International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-14 Issue-01 June 2019

Collaborative Wireless Sensor Network Security

SwapnaNaidu

Jaipur

Abstract: To authenticate several devices simultaneously, group authentication is used. Applications centered on groups make advantage of this. Because the number of people using the internet is increasing daily. For devices to communicate, we need safe authentication. Connecting devices over wireless media is what we're doing. Just one group manager is present. The workload of devices and group managers is reduced by our suggested method. We verify the devices using a technique called paillier threshold cryptography. The value of H(SS) is calculated by the group manager. It is unnecessary for devices to gather all partially decrypted messages and determine the hash value. A pass key will be provided by the group management in order to prevent devices from requesting to interact. Thus, a safe and innovative group authentication technique may be provided to authenticate devices in a strong manner.

Keywords: topics covered include group authentication, Pascal's threshold cryptography, Shamir's secret sharing, the RSA algorithm, and public and private keys.

1. Introduction

We need a secure authentication technique for authentication purposes on wireless networks due to the increased danger of data tampering. The ability to authenticate a single user was a limitation of earlier systems. It was a major pain to keep passwords safe and keys in order in knowledge and key authentication techniques. So, group authentication comes to the rescue in order to authenticate several users simultaneously.[1]

The process of establishing one's identification is known as authentication. We need to establish the device's legitimacy before it may communicate. This means that other security mechanisms were in use in earlier systems. However, it is difficult to retain both the private and public keys and passwords of poor quality. Thus, group authentication was introduced. Several devices may be authenticated simultaneously. In earlier designs, there was just one verifier and one prover, and authentication was done one-to-one. The RSA algorithm is used to create keys [7].

In a nutshell, two types of authentication methods exist. There is one that has an authentication server (AS) and one that does not. The authentication server is the rightful owner of all keys that are to be released and has full access privileges to all networks. The remaining sections of the article are as follows: 2 covers relevant work, 3 presents a suggested scheme, and 4 details the flow of the system.

2. Related Work

The author suggested a group authentication method based on Pascal's threshold cryptography in [3]. In which RSA algorithm is used to create keys. Additionally, all members may get a secret via Shamir's secret sharing. For this plan to work, GM's communication capabilities are crucial.GM must maintain constant activity in between messages. Consequently, a system's performance is impacted by the rise in computing overhead. Another crucial aspect to think about is key regeneration.

Members may verify one other's identities by exchanging challenge and answer messages, as proposed in the authentication paradigm in [1]. A secure channel is necessary for the transmission of a secret "k" between participants in this. All members may be authenticated simultaneously using this way. However, theirinclude polynomial operations so it becomes more complicate. As well as reuse of token is done so it becomes

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-14 Issue-01 June 2019

more risky for alteration of data.Shamir‟s secret sharing [2] proposes that break up data D into n parts in such a way that D is easily constructible from k pieces. There are 2 requirements of this scheme. 1. When we have information of any t or more than t parts can recreate the master secret s 2.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, 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 is having flaws, like single bad luck can make information inaccessible.To achieve secure group authentication we need to use one time session key which is distributed all over group members. For this, a new improved authenticated protocol has been made [4]. In this paper, Shamir‟s secret sharing scheme is used. It provides authentication by sending a single message to all group members. This protocol prevents both insider and outsider both attacks. Consider there are p members in a group and they want to distribute the session key to all. Then KGC (Key Generation Centre) looks for fresh session keys and distribute them. For being valid member, member must be registered firstly to KGC [1].

[5]Large number of machine type communications (MTC) is a need of today‟s increasing use. A large number of MTC accessing a network simultaneously may cause atrocious authentication signaling congestion. To solve this problem a protocol namely lightweight group authentication protocol arrives. In traditional systems they used public key cryptosystem. This protocol in the MTC in the long term evolution(LTE) network based on MAC (Message authentication codes),called LGTH which can authenticate all users simultaneously.

3. Proposed Scheme

Figure 1 shows system architecture of group authentication in which multiple devices are connected in network. GM will

give keys and pass keys to them. If H(SS)=H‟(SS), then all devices are legitimate.

Our scheme uses paillier threshold cryptography in which RSA algorithm is used.RSA algorithm is used to generate keys. Sharing of keys among all group embers securely is a tough task. Protecting keys from outside threats is point which is taken into consideration. When any new user wants to communicate in a group, GM has to increase a threshold. Here, GM is not considered as a group member itself. Its task is limited up to generating and distributing keys as well as increase and decrease threshold. GM also regenerates the keys when any new member arrives. In this way, our system is prone to key compromise attack. GM will be in idle state when all members in a group are communicating. GM will provide pass key to limited devices so that when it will receive number of requests to communicate then load on server will not increase. Each member having pass key will sign up and then will log in. As soon as this pre authentication phase will be finished, GM automatically receives a list of legitimate devices. As devices complete 1 phase, process will be completed by 33%. When it will reach to 100%, devices are ready to communicate to each other. Also devices that are logged in have a list of legitimate logged in members.

Paillier threshold cryptography includes 2 phases.

