Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)

Mahalle, Parikshit N.; Prasad, Neeli R.; Prasad, Ramjee

Published in:
4th International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems (VITAE), 2014

DOI (link to publication from Publisher):
10.1109/VITAE.2014.6934425

Publication date:
2014

Document Version
Early version, also known as pre-print

Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)

Parikshit N. Mahalle, Neeli Rashmi Prasad and Ramjee Prasad
Center for TeleInFrastruktur, Aalborg University, Aalborg, Denmark
{pnm, np, prasad}@es.aau.dk

Abstract: Internet of things (IoT) is an emerging paradigm where the devices around us (persistent and non-persistent) are connected to each other to provide seamless communication, and contextual services. In the IoT, each device cannot be authenticated in the short time due to unbounded number of devices, and receipt of their authentication request at the same time. Therefore, secure, and efficient group authentication, and authorization scheme is required that authenticates a group of devices at once in the context of resource constrained IoT. This paper presents novel Threshold Cryptography-based Group Authentication (TCGA) scheme for the IoT which verifies authenticity of all the devices taking part in the group communication. This paper also presents TCGA framework which is flexible and secure. The proposed TCGA scheme is implemented for WI-FI environment, and the result shows that TCGA scheme is lightweight, and alleviates the effect of battery exhaustion attack. This paper also presents time analysis, and formal security analysis of TCGA scheme which shows that the proposed TCGA scheme is safe from the replay, man-in-the-middle attack, and is scalable in nature.

***Keywords*: Authentication, Internet of Things, Threshold Cryptography.**

I. Introduction

The Internet of Things (IoT) refers to the network interconnection of everyday devices. An IoT is a world-wide network of inter-connected devices uniquely addressable, based on a standard communication protocol. In the IoT, people are surrounded by different types of computing devices which are billion in number, varied in size, and capabilities to communicate with each other. Devices are having limited capabilities, and computing resources which range from Radio Frequency Identification (RFID) tags to embedded devices, PDA, and sensor nodes. IoT integrates the physical world with the information world, and provides ambient services, and applications. IoT networks allow users, devices, and applications in different physical locations to communicate seamlessly with one another. In brief, the IoT facilitates different communication patterns like: user-to-user, user-to-device, device-to-device, and devices-to-user. However, the decentralized, and distributed nature of the IoT face challenges in authentication, access control, and Identity Management (IdM) [2, 3, and 4]. There are various challenges to design security solutions in the IoT like constraints, and heterogeneous communication, resource constraints, and distributed nature.

IdM of devices in the IoT is one of the important challenges, and can be achieved by efficient authentication schemes which are simple, secure, and lightweight. In the IoT, there are unbounded numbers of heterogeneous devices talking to each other. Each device should not be able to authenticate during the short time. Due to the scale of economics, more than hundreds of devices may request authentication approval at the same time. To this purpose, lightweight, scalable, and secure group authentication scheme is required which will authenticate groups of devices, and not the individual devices to achieve secure group communication. This paper proposes a group authentication scheme using Paillier Threshold Cryptography [5, 6, and 7] which is a public key variant of the (t, n) threshold scheme where t is threshold, and n is number of group members. The Paillier Cryptosystem helps to achieve homomorphic properties, which is most suited for privacy preservation in the IoT applications. It is probabilistic asymmetric public key encryption system which uses randomness in an encryption algorithm, so that when encrypting the same, plaintext for several times. This will yield different cipher texts. The key properties of Paillier Cryptosystem include homomorphic addition, indistinguishability, and self-binding [5, 8]. Essentially, the Paillier Cryptosystem comprises of three algorithms: key generation, encryption and decryption. The proposed TCGA scheme is used to verify the authenticity of all the members taking part in a group oriented application. The scheme also helps in establishing a shared secret key between the members of the group which can be used for further communication in any group oriented applications.

This paper is organized as follows: Section II presents related works, and evaluation of the related works. Section III presents the proposed TCGA scheme and TCGA framework. Section IV presents the implementation results, security analysis, and the discussion. Finally, section V summarizes the paper with the future work.

