Group Authentication with Fault Tolerance for Internet of Things

Otmane Elmouaatamid[1,2](✉), Mohamed Lahmer[1,2], and Mostafa Belkasmi[1,2]

[1] SIME Lab, ENSIAS, Mohamed V University, Rabat, Morocco
otmane.elmouaatamid@gmail.com, mohammed.lahmer@gmail.com,
m.belkasmi@um5s.net.ma
[2] My Ismail University, Meknes, Morocco

Abstract. With proliferation of the Internet of Things (IoT) applications, it is expected that 50 billion connected devices will be operating amongst us by 2020, so the normal authentication mechanism will be a big issue to handle to avoid causing a serious burden to server. As it is known, some devices could share the same characteristics such as the same geographical area, the same features. In this case, these devices could be in the same group and the group will be identify by an identity. Taking advantages from this mechanism, all devices can be authenticated at the same time using the group identity. Among group authentication issues are if a member device of the group cannot authenticate with the distributor of the group intentionally or unintentionally, the group loses its identity. This loss of identity causes the authentication failure of the other group devices. To solve this issue in IoT a fault tolerance scheme introduced for the group authentication architecture. Our algorithm of fault tolerance allows reconstructing the group authentication identity despite the lack of broken devices of the group. Indeed, reconstructing the group identity can be performed by using multi-secret sharing scheme based on an error correcting codes if a sufficient number of the group devices are available.

1 Introduction

Emerging technologies are turning the Internet of Things (IoT), into the Internet of Everything. The IoT brings to life a vision of the future where the more manual aspects of life can be automated so we can enjoy more meaningful living. Through widespread advancements in smart technologies, the time to a fully connected world is rapidly advancing. Internet of things becomes of utmost importance as it is almost involved in all our daily tasks. The development of IoT requires the use of new technologies which mean new challenges can arise. Security of exchanged data is one of these challenges that needs to be addressed. In order to ensure security of information in IoT, some security requirements such as authentication, confidentiality, and integrity have to be satisfied. Security threats to Internet of Things are not theoretical, they are already happening. Recent attacks like *the smart light bulb password leaks*, *hacks of Foscam baby*

E. Sabir et al. (Eds.): UNet 2017, LNCS 10542, pp. 299–307, 2017.
https://doi.org/10.1007/978-3-319-68179-5_26

monitors, *Belkin home automation systems*, and *hacks of smart cars systems*, are just the beginning. As the number of intelligent devices rises, the potential damage that could be caused by lack of security will continue to increase. Devices authentication is one of the most important security services in IoT application. But the unicast authentication communication from big amount devices will merge together in the network, and will cause serious burden to the server in particular at the level of energy consumption availability. Some devices have the same characteristics, such as having same features, being in the same place, working at the same time, etc. With group authentication mechanism [9], all devices can be authenticated with little signaling and calculation at the same time which reduce the network burden and save time. The group authentication is no longer a one-to-one type of authentication as most conventional devices' authentication schemes that have one prover and one verifier, but it is a many-to-many type of authentication that has multiple provers and multiple verifiers. During the process of group authentication, one or several devices of the group can be interrupted during the life cycle of the network. There are many causes of these failures ones that are intentionally or unintentionally like lacking in energy resources, damage to property, environmental interference, compromise of devices, etc. These failures will affect the overall operation of the authentication of the group. The fault tolerance [7,10] is then defined as the ability of group members to continue to function normally without interruption even after the malfunction of one or more of its devices. In this paper, we describe the security of group authentication. Then, we provide a group authentication procedures for the IoT and we explain the different steps to integrate fault tolerance into a group authentication architecture which is based on the aspect of multi-secret sharing scheme based on an error correcting codes [11]. The remainder of this paper is organized as follows. In Sect. 2, we provide an overview of the related work. Section 3 gives the procedures and a background on group authentication. Section 4 presents a detailed description of fault tolerance scheme based bounded distance decoding of linear codes. Finally, we give a brief conclusion and present some perspectives.