1. Pre authentication phase
2. Group authentication phase

Pre Authentication Phase: In figure.2 GM does a task of generating and distributing public and private keys for communication. GM will also have a pass key for all devices. That means we are limiting number of devices to send request to communicate to GM. All devices will firstly sign up and then they will log in. As all phases will be cleared, devices are added to list of GM as legitimate member. Group Authentication

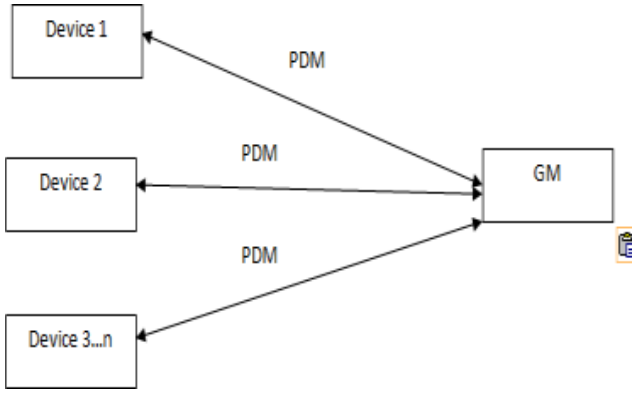
International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-14 Issue-01 June 2019

Phase: In figure.2 GM firstly checks that all devices are legitimate users then by using a public key a message is sent to all devices.

1. When a message delivered to all devices, they decrypt it using their private keys and then they get PDM.
2. All these PDMs are sent to GM to gain a complete message.
3. When GM receives all PDMs, it calculate value H(SS)= H‟(SS).
4. If both values are equal then we conclude that all devices are legitimate users and then further communication will be done.
5. If both values are not equal then we conclude that there is a non-member in a group or an attacker in a group.



International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-14 Issue-01 June 2019

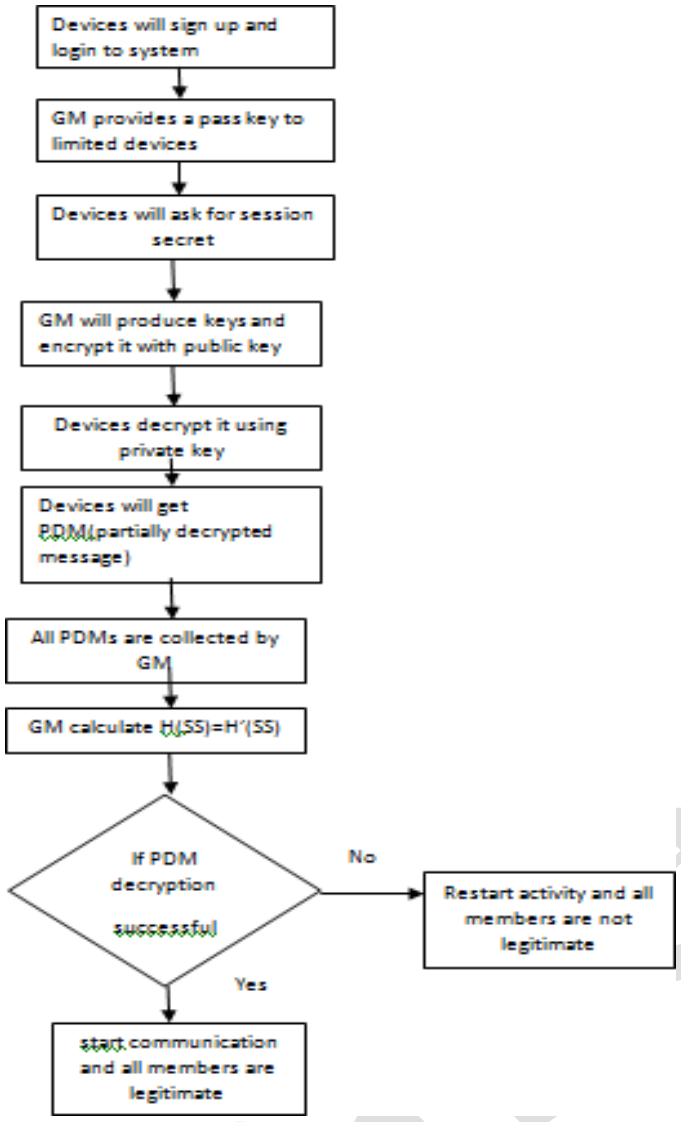


Figure 1: System Architecture of group authentication

Figure 2: Proposed scheme for system

4. Conclusion

Application that is group focused uses group authentication. This allowed for simultaneous authentication of several devices. We are reducing device tasks by allowing GM to calculate H(SS) via paillier threshold cryptography. It is not necessary for devices to gather all PDMs. the value of H(SS) is computed by GM. Device pass keys alleviate GM's overload. There is a shortage of gadgets in this area. All keys will renew whenever a new device wishes to communicate.

References

[1] Source: [1] Lein Harn, "Group Authentication." (2013), Vol. 62, No. 9.

[2]I am Adi Shamir. "How to share a secret." Volume 22, Issue 11 of the Communications of the ACM

International journal of imaging science and engineering

ISSN: 1934--9955 www.ijise.net

Vol-14 Issue-01 June 2019

(1979)
Group Authentication using Pavilliar Threshold Cryptography, by Parikhit Mahalle and Piyush Jadhav ISSN 14-6673-5999-3, published by IEEE
[4]Based on secret sharing, Yining Liu and Chi Cheng have developed an enhanced authentication group key transfer protocol. Computers and the IEEE, Volume 62, Issue 11.
[5]Lightweight Group Authentication Protocol for Machine-Type Communication in LTE Networks (LGTH) by Hui Li and Chengzhe Lai¨This is the IEEE publication number: 978-1-4799-1353-4.
Autonomous Group-based Authentication Mechanism in Mobile Ad Hoc Networks, by Parisa Memarmoshrefi and Omar Alfandi, [6] Computer Security, Privacy, and Trust: Eleventh International Conference on 2012 (IEEE).
Group Authentication in Wireless Sensor Networks, by Khyati Chaudhary and Gitanjali Shinde, 2015 International Conference on Pervasive Computing.