Group-Based Authentication Schemes used for Machine Type Communication Devices in WSN: A Review

Ullah. S[1], Raja Zahilah[2], Marina Md Arshad[3], Abdul Hanan Abdullah[4] and Rashidah Kadir[5]
[1-5]School of Computing, Universiti Teknologi Malaysia, Johor Bahru, Malaysia.

E-mail: [1]ullah.shafi@graduate.utm.my, [2,3,4,5]{zahilah, marinama, hanan, rashidah}@utm.my

Abstract.M2M communication is the next vital part of IoT infrastructure. It is extremely important for IoT systems to prosper in machine-type communication (MTC) devices that have low computational power, limited energy and small amount of memory capabilities. Thousands of devices transmitting data while working remotely and independent of any external supervision, creates concern for the security of data and devices as the topology is totally different to that of personal computers. In relation to the security of the devices, authentication is the first important part that has to be addressed against all possible security threats in IoT communication. In this regard, we focus on different types of authentication techniques being carried out by the researchers in M2M communicating environment of several remotely operating devices and address their security threats.

Keywords: Authentication and Key Agreeing (AKA), Message Access Code (MAC), Machine to Machine Communication (M2M), Machine Type Communication (MTC), Man in The Middle (MiTM)

1. Introduction

In the world of automation, machines known as IoT devices and machine-type communication (MTC) devices need to communicate over the internet. It is estimated that by 2020, over 50 billion of these devices will be used in our daily life from a smart refrigerator, smart TV and smart air-condition controllers to smart health devices, smart offices and smart parking system. These machines are working continuously without any break to make our lives better and comforting. They share and provide information with each other and with humans via the internet and make decisions based on the information created via some logical pre-programmed tasks. Some examples of such tasks are sensing air quality of our homes and cities and storing the data, controlling the temperature of the ventilation system, preoccupying parking space in a shopping mall before we even arrive and making data related to our environment in order to arrive at a better decision in the future.

The type of information being shared could be very common but, in some cases, could be very sensitive. For example, a device could share temperature data of a grid power station to fans in order to maintain temperature. Similarly, a device could send patient's heartbeat data to a doctor who is monitoring irregular heartbeats for heart patient or grant access to authorized personnel who have been given access cards in a highly secretive military facility and many more such cases. In the mentioned

cases, the data shared between devices is very sensitive. These devices are given software-based security only due to the low computational power and memory since standard security protocols cannot be applied. Trusting every device to ensure security is achieved via authentication. Every device in the network must authenticate itself so that the data being shared can be marked as trusted data. Group-based authentication is used for large number of devices working in applications based on parallel computing tasks. Certain numbers of devices form a group using local techniques for authentication, making a cluster of a single group. These groups authenticate other groups and share data. Such authentication process mainly takes place in LTE/CDMA based network infrastructures. An important part of authentication is mutual authentication where the sending and receiving devices must mutually authenticate themselves before initiating communication. Our study is based on group-based authentication schemes and making comparison of these schemes in the context of providing security and privacy to MTC devices. The generic four-layer architecture of IoT in MTC devices is shown in Table 1.

Table 1. Generic four-layer architecture of IoT

Layers	***Name***	***Function***	***Devices/Applications***
Layer 4 (Yan-rong and Tao 2013).	Application Layer	• Representation of collected and processed data into a predefined graphical interface. • to automate and make smart decisions by the device • smart business applications	• Smart home automation system • Smart healthcare system, • Smart industry
Layer 3 (Khan, Khan et al. 2012).	Middle-ware Layer	• Information processing functions • Automate flow of tasks based on received information from perceptual or network layer. • Inclusion of database related actions for storage purposes.	• Software based • Built in circuitry
Layer 2 (Yang, Li et al. 2012).	Network Layer	• Data being generated from sensors is converted into packet to suit standard protocols. • Forwarding data packets to 3G, LTE structured packets and wire medium.	• Using standard communication equipment • Software based • Built in circuitry
Layer 1 (Zhang 2011)	Perception layer	• Data generation layer, Sensing environmental data from sensors and actuators and converting to digital information • These sensors collect data and send it to MTC devices which is further processed for transmission	• Temperature, pressure, humidity and heartbeat sensors • RFID, barcode readers • ZigBee, Bluetooth, NFC

2. Security Threats in Perceptual Layer of MTC Devices

MTC devices work remotely, sometimes in harsh environments with limited computational power, memory, and battery life, making these devices an easy target for attackers. Most commonly known physical security risks are as follows:

2.1. Trojan as Hardware

Trojan hardware is an integrated circuitry fabricated by the attacker that aims to manipulate the data being shared. Patching fabricated integrated circuit on a physical device exploits its functionality [5].