2 Related Work

Harn [1] introduces a new type of authentication called group authentication, which authenticates all users belonging to the same group. But they include polynomial operations so it becomes more complicated. As well as reuse of token is done so it becomes more risky for alteration of data. In [2], Mahalle and Jadhav proposed a group authentication using paillier threshold cryptography in which RSA algorithm is used to generate keys. As well as Shamir's secret sharing is used to distribute a secret to all members [5]. In this scheme, Group Manager (GM) plays a vital role in communication. GM has to stay active all the time between communication. Shamir's secret sharing [3] proposes to break data D into n parts in such a way that D is easily constructible from k pieces. There are two main requirements for this scheme: the first is when we have information of any t or more than t parts can recreate the master secret s; The second is with information of less than t parts can't reveal any information about the master secret s. This is called as $(t, n) - threshold$ scheme. In this reference paper [4], key management is considered. When we want to keep data secure, we encrypt it. But when we want to keep key secure, we keep it at a secure location. But this not optimal: an unusual situation can make the information inaccessible.

3 Group Authentication in IoT

Group authentication is a sort of authentication technologies [1] with which a group of users or devices can be authenticated together at the same time. Instead of authenticating a number of terminals of a group one by one, group authentication mechanism treats these devices in the group as a whole, and authenticates them together. Each group has a unique identifier, and a distributor, which can be called as group distributor, cluster distributor, etc.

Group authentication scenario description: Group authentication consists of three steps as follows:

The first step: Devices should be authenticated whether it belong to a specific group. This can be implemented through the proprietary authentication technology in a group, such as IEEE 802.15.4, ZigBee, Bluetooth or any other protocol of Communication/Transport layer.

The second step: A mutual authentication should be made between a specific network entity, and a group distributor who is eligible to delegate all devices in the group.

The third step: An authentication between network server and IoT cloud services will establish [8].

After the success of the authentication, devices and network entity can generate separated session keys individually if there is some demand to make individual communication between network entity and each device.

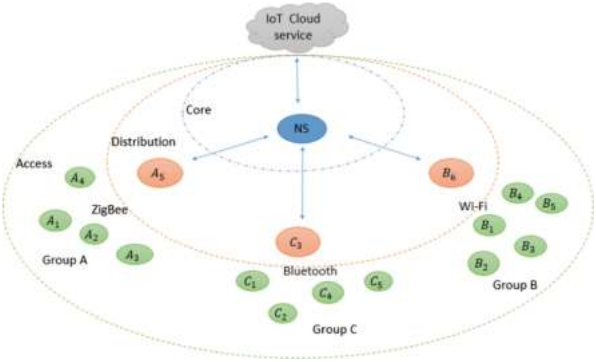

Fig. 1. Group authentication in hierarchical network for IoT

The Fig. 1 present a Group Authentication Architecture for IoT, there is detailed architecture description as following in Fig. 1. There are three Communication/Transport layer protocols IEEE 802.15.4, ZigBee, and Bluetooth. In each area of this protocols there are devices inside a given group. for example, in the group A devices communicate via Zigbee protocol: Where A_1, A_2, A_3, A_4 represent the network access and A_5 represent the group distributor. All devices in the group A can communicate with each other. Furthermore, the distributor A_5 of group A is able to communicate with others Groups distributors and with network entity directly via other protocols e.g. WiMax, LTE, GPR. etc. Network entity will stock the group information, such as identifiers, root keys used for all devices inside the group. Network entity is also in charge of for generating group authentication vector. The scenario is illustrated above.

Group Authentication procedures: As mentioned in the beginning of this section the group authentication procedure can be divided into three steps as shown in Fig. 2.

In the first step authentication between group members and the distributor of the group, the second step authentication will be performed between the group distributor and network server and the finally step is the authentication between network server and IoT cloud services.