II. Related Works

In a group authentication [9], participants belonging to the same group are authenticated. It is many-to-many type of authentication, which is more suited for group oriented IoT applications as there are more number of devices. Group authentication for users is presented in [9], which is t-secure, m-user, n-group Group Authentication Scheme (GAS): ((t, m, n) GAS), where t is a threshold of the proposed scheme. In [9], resources, constrained devices are not considered. Scalable, and decentralized group authentication protocol for vehicular communication is presented in [10]. Detail security analysis of the proposed scheme is not presented in [10]. Group-based handover authentication scheme for mobile WiMAX networks is presented in [11], where handover of security context takes place at the each mobility. It consists of point multiplication operation at each node which adds extra overheads. Secure mutual authentication protocol for RFID is presented in [12]. Hash-based encryption adds more overhead to this scheme. In [13], the profile based authentication, and authorization is

discussed without implementation details, and results. A group-based negotiation in peer to peer system is presented in [14], but authors have failed to discuss the security analysis of the proposed scheme. Resource negotiation language is discussed in the scope of this paper but, its applicability to other ad-hoc networks is left unaddressed. A lightweight, and distributed group authentication scheme for ad-hoc network devices is presented in [15]. Performance analysis of the proposed scheme is not discussed in [15].

From the state of the art, it must be however noted that existing group authentication schemes are not lightweight, and secure. Also in the context of IoT, there is a need of scalable group authentication scheme due to large number of heterogeneous devices.

III. Proposed TCGA Scheme

In [9], the author has achieved group authentication by releasing token based on Shamir's (t, n) secret sharing scheme. This paper extends this work using Paillier Threshold Cryptography. Proposed TCGA scheme also establishes a secret session key at the end of each group authentication which can be used for group application. TCGA scheme is implemented in WI-FI environment.

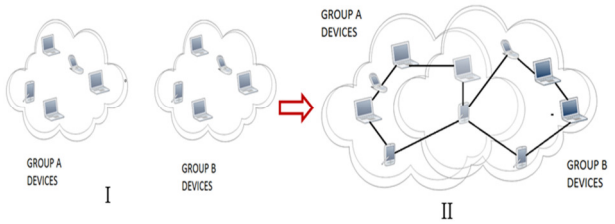

Figure 1: Group Authentication

Initially, let's consider an environment where we have devices in two contexts as shown in above Part I of the Figure 1. Each group contains a set of devices communicating with each other using shared secret key. There can be any number of groups each having its specified range of connectivity according to the WI-FI standard. These groups can even overlap with each other with many devices capable of being a part of more than one group. Part II in the Figure 1 depicts the state of the environment when a member has group authenticated with a group. Now, if a device of the group B, wants to communicate with any device in the group A, then device will initiate the handshake, thereby authenticating itself with the group A. Eventually, only authenticated devices from the group B will have the secret of the group A. Now it can communicate with all the members of the group A since it is group authenticated. On the other hand, all the devices of the group B except the authenticated one cannot communicate with the group A devices. The head of the group is required to generate, and distribute the new key pairs every time a new member enters the group to maintain group key leakage, and it is referred as Group Authority (GA) in this paper. TCGA comprises following five modules:

1. Key Distribution.
2. Key Updation.
3. Group Credits Generation.
4. Authentication Listener.
5. Message Decryptor.

Algorithms for these five modules are presented below. Time analysis of key distribution shows that it takes O (n) time for 'n' devices which is linear time, and, hence efficient for large number of devices. Time analysis of group authentication is polynomial time with O (n^2) which is fairly good time for group oriented applications in IoT.