2.2. Non-Network Side Channel Risk

In WSN, MTC devices are connected through a wireless medium. These signals create specific types of electromagnetic signatures known as electromagnetic waves, being transmitted and received by MTC devices that carry crucial data, as demonstrated by [7].

2.3. DoS Attacks

MTC devices are often affected by these common but lethal attacks. HIGH (active) status of related sensing data are being sent to IoTs, CPs and MTC devices just to keep device busy.

2.4. Physical Attack

MTC devices are exceedingly defenseless against physical attacks due to the nature of the business applications of these devices where they are usually working at remote places or in areas where human invention is undesired and difficult. Attacker with easy physical access may extricate crucial cryptographic data, infiltrate internal circuitry and modify instructions [8].

2.5. Node Capture/Node Replication

Attacker replicate captured node and turning it into malicious node. Malicious node is introduced into the network by imitating genuine devices' ID or pre-shared keys. The attacker will be able to redirect packets to the desired network [10].

2.6. DisguisedNode

The attacker embeds a fake edge node or attacks an approved device in request to cover up at the edge level. A while later, the changed/fake device can work as a typical node to acquire, process, send, or divert packets [12].

2.7. Eavesdropping/MiTM

Eavesdropping is one of the most lethal attacks in IoT world, where data transmitted over physical line of communication is monitored by another unauthorized device. Both transmitting and receiving devices have no clue if the data is being monitored, also known as Man in the Middle (MiTM) attack. The monitored data is then decoded for malicious purposes [14].

2.8. Spoofing

Data is briefly monitored over a brief period of time. Enough data packets is captured to be decrypted or interpreted, made sense of the data and then merge malicious data packets to demonstrate the nature of genuine data [14].

3. Security Features in Perception Layer

The challenges of perception layer security can be separated into two categories: security challenges and technological challenges. The technological category mainly focuses on challenges due to the dynamic topologies of MTC devices and ubiquitous behavior of IoT and M2M communication devices. It includes areas such as energy, power, distributed features and risks. Whereas, challenges related to security primarily aims to address solutions and weaknesses in end-to-end security, data integrity, data confidentiality, scalability and to ensure authentication between these devices [17]. Our studies extend the area of security challenges in authentication in terms of achieving data integrity, data confidentiality and data availability in group-based authentication.

Table 2. Basic security features in perception layer

Data Integrity	Data Availability	Data Confidentiality	Authentication
• Accuracy of data being shared between devices • Data is susceptible to errors in heterogamous devices. • Errors could be human errors, machine errors or infused attacks. • Data is trusted, accurate and clean from intended or unintended interference. • Made possible by imposing end-to-end cryptography.	• Serve users/devices with constant flow of data whenever data is required. • Operate all the time under any circumstances with minimal cost. • Emphasize on the availability of data in harsh environments, even during the time of failure. • Mainly applies to systems dealing with risk monitoring and assessments.	• Privacy of data being shared and protected could be very sensitive. • Mainly depend on the type of business application. • Data is not only kept secret from other user but from other devices as well. • Maintained by combining features of authentication and integrity.	• Key feature of security in MTC network • Vital for data from sending device to be trusted. • Each device is given a secret key which is sent to other device for processing. • Device allows the data to be shared after the process of decoding keys (encrypted/used in hash functions)

4. Group-Based Authentication

Generally, group-based authentication is used when a large number of MTC devices communicate simultaneously. In contrast, individual device authentication adds network overheads that are not cost-efficient, especially in an area where coverage is extremely large. Group-based authentication proves to be an effective counterpart against network overheads [18]. Authentication takes place with Authentication Key Agreeing (AKA) techniques. MTC devices are introduced in LTE-A networks, adopting 4G heterogeneous network pertaining to low latency and high capacity in terms of resources. LTE and LTE-A networks tend to have predefined authentication mechanisms between communicating entities for MTC architecture which was introduced by 3GPP committee [19]. The network consists of a Mobile Management Entity (MME) and Home Subscriber Server (HSS) communication entities. It further includes MTC users and servers [20].

