International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 6, Nov-Dec-2020, ISSN (Online): 2395-566X

Wireless SensorNetworks for Distributed Access Control using Priccess Method

Asst. Prof. A. Rajiv, Asst. Prof. C. Lakshmi
Department of ECE,
Sriram Engineering College,Tamilnadu,India

Abstact- **The Distributed access control allows the network to authorize and grant the permission to user to access the data in Wireless Sensor Network. In terms of providing security and authentication to the Wireless sensor network, our project is created. A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical conditions and to cooperatively pass their data through the network to a main location. The more modern networks are bi- directional, also enabling control of sensor activity. Hence the wireless sensor network is especially creating a high secure environment. Our paper mainly focuses on designing such access control modules for WSNs. It focuses on group sharing too. That is a distributed access control will share the data to all the users in that network whereas it will provide security to the WSN by avoiding a new user to unaccess the data. Sometimes a user does not want to associate his identity to data which he request. Only the data he needs. Because it might helps a new user to know his details while sharing the data. To avoid such issues here in our project we are introducing a query for a group to access the data. Here a single person will act as a leader in a group and he can create a query to sign in. So that the identity of the users will not known by anyone and also the whole group can get the data via this process.**

Keywords:- **Distributed access control, Wireless Sensor Network, bi-directional, secure environment.**

I.INTRODUCTION

The primary purpose of deploying a wireless sensor network (WSNs) is to monitor the physical world and provide Observation for various applications. As WSNs are usually deployed in an environment that is vulnerable to many Security attacks, it is critical to control the access to the sensor node, especially when there are many users in the system. Additionaly, different users may have different access privileges. for example, in the case of WSN deployed in a battlefield, a soldier only needs to access the data related to his task but a higher rank officer often requires information gathering for an overall manoeuvre and therefore should have more information access privileges than a soldier.

The application will be compromised if access control is not properly enforced. Access control can be executed by two approaches, namely, centralized and distributed. A centralized access control approach requires a base station to be involved whenever a user stored in the sensor node.Unfortunely it is inefficient, not scalable, and vulnerable to many potential attacks along the long communication path. For example, for sensor networks deployed in extreme and hazardous environments such as oceans and animal habitats, it may be impossible or prohibited to maintain a stable communication connection between an in network base station and outside network. Therefore, a centralized approach makes sense only for small, experimental network, but not for large scale sensor networks. On the other hand, in distributed access control the authorized user can ented the sensor field to directly access the data on sensor node without involving a base station. This approach can avoid weekness such as single point of failure, performance bottleneck, which are inevitable in the centralized case. These advantages together have led to recent increasing popularity of distributed data access control.

A privacy preserving access control in WSNs should satisfy the following requirements:

1. User Authentication: user authentication needs to be enforced for sensor data inWSNs.

2. User Privacy: Preserving: a network user may want to hide his data access privacy from anyone else including the network owner and other network users. More specifically, anyone else should be prevented from either knowing who is the sender of the query command, or whether two query commands originate from the same (unknown) sender.

3.Integrity Protection of Query Commands: The adversary may try to modify the query command constructed by a user, and a secure access control method should support the integrity protection of the query command.

4. Freshness: to defend against replay attacks, a node should have the capability of freshness checking for any query message.

5. Limits of Access Privileges: Access restriction may be enforced for users with different access privileges.
6. Dynamic Participation: New users can easily join the network, and users can easily be revoked when they are expired.
7. Availability of Secure Channels between a Network User and Sensor Nodes: In some application scenarios, it is necessary to establish secure channels between a network user and the targeted nodes.
8. Efficiency: Due to the limited energy, processing and storage resources of sensor nodes, a cryptographic technique should be efficient.

This paper makes two main contributions:
1. We first identify the characteristics of a single-owner multi user sensor network and present the requirements of distributed privacy-preserving access control. Then we pro- pose a novel approach to ensure distributed privacy preserving access control, called Priccess, which is built on a ring signature technique.Since a ring signature scheme was not originally designed for privacy-preserving access control, a direct application of the method cannot satisfy requirements(3), and (6)-(9), which are very challenging for ensuring secure, efficient and robust distributed privacy-preserving access control. To address these issues,some additional mechanisms are incorporated into the design of the proposed protocol. Finally, Priccess satisfies all of the above requirements. In addition, our heoretical analysis demonstrates the security properties of Priccess.