Algorithm 1 TCGA – *Key Distribution*

```
1: GA <-- Key Distributor
2: NewM <-- New Member
3: Gcurr <-- The Group member wants to join
4: START
5:     if (REQUEST == JOIN)
6:     if (groupListContains(Gcurr) &&
       Pssword= = Gcurr.Password)
7:     updateMemberList(IP[NewM])
8:     updateThreshold(n)
9:     keys [] = KeyGen. PaillierThresholdKey (128, n, threshold,
10:    randomNum( ))
11:    for (k: Gcurr.groupMembers )
12:    Connect (Gcurr.groupMembers.i)
13:    Send (Gcurr, key [k++])
14:          else
15:                Display ("ERROR")
16: END
```

Time Analysis: n = Number of devices

Recurrence relation can be written as:

$$T(n) = T(n-1) + T(1)$$
$$= T(n-2) + 2*T(1)$$
$$= T(n-3) + 3*T(1)$$
$$\ldots$$
$$= T(n-k) + k*T(1), \text{ let's put } k = n-1$$
$$T(n) = T(1) + n-1(T(1))$$
$$T(n) = 2 + n*2 - 2$$

Hence $T(n) = O(n)$

Time analysis of key distribution shows that, in the proposed TCGA scheme, it takes O (n) time to distribute key amongst n devices. This shows that, even for large number of devices, the time required for key distribution is linear and more appropriate for the scalable IoT.

Algorithm 2 TCGA – *Key Updation*

```
1: Gcurr <-- Current Group
2: START
3:     if (REQUEST == "UPDATE_KEY")
4:     Update (Gcurr.set(PrivatePartKey) ,
       Gcurr.set (GroupMemberList))
5: END
```

Algorithm 3 TCGA – *Group Credits Generation*

```
1: Gcurr <-- Current Group
2: START
3:      secret = Random (r)
4       hash = MessageDigest ["SHA-512", secret]
5:      GroupCred = Encrpyt ([secret, hash]_KPublicKey )
```

```
6:    for (i: Gcurr.groupMembers)
7:    Send (GroupCred,i )
8:    //After Group Cred sent to all the members,
      GAuthentication starts
9:    for (i: Gcurr.groupMembers)
      Send ("Start Distribution")
10: END
```

Algorithm 4 TCGA – *Authentication Listener*

```
1: GroupCred <- [Secret, H (Secret)]
2: Gcurr <-- Current Group
3: PDM <-- Partially Decrypted Message
4: START
5:    if (REQUEST == "START DISTRIBUTION")
6:    myPDM = DECRYPT (GroupCred, Gcurr.
      PrivatePartKey)
7:    START [ PDMMessageDecryptor ]
8:    for (i: Gcurr. GroupMembers)
9:    Send (myPDM)
10: END
```

Algorithm 5 TCGA – Message Decryptor

```
1: Gcurr <-- Current Group
2: PDM   <-- Partial Decrypted Message
3: START
4:    while ( Gcurr.groupMembers - 1 )
5:    PartialDecryption [k++] = Received [PDM]
6:    if (finalDECRYPTION = CombineShares (
      PartialDecryption []))
7:    GROUP AUTHENTICATION SUCCESSFUL
8:     else
9:     GROUP AUTHENTICATION UNSUCCESSFULL
10: END
```

Time Analysis: Group Authentication

Recurrence relation can be written as:

$$
\begin{aligned}
&T(n) = T(n-1) + O(n)\\
&= T(n-2) + O(n-1)) + O(n)\\
&= T(n-2) + O(n-1) + O(n)\\
&= T(n-3) + O(n-2) + O(n-1) + O(n)\\
&\quad ...\\
&= T(1) + O(2) + ... + O(n-1) + O(n)\\
&= O(1 + 2 + ... + n-1 + n)\\
&= O(n^2)
\end{aligned}
$$

Time analysis of the proposed TCGA scheme shows that, to authenticate n devices to each other from different group, it takes O (n^2) time. O (n^2) represents polynomial time complexity and for even large number of devices, it performs better. This time is also logarithmic time as the running time of this algorithm is proportional to the square of input size. To summarize, detailed time analysis of the proposed TCGA scheme shows that it is time efficient and, most suited for the IoT consisting of unbounded number of devices.

