space network provides property between the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

M2M entrance and also the M2M devices. It's typically supported short vary wireless technologies like ZigBee, Bluetooth Low Energy (BLE) and Ultra-wide band (UWB). In respect of direct communication, the M2M device is supplied with a communication module sanctioning it to access the network via mobile or fastened line and perform authentication, registration and management procedures by itself.

In general, the architecture of M2M communication networks can be divided into three domains, i.e., device domain, network domain, and application domain. There are some limitations in both device and network domains, which make M2M communications vulnerable. First, communication media is wireless radio channels, which are easy to be eavesdropped. Second, Most M2M devices are power and cost limited, which makes it impossible to use sophisticated security schemes. Many attacks can pose serious threats to M2M devices. Third, interworking of wireless and wired communication networks leads to a need for translation of security protocols between different networks, which are a potential weakness for M2M communication security. The above three points make M2M communications extremely vulnerable to malicious attacks. [5] proposed a system in which FASTRA downloads and data transfers can be carried over a high speed internet network. On enhancement of the algorithm, the new algorithm holds the key for many new frontiers to be explored in case of congestion control. The congestion control algorithm is currently running on Linux platform. The Windows platform is the widely used one. By proper Simulation applications, in Windows we can implement the same congestion control algorithm for Windows platform also. The Torrents application which we are currently using can achieve speeds similar to or better than —Rapid share (premium user) application.

III. SECURITY PROBLEMS

As they consider the fusion of heterogeneous networks, M2M communications need to address all the safety threats of different network-based communications. even supposing M2M haven't elicited new threats, they need amplified the present ones as, within the case of M2M, these threats cause not solely money losses however additionally cause a threat to human lives. Like Wireless Sensor Networks (WSNs), M2M devices are typically deployed in approachable locations and expected to work for extended periods. Therefore, many physical attacks will pose against the devices. The following are the two categories of attacks.

A. *Physical attacks:*

Targeting the physical layer also M2M devices hardware and software.

1) Co-channel attacks: Devices are typically settled in approachable locations wherever adversaries will simply access them and perform co- channel attacks. These attacks can be supported either power consumption, temporal order information, fault or magnetic force leaks and change the retrieval of the used secret keys. For instance, associate antagonist could conduct a aspect channel attack on any of the users devices so as to retrieve the key accustomed write in code changed info. Therefore, he would be ready to decode all the changed knowledge.

2) *Program modification associated intrusions*: Program modifications will be performed by an antagonist, or perhaps a malicious user, to change the right operations of the M2M device. Malicious users could hump so as to cut back the number of the costs that they need to pay.

B. *Logical attacks:*

Targeting the right functioning of the system while not creating any changes to the device's data.

1) Impersonation: Once addressing M2M communications, associate wrongdoer could spoof the identity of a back-end server, an M2M device or entrance so forth. These attacks could cause vital money and human losses. For instance, associate antagonist United Nations agency succeeds in spoofing a sensible meter identity will create its owner get hold of the adversary's charges. it's even worse if he impersonates the server as he would be ready to send remote to the corresponding M2M devices. Within the case of the health applications, such attack could cause a threat to human lives.

2. Denial of Service (DoS): Since most M2M devices are battery steam-powered, the constant broadcast of vacuous packets can untimely drain the device battery inflicting the applying failure. Such attacks are also conducted, for example, once addressing surveillance application so as to stop it from notifying the user of associate intrusion detection.

C. *Data attacks:*

*T*argets the information exchanged between devices.

1) Attack on Privacy: Attributable to the generality of M2M devices, through the dropping of changed packets, malicious parties will invade user's privacy and link M2M devices or the transiting info to people and thereby inferring users' habits, health condition so forth. Indeed, if the device's Media Access management (MAC) address is static and indicates that it's a heart monitor, for instance, then the antagonist can grasp that its owner suffers from heart issues.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

2) Attack on Integrity: Knowledge will be compromised throughout its transmission also as at rest on a tool or an application's server. The modification of measured values or localization information will endanger people's lives. On the opposite hand, in some applications, false knowledge injection could cause money losses.

Selective forwarding/ Interception: Associate antagonist could intercept and delay or drop a number of the received packets. Note that the impact of such a threat depends on the content of the born packets. Indeed, if the born info originates from a sensitive application. Generally, such attacks are conducted against the underlying infrastructure.

IV. M2M SECURITYSOLUTIONS

To prevent the threats to that M2M communications is also subject, a group of security services ought to be secured. Among these services, we have a tendency to note authentication that doesn't solely aim to make sure that knowledge extremely originates from a given entity however additionally avoids impersonation, confidentiality preventing changed packets from being scan by eavesdroppers, integrity keeping devices and sent packets from being altered preserve user's privacy.

1) We classify the connected solutions into three classes as described below:

Authentication: Asymmetric and symmetric keys are two basic methods to authenticate M2M communications. Both the techniques are used to accommodate a variety of deployment situations. Unfortunately, asymmetric key cryptosystems are not economic for M2M communications, and symmetric key cryptosystems have a limitation in key distribution and number of keys. In order to design a cost effective system multiple solutions were proposed. In asymmetric key cryptosystem, the burden of required computations in M2M devices can be moved to gateways, which will reduce energy consumption in M2M devices and increase the speed of computation in M2M devices. However, this method is useful only when gateways are trustful and communication links between M2M devices and gateways are secure. Another way to solve this predicament is to design a cost-saving asymmetric key cryptosystem. Proposed a hardware-based public-key cryptosystem. Another way to provide authentication is using dynamic authentication scheme. In this approach, a dynamic encryption algorithm is used between M2M device and service provider. Each time a M2M device wants to communicate with other device, it needs to be authenticated by the service provider to set up a session.