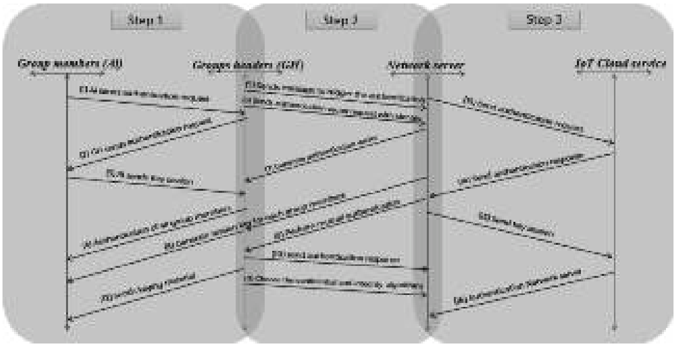

Fig. 2. Group Authentication Mechanism

- Step 1: Authentication mechanism between group members and the group distributor.
  1. At first each device member of the group Ai send a message to establish authentication with the distributor of the group.
  2. Group distributor send authentication request to each group member Ai.
  3. Each group member Ai will verify group distributor at first. If successful, Ai will generate session key for the communication with group distributor, and sends response mentioned such session key back to group distributor. If not success, the authentication is failed and group authentication procedure will be abort.

4. Group Header authenticate each group member Ai through the response message and record the authentication result in a mapping table.

   If all member of the group success to authenticate by the group distributor the group authentication will past to second step.

- Step 2: Authentication mechanism between each group distributor and the network server.

5. Group distributor sends message to network server to establish the authentication outside the group.
6. For now, the distributor of the group sends authentication vector request to network server with identity.
7. Network Server will generate authentication vector according to group distributor identity.
8. What is more, network server should be able to recognize that a group authentication is being performing based on group distributor identity and will generate session key for each group members. Network Server will send such authentication vector and session keys together back to group distributor.
9. Network server will perform mutual authentication with group distributor.
10. Group distributor authenticate group members and send authentication response back to network server.
11. Network server authenticates group distributor. If successful, it can be considered that group distributor and all group devices is authenticated successfully.
12. Group distributor will communicate with network server to choose the confidential and integrity protection algorithms. After that, group distributor will send keying material, selected algorithms to each group member.

  After these two steps, each device of the group is authenticated with network server.

- Step 3: authentication mechanism between the network server and IoT cloud service.

13. Network server sends a message to trigger authentication with the IoT cloud service at first.
14. Cloud service sends authentication request to the network server.
15. Network server verifies cloud server at first. If success, network server will generate session key for the communication with IoT cloud service.
16. IoT cloud service authenticates the network server.

4 Fault Tolerance Scheme Based Error Correcting Codes

In the third section, we presented the procedures and steps of Group Authentication. If every device is functioning then the authentication will be successful. Otherwise, if device member of the group breakdown, the other group members become unable to authenticate. Because a part of the identity of the group is missing, so we have proposed a fault tolerance scheme based on bounded distance decoding of linear codes [5,6]. In this section, we present how to reconstruct the identity of the group despite the absence of a number (threshold) of the members of the group which they have a breakdown. We proposed an algorithm based on multisecret sharing schemes [12,13]. The principe of this algorithm is as follows: It allows a secret known from a member call the group distributor to be distributed to n members of the group. The secret is unknown to each member but some special subsets of the network called the coalition of group members, can distribute the secret throughout the network. Because of this secret, we can construct the identity of the group. If the coalition of the group authentication did not happened we can reconstruct the group identity by the reconstruction of the secret based a $(m, n) - threshold$ system such that $m > 1$ member of the group can reconstruct the secret but $m - 1$ cannot.

4.1 Sharing Secret Key Scheme Based on an Error Correcting Code

In this section we present a group authentication sharing secret key scheme based on an error correcting code where secret key reconstruction is made by using bounded distance decoding of the code.

Error correcting code. Let $C(n, k)$ be a linear code over the finite filed of order q denote by F_q is a subspace in $(F_q)^n$ with q a prime power.