TCGA scheme uses a variant of the public-key cryptography known as Threshold Cryptography to develop a lightweight group authentication mechanism suitable for ad-hoc devices. Group authentication aims at removing the need to establish a secure connection between all the devices in a particular group every time they want to communicate, and thereby reducing the number of handshakes done before the communication starts. This reduced overhead will help in conserving battery power as well as ensures that minimum numbers of resources are used. This provision of joining new member to the group, and updating threshold value for new device, and generating key using Threshold Cryptography is the task of key distribution module. Key Updation module generates public/ private key pairs for GA. The other members of the group change their private part keys using this module. The Message Decryptor module combines all the partially decrypted messages, and produces final a decrypted message. The Authentication Listener module listens for authentication request if any, and accepts the Partially Decrypted Message (PDM) from all the members. TCGA works in two phases:

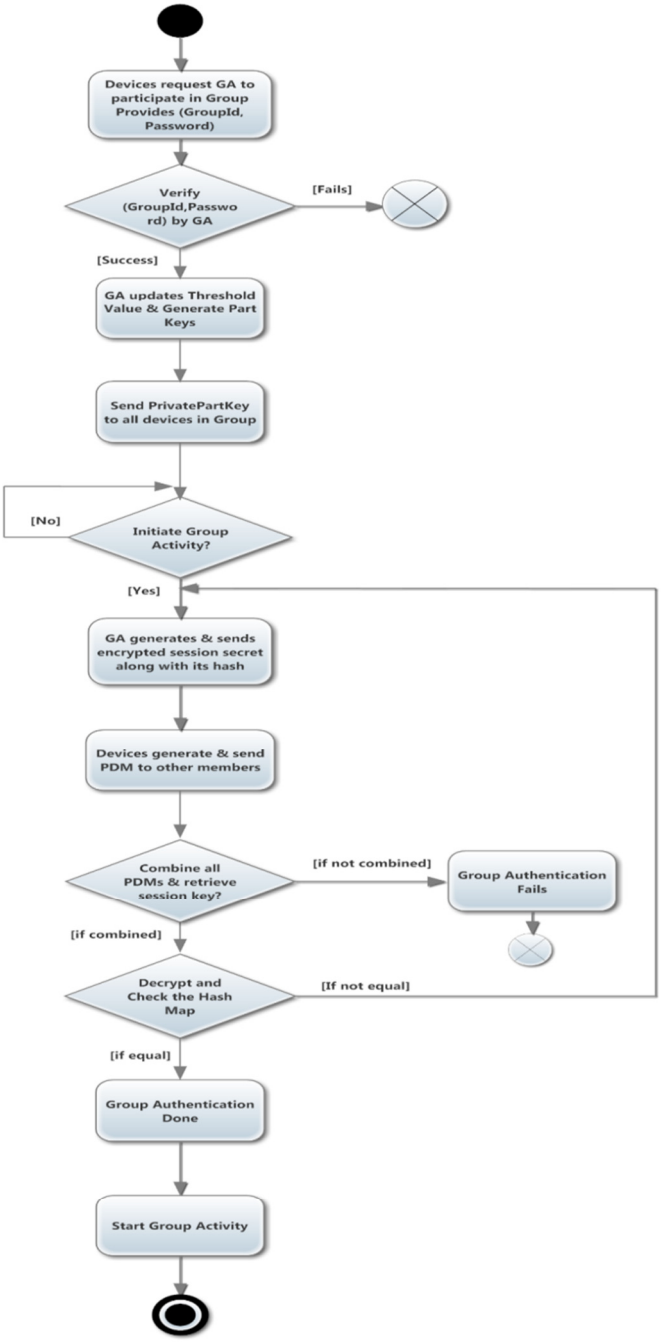

Figure 2: TCGA Activity Diagram

Complete TCGA scheme is depicted in the Figure 2 with an activity diagram which describes the logical processes, or functions where each process describes a sequence of tasks, and decisions that govern when, and how they are performed.