4.1. Related Work in GBA

GBA based key agreeing protocols have been introduced in LTE and LTE-A based 3GPP network architecture. These protocols are addressed in AKA in terms of improved security and network overhead. AKAs techniques use symmetric, asymmetric and hybrid key cryptosystems. At first, Jung et al. [21] proposed congestion avoidance to avoid signaling congestion problems in M2M networks. A group leader device, selected within a local group, was responsible for the transmission of data to-and-from other devices. An extension of their work, Chen et al. [22] using the same grouping method, proposed G-AKA protocol in which, the first device was authenticated by HSS, which farther authorized the MME entity. Nevertheless, these protocols generated high signaling overheads when many devices demanded network access simultaneously. G-AKA technique was vulnerable to MiTM and DoS attacks, thus data integrity and confidentiality were not guaranteed. Lai et al. in [2] proposed asymmetric cryptosystem-based key agreeing protocol (SE-AKA). The asymmetric approach was a novel way of encrypting key but proved less effective against signaling congestion. Jiang et al. [3] proposed EG-AKA that aimed to authenticate local group of MTC devices in non-3GPP networks. But the protocol tended to be vulnerable against MiTM, DoS, re-directional attacks and has high computation overload due to its operations in asymmetric cryptosystem. Meanwhile, NOVEL-AKA utilized symmetric key-based cryptosystem. The protocol first used MTC device, which is fully authenticated with HSS. This device would farther authenticate the remaining MTC devices where HSS calculated GTK (Group Temporary Key) and authenticate data including index table, which later is forwarded to MME. Remaining MTC devices within the local group were validated by MME despite the fact that HSS is a crucial entity to be authenticated. This protocol too suffered security attacks. To mitigate signaling congestion, Choi et al. [1] endorsed GROUP-AKA protocol where a group of MTC devices was successfully authenticated without producing large signaling congestion. Devices could easily join and leave the group but lacked in device privacy preservation made them vulnerable to identity theft attacks during the new arrival of MTC device in the group. To address these problems, Cao et al. [6] proposed GBAAM-AKA, a group signature-based protocol. In GBAAM-AKA, each group was assigned a specific signature. Then, the aggregated signature was computed by a group leader which was then sent to MME. MME verified the signature and crosschecked against each corresponding MTC device. However, GBAAM-AKA also suffs with computational overheads which were further improved by Fu et al. [11] by introducing PRIVACY-AKA protocol that used pseudo-identity through elliptic curve cryptography. In this protocol, MME gets authenticated via HSS, compiles group vectors and validates devices within the group. The protocol successfully countered basic security risk except key secrecy but produced high network overheads due to it being an asymmetric key cryptosystem. Lai et al. [9] proposed another group based authentication known as GLARM-AKA. The technique is light-weight thus producing fewer network overheads, suitable for resource-constrained MTC devices. During the time where new devices joining and current devices leaving the system, this protocol unfortunately offered open paths for nodes to be captured and to DoS attacks. Li et al. [13] improved unlink-ability problem in GLRAM-AKA by introducing GR-AKA. GR-AKA endured the dynamic policy of LTE-A network. It encountered impersonation attacks using privacy preservation technique. MAC was generated by Lagrange Component (LC) which tends to timely update group keys and avoided basic security attacks. However, updating group keys in timely manner and encountering impersonation attacks resulted in high bandwidth consumption due to the strong cryptography technique. Group based secure authenticating protocol GBS-AKA was proposed by Yao et al. [15] to address issues in GR-AKA by improving overheads and bandwidth consumption but failed to incorporate privacy preservation. According to B.L.Parne et al [16], groupauthentication protocols' security mainly depends on the confidentiality of shared/pre-shared symmetric/asymmetric key cryptosystem through transmission channels and devices. If the key is captured by attacker at any point, then all keys in the whole system could be at risk. In this regard, B.L.Parne et al. introduced SEGB-AKA protocol which is based on

public key but under symmetric cryptography. The system is mainly dependent on NSP that is responsible for main computational tasks including the generation of keys and authentication. A group leader is chosen by variables such as power, battery life and binary tree. These values are updated continuously in order to choose the best group leader. However, it couldn't provide low computational cost because of the use of public keys.