Where k is the dimension of the code and n is length of C and the dual code of C is defined to be the set of those vectors $(F_q)^n$ which are orthogonal to every codeword of C. It is denoted by $C^\perp$. The code $C^\perp(n, n-k)$ is a linear code. A generator matrix G for a linear code C is a $k * n$ matrix for which the rows are a basis of C. A parity-check matrix for a linear code C is a generator matrix for its dual code $C^\perp$. It is denoted by H.

The code C contains q^k codewords and can be used to communicate any one of q^k distinct messages.

We encode the message vector $x = x_1, x_2, \ldots, x_k$ as $(x_1, x_2, \ldots, x_k)G$; hence $C = \{uG | u \in (Fq)^k\}$. The map $u \rightarrow uG$ sends the vector space q^k onto a k-dimensional subspace of $(F_q)^n$.

Suppose that C is an $[n, k]$-linear code over F_q and a is any vector in $(F_q)^n$. Then the set $a + C$ defined by $a + C = \{a + x | x \in C\}$ is called a coset of C [6]. Suppose that a codeword x is sent, and that a vector y is received. Then $e = y - x(x, y \in (F_q)^n)$, $e = e_1, e_2, \ldots, e_n$, is an error vector.

Theorem. Suppose $C(n, k)$ is a linear code over F_q.

1. *Every vector of $(F_q)^n$ is in some coset of C,*
2. *Every coset contains exactly q^k vectors,*
3. *Two cosets either are disjoint or coincide,*
4. *C contains exactly q^{n-k} cosets.*

Proof: In this scheme, the key secret is recovered due to the minimal access sets. The minimal access sets consist of the vectors as $c + h$ with the support of h contained in the support of c and h of weight t.

There are n members participants in every set, as many as coordinates of C. The set of participants that is recovering the secret is also the support of these minimal access sets.

The number of the participants in each of minimal access set is equal to the weight of $c + h$.

This scheme satisfied the hypothesis of theorem above is also a $(d - t, n)$-threshold secret sharing scheme, where d is the minimum distance and t the error-correcting capacity of C.

4.2 Fault Tolerance Scheme Description

This scheme permit to reconstruct the secret key based on linear codes with a known bounded distance [14].

We consider a code $C(n, k)$ over F_q which is a t-error correcting code.

We construct now this scheme based on code C.

Let $(F_q)^k$ be the key space and $(F_q)^n$ be the share space. The distributor uses a share function $f : (F_q)^k \rightarrow (F_q)^n$ to compute the shares among the n members of the group. The sharing function is chosen as $f(s) = sG + h$, where $s = (s_1, \ldots, s_k) \in (F_q)^k$ is the secret and G is a $k * n$ generator matrix over $(Fq)^n$ with rank k. Suppose for convenience $s \neq 0$. Thus $c = sG$ is a nonzero codeword of the code C.

The translation vector h is chosen by the leader to satisfy the following requirements:

- the weight of h is t.
- the support of h is included in the support of c.

Then the n members recover the key secret by combining their shares as follows:

- get $c + h$ by collecting its n coordinates (shares)
- get c from $c + h$ by decoding
- get the secret s from c by solving the linear system $sG = c$ of rank k.

This scheme satisfied the hypothesis of the theorem is also a $(m = d - t, n)$-threshold secret key sharing scheme, where d is the minimum distance and t the error-correcting capacity of C.

Application Example

In our architecture we consider the group A consist of $n = 5$ members participants of group authentication, the distributor of the group and other four members.