a. Pre-Authentication Phase

In this phase, the GA of the group, who creates the group, is responsible for generating a public key $K_{Pu\ (G)}$ and multiple private keys K_{Pr1} (G).....K_{Prn} (G) using Paillier Threshold Cryptosystem depending upon the number of members (n) in the group, and the threshold value t. Private keys $K_{Pr1(G).....}K_{Prn(G)}$ are then distributed by the GA among all the members of the group. When a new member joins the group, the threshold value is changed appropriately, and keys are generated, and distributed again. This threshold value changes dynamically as new members join so that the high level of security is maintained.

b. Group Authentication Phase

If a group activity needs to be started, group authentication needs to be performed as a pre-requisite to check if all the members $M_1...M_m$ *(where m<=n)* are part of the group. The GA chooses a pseudo-random number as a session secret [SS] key which is going to be shared with all the members of the group once the group authentication is done. This is encrypted using the public key [K_{Pu}] of the group, and sent to all the members of the group. The hash of the session secret H [SS] is also sent along with it.

$$Message = \{[SS]\ K_{Pu}, H\ [SS]\}$$

Each of the members, upon reception of this message, applies their private key part to decrypt it, giving them a PDM. Each device has a unique PDM corresponding to a different part key.

$$PDM = Decrypt\ (Message, PrivatePartKey)$$

Each device then sends this PDM to every member including the GA. All the devices wait to combine all the PDMs until n-1 PDMs are received. Each device combines all the PDMs so as to get the decrypted session key.

$$Session\ Key = Combine\ (PDM_1, PDM_2 \ldots PDM_m)$$

If combining all PDM shares is successful, the session key is obtained and it proves that all the members are a part of that group only. The Decrypted session key is hashed to get H' [SS] and checked with the one sent by the GA. If H' [SS] = H [SS], then authentication is successful, and session key [SS] is obtained. This comparison is made to check whether the session key obtained is valid. The session key [SS] obtained in the last step can be used for further communication between the devices which can be carried out using Symmetric Key Encryption. If combining all PDM shares is unsuccessful means that there is at least one non-member in the group, and, hence the activity cannot be initiated, and group authentication fails. Further individual authentication needs to be done to identify the non-member in the group.

To summarize, when any particular member wants to start a group activity, it send a request to the current GA. On reception of the request, the GA generates a session secret which is going to be shared by all the members of that group. This session secret is then encrypted with the public key of the group. This provides the required security as it can only be decrypted by the complete private key. A Hash map function is applied to the session secret which is going to be used in further steps to prove the integrity of this message. It is sent along with the encrypted session secret in a single message. This message is sent to all the members of the group. All the devices then use their own part private keys to decrypt this message which gives them a PDM which is not the final session secret. Now it sends this PDM to each member in the group. Until n-1 PDMs are received each of the devices waits. All the devices then try to combine all of the shares which will ultimately give them the final session secret. If successful, means that all the PDMs received are by the legitimate group members only, and, hence the group authentication succeeds. The group activity can then be started using the session secret for further communication. If unsuccessful, means that there is at least one device which is using a fake part private key and hence the partial decryption generated by him is not genuine. Therefore, upon trying to combine all the shares it was result in failure. This means that group authentication fails, and there is a need to restart the process.

