International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2014): 3.05

Group Authentication in Wireless Sensor Networks

Khyati Chaudhary[1], Gitanjali Shinde[2]

[1]Smt.Kashibai Navale college of engineering,Savitribai Phule Pune University, Off Sinhgad Road,Vadgaon(Bk), Pune

[2]Smt.Kashibai Navale College of Engineering, Savitribai Phule Pune University, Off Sinhgad Road,Vadgaon(bk), Pune

Abstract: ***Group authentication is used to authenticate multiple devices at once. This is used for group oriented applications. As nowadays a use internet is growing day by day. We need secure authentication for devices for communication. So we are connecting devices in wireless media. One group manager is there. Our proposed scheme is decreasing task of devices and group manager. Using paillier threshold cryptography we authenticate devices. we let group manager calculate value of H(SS). Devices have no need to collect all partial decrypted messages and calculate value of hash. Group manager will provide a pass key to avoid devices requests who want to communicate. In this way, a robust scheme provide secure and novel group authentication scheme to authenticate devices.***

Keywords: group authentication, paillier threshold cryptography, shamir's secret sharing, RSA algorithm, public and private keys

1. Introduction

In wireless networks, risk of data alteration is increases so for authentication purpose,we need a secure authentication scheme. In older systems, there was only facility to authenticate a single user at a time. In key and knowledge authentication schemes, maintaining keys was difficult task and keeping password secure was tough job. So to authenticate multiple users at once, group authentication arrives.[1]

Authentication is of act of proving sum one's identity. We have to prove that device which wants to communicate is legitimate. So in older systems, they were using different security systems. But maintaining passwords of low quality as well as maintaining private and public key is difficult. So group authentication came into picture. We can authenticate multiple devices at once. Older schemes were one-to-one authentication in which 1 verifier and 1 prover was there. Keys are generated using RSA algorithm[7].

There are generally 2 kinds of authentication systems. One is Authentication Server (AS) and other is no authentication server. Authentication server has all rights to access networks and it belongs to all keys which are to be distributed. In remaining paper, section 2 is related work, section 3 is proposed scheme, section 4 is flow of system.

2. Related Work

In [3], author 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. In this scheme, GM plays a vital role in communication.GM has to stay active all the time between communication. So computation overhead increases and it affects performance of a system. As well as regeneration of keys is a important point to consider.

In [1], author suggested authentication model in which member can authenticate them by sending challenge and response. In this, a secret 'k' is shared between members which requires a secure channel to send it to members. This method can authenticate all members at once. But they include polynomial operations so it becomes more complicate. As well as reuse of token is done so it becomes 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 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.

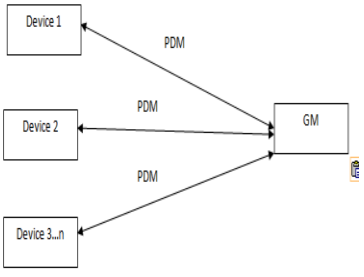

Figure 1: System Architecture of group authentication

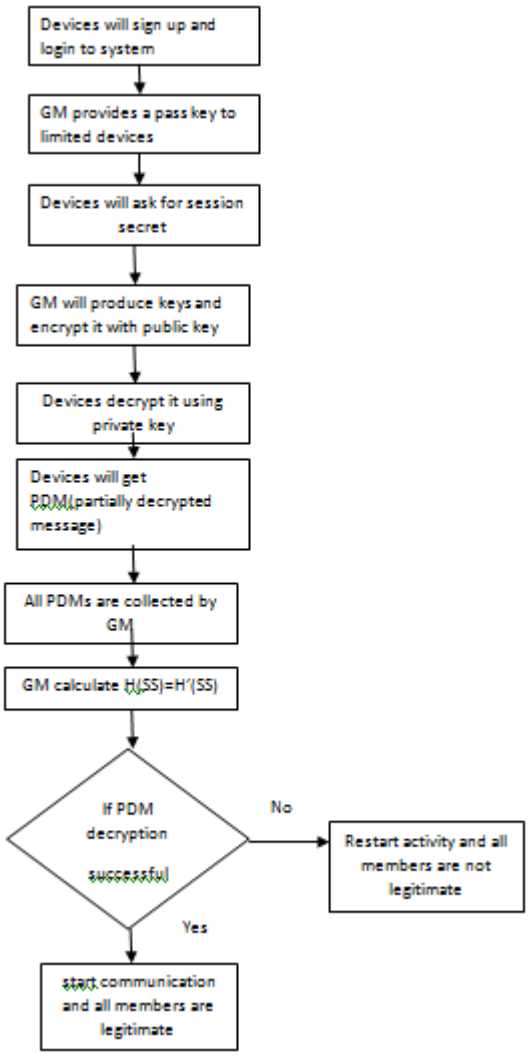

Figure 2: Proposed scheme for system

4. Conclusion

Group authentication is for group oriented application. In this multiple devices authenticated at once. Using paillier threshold cryptography, we are lessening tasks of devices by letting GM compute H(SS). Devices don't need to collect all PDMs. GM calculates value of H(SS). Providing pass key to devices reduces overload on GM. No of devices are limiting here. When any new device wants to communicate all keys will regenerate.

References

[1] Harn, Lein. "Group Authentication." (2013), VOL:62, NO:9
[2] Shamir, Adi. "How to share a secret." Communications of the ACM (1979) VOL:22, NO:11
[3] Parikshit Mahalle, Piyush Jadhav " Group Authentication using pailliar Threshold Cryptography" IEEE 978-1-4673-5999-3
[4] Yining Liu, Chi Cheng," An Improved Authenticated Group Key Transfer Protocol Based on Secret Sharing" IEEE Transactions on computers , VOL. 62, NO. 11.
[5] Chengzhe Lai§,, Hui Li," LGTH: A Lightweight Group Authentication Protocol for Machine-Type Communication in LTE Networks"IEEE 978-1-4799-1353-4.

[6] Parisa Memarmoshrefi, Omar Alfandi, "Autonomous Group-based Authentication Mechanism in Mobile Ad Hoc Networks" 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.
[7] Khyati Chaudhary,Gitanjali Shinde,"Group Authentication in Wireless Sensor Networks" International Conference on Pervasive Computing, 2015.