Table 3: Comparison of GBA Techniques

Protocols	***Basic Security Features***				***Achievements***	***Threat Vulnerabilities***					***Performance weaknesses***
	S1	**S2**	**S3**	**S4**		**T1**	**T2**	**T3**	**T4**	**T5**	
G-AKA by [1]	N	N	Y	N	Entity-Based Mutual Authentication	Y	Y	Y	Y	Y	High Computational Overhead
SE-AKA [2]	N	Y	Y	Y	A-Symmetric Cryptosystem	Y	Y	N	N	Y	Network Signaling Congestion
EG-AKA [3]	Y	Y	Y	N	Non-3GPP Network Authentication	Y	N	Y	Y	Y	High Computation Overload at Network
NOVEL AKA [4]	N	Y	Y	Y	Entity-Based Mutual Authentication	Y	N	N	N	Y	DoS Infused Re-directional Attacks
GBAAM-AKA [6]	N	N	Y	N	Signature Based Authentication	N	N	N	Y	Y	High Computational Overheads
GROUP-AKA [1]	Y	N	Y	N	Improved Unlink-Ability	N	Y	N	Y	Y	Weak Key Forward Secrecy
GLARM-AKA [9]	Y	Y	Y	N	Group Base Lightweight Cryptography	N	N	Y	Y	Y	Weak Unlink-Ability (Both KFS/KBS)
Privacy-AKA [11]	N	Y	Y	Y	Pseudo Identity Via ECC Based Mutual Authentication	N	N	Y	Y	N	Weak Key Forward Secrecy
GR-AKA [13]	Y	Y	Y	Y	Flexible Policy by Lagrange Component (LC)	N	N	N	Y	N	High Bandwidth Consumption
GBS-AKA [1,15]	Y	N	Y	N	Secure Entity-Based Mutual Authentication	Y	N	N	Y	Y	Weak Unlink-Ability (Both KFS/KBS)
SEGB-AKA [16]	N	Y	Y	Y	Public Key Based Mutual Entity Authentication	N	N	Y	Y	Y	Weak Unlink-Ability (Both KFS/KBS)

[Y].YES. [N].NO [S1]. Integrity, [S2]. Confidentiality, [S3]. Authentication, [S4]. Privacy Preservation, [T1]. MiTM, [T2]. DoS attacks, [T3]. Impersonation attack, [T4]. Node-Replication Threat, [T5]. Spoofing

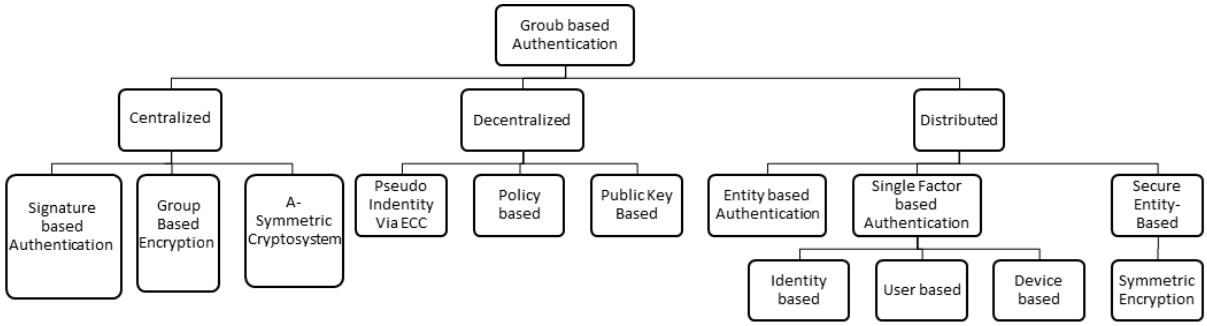

Figure 1. Taxonomy of Group based Authentication

5. Discussion

Based on the schemes and protocols in Table 3, it can be summarized that for data integrity, methods with good encryption technique have successfully achieved the goal of data integrity. Good encryption during data transmission can counter MiTM attacks as well as data spoofing attacks. The schemes with mutual authentication with good encrypted keys successfully achieved the goal of providing user and device privacy. Schemes with only key encryption are liable to MiTM and impersonator attacks because an impersonator can conclude that the encrypted MAC between M2M are keys which will be then used to retrieve secrets. An efficient two-layer encryption for keys and end-to-end communication encryption would be a challenge itself as it might produce network overheads and would prove costly. Achieving optimal security protocol for MTC devices is still a challenge because of the large number of devices working simultaneously in one network. Our study elaborates the weaknesses and strengths of the current protocols and schemes that countered certain challenges. However, MiTM and Spoofing attacks are yet to be encountered with efficiency.

6. Conclusion

MTC devices are growing extensively and becoming part of almost every technology that we have in the modern world. These devices produce abundance of data that has to be made secure for the framework to be fully trusted and relied upon. Due to the remoteness and vulnerability, the trust issues of such devices and users are addressed by authenticating and verifying the transmitted data and users. Group-based authentication schemes are best used for remote operation of numerous devices interconnected within one network but GBA faces issues of efficiency and cost benefits in business model. Our study shows that, for general use of the scheme, there exists a gap in achieving a standard authentication and secure model that can address all general M2M communication networks.