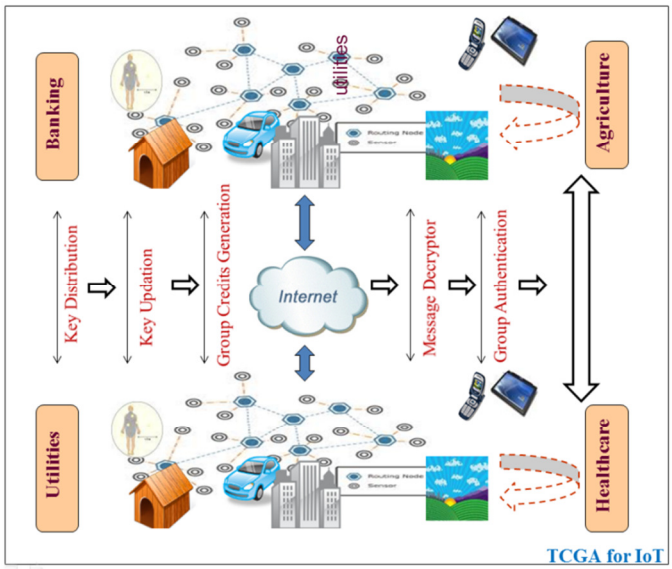

Figure 3: Proposed TCGA Framework

- ***Proposed TCGA Framework***

In the IoT communication, there are devices belonging to same group or different group communicating to each other in distributed manner. When devices of the same group communicate with each other, there is some amount of trust available between them. But when the devices of the different group communicate to each other, proposed TCGA scheme is required. Proposed TCGA framework is presented in the Figure 3. Framework depicts the major components of authentication process. In the IoT applications like banking, utilities, agriculture and healthcare, authentication is a major

concern. When the devices belonging to different groups communicate to each other through Internet, TCGA performs key distribution, key updation, message decryption and finally group authentication in order to authenticate each other.

The security analysis of the proposed TCGA framework is given below. Security analysis shows that proposed TCGA framework is flexible which realizes many-to-many authentication and secure in distributed environment.

IV. Results and Discussion

TCGA scheme is implemented for WI-FI using laptop devices. All the devices communicate with each other with respect to their individual group. Implementation results are discussed below.

- ***Implementation Results:***

Working of TCGA shows that, generating session secret, encryption, and hashing take place at GA. In this paper, TCGA scheme is compared with the group authentication scheme presented in [9] in terms of the number of handshake between GA, and device to device. Number of handshakes between communicating entities and the computation at the respective entity is directly related to the computational overhead of the authentication scheme. In the TCGA scheme, the number of handshakes between devices, and GA are three which include request for the session secret, sending a reply to the device comprising of (SS, K_{pu} (G), H [SS], and finally the reply from device which includes either successful authentication, or failure. In the scheme presented in [9], the number of handshakes between GA, and communicating entity (user) are four which includes all user registration, sending private token to each user, GA assisted group authentication, and the result of authentication to GA. In TCGA scheme, three types of computation takes place at GA which includes generation of session secret, encryption, and hash creation.

In [9], computations takes place at GA includes selecting random polynomial of degree t-1, computing n tokens, token distribution to all group members, and the selection of secret. Hence, there are four different types of computation taking place at GA in this case. Table I shows the comparison of TCGA scheme with the scheme proposed in [9] for different comparative parameters.

The proposed TCGA scheme is implemented for WI-FI devices using laptop devices of the same configuration in order to compare the computational time. Computational time is measured at GA for authenticating one device, and the average of three measurements is taken to avoid the variation caused by environmental parameters. Result shows that TCGA scheme takes 0.496 seconds at GA, and GAS [9] takes 0.681 seconds. This difference in the computational time at GA to authenticate one device shows that TCGA is energy efficient as compared to the GAS. This makes TCGA lightweight, and it helps to alleviate battery exhaustion attack.

TABLE I: COMPARISON BETWEEN TCGA AND GAS [9]

Parameters ↓ Scheme →	TCGA	GAS [9]
Number of Handshake (GA and Device)	03	04
Number of computations at GA	03	04
Computational time at GA	0.496 s	0.681s

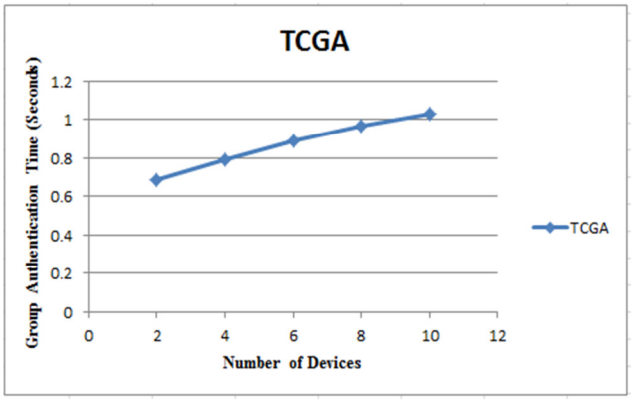

Figure 4: Number of Devices Vs Group Authentication Time

A series of three measurements have been taken to find the group authentication time in seconds by increasing the number of devices from two to ten. Figure 4 shows that, with the increase in the number of devices, there is no significant change in the authentication time. This result shows that, even the numbers of devices are increased at a faster rate; there is no increase in the authentication time at the same rate. This shows that TCGA scheme is scalable, and best suited for IoT consisting of unbound number of devices.