2) *Encryption*: Data encryption is used to achieve confidentiality. This we can achieve by using either symmetric key or asymmetric key cryptography techniques. Both the techniques having its own limitations in implementation point of view. In a symmetric key cryptography, a shared key will be used to protect the data transmitted between M2M devices. First, a shared secret key have to be exchanged among the M2M devices in a network and then initiates the communication. For exchanging shared secret key we can use any key exchange mechanism described by key distribution scenario. Second approach is using asymmetric key cryptosystems. In this, each M2M device can use publicly available key of other M2M device to encode the information. Due to the computation constraints in M2M devices we have to prefer lightweight cryptography techniques in M2M communications. Sometimes we can go for hardware-assisted cryptography algorithms. There is an advantage with the use of public key cryptography instead of secret key cryptography in a M2M networks. It is sometimes sufficient to implement a lightweight encryption system without decryption process. Decryption may be done by the gateways. Another method for protecting data in M2M communication is using elliptic curve cryptography. It also offers same security level. Hardware based implementation of asymmetric key cryptography requires less computation burden and minimum memory capacity. It avoids the existing drawback with M2M devices like sensors.

3) Privacy: Personal information should not be disclosed. Otherwise can be the cause of huge loss in personal or cooperate assets. In M2M it is essential to fulfill the requirement of privacy due to the presence of smart objects, threat of technology mishandling. Huge number of smart entities makes it a big challenging issue to maintain privacy of personal information. One method is to establish a third party trusted security organization, which is the only one responsible for authentication information distribution. However, if there are a large number of M2M devices with dissimilar applications, this method seems to be too costly to be practical.

V. CONCLUSION

In this paper, we briefly introduced the sensitivity of the data exchanged between M2M devices and the possible attacks which are more harmful. We also discussed the limitations in M2M devices and proposed security mechanisms. For the security and privacy of M2M communications, the main issue is to develop a cost-effective security enhanced for large number of devices. In order to reduce system implementation cost, a simple cryptosystem

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 4, February 2018

and security protocol can be used. Finally a less focus on privacy was discussed.

REFERENCE

[1] Ericsson, "More than 50 billion connected devices," in 284, 23-3149, Uen, February 2011.

[2] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home m2m networks: Architectures, standards, and qos improvement," Communications Maga-zine, IEEE, vol. 49, pp. 44–52, April 2011.

[3] R. Ma, H.-H. Chen, Y.-R. Huang, and W. Meng, "Smart grid communication: Its challenges and opportunities," Smart Grid, IEEE Transactions on, vol. 4, pp. 36–46, March 2013.

[4] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," Security Privacy, IEEE, vol. 7, pp. 75–77, May 2009.

[5] Christo Ananth, A. Ramalakshmi, S. Velammal,B. Rajalakshmi Chmizh, M. Esakki Deepana, "FASTRA –SAFE AND SECURE", International Journal For Technological Research In Engineering (IJTRE), Volume 1, Issue 12, August-2014,pp: 1433-1438

[6] Shuyi Chen, Ruofei Ma, Hsiao-Hwa Chen, Hong Zhang, Weixiao Meng, Jiamin Liu, Machine-to- Machine Communications in Ultra-Dense Networks – A Survey", in IEEE Communications Surveys & Tutorials, 2017

[7] X. Duan and X. Wang, "Authentication Handover and Privacy Pro-tection in 5G Hetnets Using Software- Defined Networking," IEEE Communications Magazine, vol. 53, no. 4, pp. 28-35, Apr. 2015.

[8] oneM2M Technical Specification:Security Solutions," TS-0003- v1.4.2, oneM2M, Feb. 2016, Available:

[9] D. Adrianto, and F. J. Lin, "Analysis of Security Protocols and Corresponding Cipher Suites in ETSI M2M Standards," 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp. 777-782, 2015.

[10] J. R. Shih, Y. Hu, M. C. Hsiao, M. S. Chen, W. C. Shen, B. Y. Yang, A. Y. Wu, and C. M. Cheng, "Securing M2M With Post-Quantum Public-Key Cryptography," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, pp. 106-116, Mar. 2013.

[11] Chengzhe Lai, Rongxing Lu, Dong Zheng, Hui Li, and Xuemin Shen, "Toward Secure Large-scale Machine-to-machine Communications in 3GPP Networks: Challenges and Solutions," IEEE Communications Magazine, vol. 3, no. 12, pp. 12- 19, Dec. 2015.

[12] H. Shariatmadari, R. Ratasuk, S.Iraji, A. Laya, T. Taleb, R. Jantti, and A. Ghosh, "Machine-type Communications: Current Status and Future Perspectives toward 5G Systems," IEEE Communications Magazine, vol. 53, no. 9, pp. 10- 17, Sep. 2015.

[13] 26. M. Chen, J. Wan, S. Gonzalez, X. Liao, and V. Leung, "A Survey of Recent Developments in Home M2M Networks," IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 98-114, First 2014.

[14] 143. S. Chen and M. Ma, "A Dynamic-Encryption Authentication Scheme for M2M Security in Cyber Physical Systems," 2013 IEEE Global Communications Conference (GLOBECOM), pp. 2897-2901, Dec. 2013.

[15] J. R. Shih, Y. Hu, M. C. Hsiao, M. S. Chen, W. C. Shen, B. Y. Yang, A. Y. Wu, and C. M. Cheng, "Securing M2M With Post-Quantum Public-Key Cryptography," IEEE Journal on Emerging and Selected Topics in Circuits and Systems, vol. 3, no. 1, pp. 106-116, Mar. 2013.

[16] J. Kim, J. Lee, J. Kim, and J. Yun, "M2M Service Platforms: Survey, Issues, and Enabling Technologies," IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 61-76, First 2014.