Acknowledgment

This research is sponsored partly by the School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia and Vot No. (Q.J130000.2451.07G47).

References

[1] Choi, D., H.-K. Choi, and S.-Y. Lee, *A group-based security protocol for machine-type communications in LTE-advanced.* Wireless networks, 2015. **21**(2): p. 405-419.
[2] Lai, C., et al., *SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks.* Computer Networks, 2013. **57**(17): p. 3492-3510.
[3] Jiang, R., et al., *EAP-based group authentication and key agreement protocol for machine-type communications.* International Journal of Distributed Sensor Networks, 2013. **9**(11): p. 304601.
[4] Lai, C., et al., *A novel group access authentication and key agreement protocol for machine-type communication.* Transactions on emerging telecommunications technologies, 2015. **26**(3): p. 414-431.
[5] Bhasin, S. and F. Regazzoni. *A survey on hardware trojan detection techniques*. in *Circuits and Systems (ISCAS), 2015 IEEE International Symposium on*. 2015. IEEE.
[6] Cao, J., M. Ma, and H. Li, *GBAAM: group-based access authentication for MTC in LTE networks.* Security and communication networks, 2015. **8**(17): p. 3282-3299.
[7] Tanaka, H. *Information leakage via electromagnetic emanation and effectiveness of averaging technique*. in *Information Security and Assurance, 2008. ISA 2008. International Conference on*. 2008. IEEE.
[8] Hernandez, G., et al., *Smart nest thermostat: A smart spy in your home.* Black Hat USA, 2014.
[9] Lai, C., et al., *GLARM: Group-based lightweight authentication scheme for resource-constrained machine to machine communications.* Computer Networks, 2016. **99**: p. 66-81.
[10] Parno, B., A. Perrig, and V. Gligor. *Distributed detection of node replication attacks in sensor networks*. in *Security and Privacy, 2005 IEEE Symposium on*. 2005. IEEE.
[11] Fu, A., et al., *A privacy-preserving group authentication protocol for machine-type communication in LTE/LTE-A networks.* Security and Communication Networks, 2016. **9**(13): p. 2002-2014.
[12] Padmavathi, D.G. and M. Shanmugapriya, *A survey of attacks, security mechanisms and challenges in wireless sensor networks.* arXiv preprint arXiv:0909.0576, 2009.
[13] Li, J., M. Wen, and T. Zhang, *Group-based authentication and key agreement with dynamic policy updating for MTC in LTE-A networks.* IEEE Internet of Things Journal, 2016. **3**(3): p. 408-417.
[14] Mitrokotsa, A., M.R. Rieback, and A.S. Tanenbaum, *Classification of RFID attacks.* Gen, 2010. **15693**: p. 14443.
[15] Yao, J., et al. *GBS-AKA: Group-based secure authentication and key agreement for M2M in 4G network*. in *2016 International Conference on Cloud Computing Research and Innovations (ICCCRI)*. 2016. IEEE.
[16] Parne, B.L., S. Gupta, and N.S. Chaudhari, *Segb: Security enhanced group based aka protocol for m2m communication in an iot enabled lte/lte-a network.* IEEE Access, 2018. **6**: p. 3668-3684.
[17] Mahalle, P.N., et al., *Identity authentication and capability based access control (iacac) for the internet of things.* Journal of Cyber Security and Mobility, 2013. **1**(4): p. 309-348.
[18] Hassan, H.A.H., A. Pelov, and L. Nuaymi, *Integrating cellular networks, smart grid, and renewable energy: Analysis, architecture, and challenges.* IEEE access, 2015. **3**: p. 2755-2770.
[19] Aspects, T.S.G.S.a.S., *3GPP System Architecture Evolution (SAE); Security Aspects of Non-3GPP Accesses.* 2012. **11**(4.0).
[20] Mišić, J., V.B. Mišić, and N. Khan, *Sharing it my way: Efficient M2M access in LTE/LTE-A networks.* IEEE Transactions on Vehicular Technology, 2017. **66**(1): p. 696-709.

[21] Jung, K.-R., A. Park, and S. Lee. *Machine-type-communication (MTC) device grouping algorithm for congestion avoidance of MTC oriented LTE network*. in *International Conference on Security-Enriched Urban Computing and Smart Grid*. 2010. Springer.
[22] Chen, Y.-W., et al., *Group-based authentication and key agreement.* Wireless Personal Communications, 2012. **62**(4): p. 965-979.