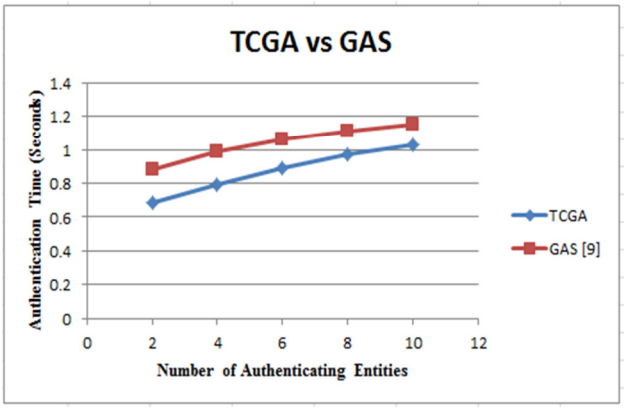

Figure 5: TCGA Vs GAS

The proposed TCGA scheme is also compared with GAS scheme in terms of the computational time required for authenticating devices. The number of devices varies from two to ten, and authentication time in seconds in measured for both TCGA and GAS. Figure 5 shows that, TCGA scheme performs better than GAS scheme. Results shown in the Figure 4, and 5 shows that the proposed TCGA scheme performs better in terms of the number of handshake, computations at GA as well as the time required to authenticate varied number of devices.

- ***Security Analysis***

The proposed TCGA scheme is also analyzed for the replay attack, and man-in-the-middle attack. The analysis is as follows:

i. Replay Attack

Replay attack is one in which a valid data transmission between two devices is intercepted, and is reused with malicious intent. Let's consider the scenario in which an attacker M possessing the symmetric key tries to communicate with a third person belonging to the same group in subsequent sessions. This will not be possible as the session key is dynamically changed as each new group activity is initiated.

ii. Man-in-the-Middle Attack

A man-in-the-middle attack is a one in which an attacker M makes an independent connection with the victims A, and B, making them believe that they are communicating with each other. The attacker M intercepts the message coming from A to B, and B to A, and re-routes them. In our proposed scheme, the session key is established between the members of the group participating in the group activity. Any communication between the group members is secured by using symmetric key encryption using this session key. Hence, the attacker M cannot decrypt the messages between A, and B, and misuse the information sent between the legitimate devices.

V. Conclusions and Future Work

In the IoT, there are unbounded numbers of heterogeneous devices talking to each other. Each device should not be able to authenticate during the short time. Due to the scale of economics, more than hundreds of devices may request authentication approval at the same time. To this purpose, this paper has presented TCGA which is Threshold Cryptography-based lightweight, scalable, and secures the Group Authentication scheme. This scheme not only established a group authentication scheme which ensures the simultaneous authentication of all the members of a group using Paillier Threshold Cryptography but also established a secret session key which can be used for communication that might occur in group oriented applications. The Implementation results have been measured for computational time and authentication time, and also compared with the existing work. Results shows that, proposed TCGA scheme is lightweight and scalable, and alleviates the effect of battery exhaustion attack. Security analysis of TCGA is also presented in this paper which shows that, TCGA is resistant to replay, and man-in-the-middle attack.

The future plan is to integrate TCGA scheme with the IdM framework presented in [16]. Implementation of TCGA for wireless sensor network, and RFID is also another good research area to continue.

References

[1] Maarten Botterman, "Internet of Things: an Early Reality of the Future Internet," Workshop Report, European Commission Information Society and Media, May 2009.