Let $C(5, 2)$ be a binary linear code with generator matrix

$$G = \begin{pmatrix} 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{pmatrix} \tag{1}$$

With a minimum distance $d = 3$ and the code C corrects a single error $t = 1$. Now we can construct a $(2, 5)$ threshold scheme based on C by using bounded distance decoding and examine some properties of this scheme.

$$C = 00000, 10101, 01011, 11110$$

and the cosets of C are:

$$\begin{aligned}
00000 + C &= 00000, 10101, 01011, 11110 \\
10000 + C &= 10000, 00101, 11011, 01110 \\
01000 + C &= 01000, 11101, 00011, 10110 \\
00100 + C &= 00100, 10001, 01111, 11010 \\
00010 + C &= 00010, 10111, 01001, 11100 \\
00001 + C &= 00001, 10100, 01010, 11111 \\
11000 + C &= 11000, 01101, 10011, 00110 \\
10010 + C &= 10010, 00111, 11001, 01100
\end{aligned}$$

Let the message vector 10 be the key secret s. So, the sharing function will be as:

$$\begin{aligned}
f(s) &= sG + h \\
&= (10) * \begin{pmatrix} 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{pmatrix} + (10000) \\
&= (10101) + (10000) \\
&= (00101)
\end{aligned} \tag{2}$$

We get $c = sG = (10101)$ from (00101) by decoding. Then we get the key secret s from c by solving the linear system $sG = c$ of rank $k = 2$:
$(s1, s2)$.

$$\begin{pmatrix} 1\,0\,1\,0\,1 \\ 0\,1\,0\,1\,1 \end{pmatrix} = (10101) \tag{3}$$

Therefore we recover the key secret as $s = (10)$.

5 Conclusion and Perspective

In this paper, we proposed a new solution to secure group authentication in IoT with fault tolerance. Our solution is based on the fact that some users can share some similarities such as they can belong to the same area or launch a task at the same time. Taking advantage of these similarities users can form a group and get authenticated at the same time. Our scheme does not only establish a simultaneous authentication of all the members belonging to the same group, but also allows them to be authenticated even if one member or more encounter a problem this can be achieved by using a fault tolerance scheme based on an error correcting codes.

As future work we intend to integrated a key pre-distribution technique which is based on Balanced Incomplete Block Design (BIBD) to ensure the fault tolerance of group authentication in IoT environment.

References

1. Harn, L.: Group authentication. IEEE Trans. Comput. **62**(9), 1893–1898 (2013)
2. Mahalle, P., Jadhav, P.: Group authentication using Pailliar threshold cryptography. IEEE ISBN 978-1-4673-5999-3
3. Harari, S.: Application des codes correcteurs au partage du secret. Traitement du Sig. **4**(4), 353–356 (1987)
4. Liu, Y., Cheng, C.: An improved authenticated group key transfer protocol based on secret sharing. IEEE Trans. Comput. **62**(11), 2335–2336 (2013)
5. Csirmaz, L.: Gruppen secret sharing or how to share several secrets if you must? Mathematica Slovaca **63**(6), 1391–1402 (2013)
6. Hill, R.: A First Course in Coding Theory. Oxford University, Oxford (1986)
7. Geeta, D.D., Nalini, N., Biradar, R.C.: Fault tolerance in wireless sensor network using hand-off and dynamic power adjustment approach. J. Netw. Comput. Appl. **36**(4), 1174–1185 (2013)
8. Kalra, S., Sood, S.K.: Secure authentication scheme for IoT and cloud servers. Pervasive Mob. Comput. **24**, 210–223 (2015)
9. Sakarindr, P., Ansari, N.: Survey of security services on group communications. IET Inf. Secur. **4**(4), 258–272 (2010)
10. Anurag, D., Bandyopadhyay, S.: Achieving fault tolerance and network depth in hierarchical wireless sensor networks. In: International Conference on Communications Systems and Telecommunications (2008)
11. MacWilliams, F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes. North Holland, Amsterdam (1977)
12. Massey, J.L.: Minimal codewords and secret sharing. In: Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory, pp. 276–279 (1993)
13. Ding, C., Kohel, D.R., Ling, S.: Secret-sharing with a class of ternary codes. Theor. Comput. Sci. **246**(1–2), 285–298 (2000)
14. Bulygin, S., Pellikaan, R.: Bounded distance decoding of linear error-correcting codes with Grbner bases. J. Symbolic Comput. **44**(12), 1626–1643 (2009)