[2] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity Authentication and Capability based Access (IACAC) Control for the Internet of Things," In Journal of Cyber Security and Mobility", River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013.

[3] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad, and Ramjee Prasad, "Identity Establishment and Capability Based Access Control (IECAC) Scheme for Internet of Things," In proceedings of IEEE 15th International Symposium on Wireless Personal Multimedia Communications (WPMC – 2012), pp: 184-188, Taipei - Taiwan, September 24-27 2012.

[4] Sachin D. Babar, Parikshit N Mahalle, Neeli R. Prasad and Ramjee Prasad, "Proposed on Device Capability based Authentication using AES-GCM for Internet of Things (IoT)," In proceedings of 3rd International ICST Conference on Security and Privacy in Mobile Information, and Communication Systems (Mobisec 2011), Aalborg – Denmark, May 17-19, 2011.

[5] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes," In Proceedings of the 17th International Conference on Theory, and Application of Cryptographic Techniques (EUROCRYPT), pp: 223-238, 1999.

[6] Miao Pan, Jinyuan Sun, and Yuguang Fang, "Purging the Back-Room Dealing: Secure Spectrum Auction Leveraging Paillier Cryptosystem," In IEEE Journal on Selected Areas in Communications, Volume: 29, no.4, pp: 866-876, April 2011.

[7] Rongxing Lu, Xiaohui Liang, Xu Li, Xiaodong Lin, and Xuemin Shen, "EPPA: An Efficient, and Privacy-Preserving Aggregation Scheme for Secure Smart Grid Communications," In IEEE Transactions on Parallel and Distributed Systems, Volume: 23, no.9, pp: 1621-1631, September 2012.

[8] E. Goh, "Encryption Schemes from Bilinear Maps," Ph.D. Thesis, Stanford University, USA, September 2007.

[9] Lein Harn, "Group Authentication," In IEEE Transactions on Computers, IEEE computer Society Digital Library, IEEE Computer Society, 16 October 2012.

[10] Lei Zhang, Qianhong Wu, Solanas A., and Domingo-Ferrer J., "A Scalable Robust Authentication Protocol for Secure Vehicular Communications," In IEEE Transactions on Vehicular Technology, Volume: 59, no. 4, pp:1606-1617, May 2010.

[11] Anmin Fu, Shaohua Lan, Bo Huang, Zhenchao Zhu, and Yuqing Zhang, "A Novel Group-Based Handover Authentication Scheme with Privacy Preservation for Mobile WiMAX Networks," In IEEE Communications Letters, Volume:16, no:11, pp:1744-1747, November 2012.

[12] Morshed M.M., Atkins A., and Yu H., "Efficient Mutual Authentication Protocol for Radiofrequency Identification Systems," Communications, IET, Volume: 6, no: 16, pp: 2715-2724, November 6 2012.

[13] Pfleeger Shari Lawrence, Rogers Marc, Bashir Masooda, Caine K., Caputo Deanna, Losavio Michael, and Stolfo Sal, "Does Profiling Make Us More Secure?," In IEEE Journal of security and privacy, Volume:10, Issue:4, 2012.

[14] Squicciarini A.C., Paci F., Bertino E., Trombetta A., and Braghin S., "Group-Based Negotiations in P2P Systems," In IEEE Transactions on Parallel, and Distributed Systems, Volume: 21, no:10, pp:1473-1486, October 2010.

[15] L. A. Martucci, T. C. M. B. Carvalho and W. V. Ruggiero, "A Lightweight Distributed Group Authentication Mechanism," In Proc. of 4th International Network Conference, Plymouth, UK.

[16] Parikshit N. Mahalle, Neeli R. Prasad, and Ramjee Prasad, "Novel Context-aware Clustering with Hierarchical Addressing (CCHA) for the Internet of Things (IoT)," In the Proceedings of IEEE 4th International Conference on Recent Trends in Information, Telecommunication and Computing – ITC 2013, August 01-02, 2013, Chandigarh, India.