2. We also implement the proposed protocol in a network of Imote2 motes. Evaluation results show the efficiency of Priccess in practice. To the best of our knowledge, this is also the first implemented privacy preserving access control on the WSN platform.

II. OVER VIEW OF THE SYSTEM

In this paper, a ring signature technique is introduced to the design of Priccess. In Particular, sends a query command to the sensor nodes through a ring signature algorithm. The ring signature allows a user from a set of possible signers (i.e.,a subset of the group) to convince the verifier (i.e.,the sensor nodes) that the signer of the signature belongs to the set but theidentity of the signer is not disclosed. It protects the anonymity of a signer since the verifier knows only that the signature comes from a member of a ring, but does not know exactly who the signer is. There is no way to revoke the anonymity of the signer.Obviously, the ring signature technique can remedy the security issues of the group signature application.The ring signature is signer- ambiguous in the sense that the verifier is unable to determine the identity of the actual signer in a ring of the size of the ring is greater than 1/r.

Detailed description of these mechanisms will be given in Section II and III.Priccess consists of six phases: system initialization, user query generation, sensor node verification, establishing secure channels between the network user and sensor nodes, newuser joining phase, and user revocation phase. In the system initialization phase, the network owner and all users create their public and private keys.Then the network owner divides all users into groups and maintains a group access list pool [1].

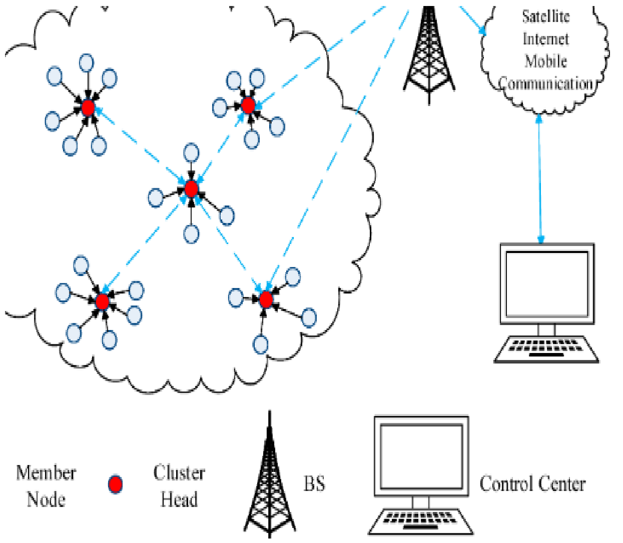


Fig 1. Overview of Wireless sensor network.

The group access list pool is pre-loaded on the corresponding sensor nodes before they are deployed. In the user query generation phase, if a user has a new query,the malicious node need to construct the query command and the ring signature and then send them to the sensor nodes[2]. In the sensor node verificationphase, if the query verification passes then the sensor nodes respond to the user's query command. The new user joining phase is invoked whenever a user wants to join the network while user revocation phase runs whenever a user is to be revoked. In this paper, we just focus on the access control on sensor networks, the secure storage on sensor nodes is out of our scope [3].

Additionally, in Priccess, we choose Elliptic Curve Cryptography (ECC) because ECC [4] has a significant advantage over RSA due to its computational efficiency, small key size, and compact signatures. Routing is important in wireless sensor network .The the routing tree generated by CTP (Collection Tree Protocol) as routing path for data transmission. By dividing at the source node, it adds the hidden information and also the privacy homomorphism [5]. The various security threats is discussed in [6].In this paper, current problems are assessed in the security of wireless sensor networks, and authentication security policies are discussed. In [7] discusses overall constraints, security requirements, security threats, typical attacks and their defensive techniques or countermeasures relevant to the sensor networks. Besides that, best practical suggestions are given to improve current security mechanisms on Wireless Sensor Network.

1. Network Model:

A WSN consists of a large number of resource constrained sensor nodes, many sensor network users, a single network owner and an offline certificate authority (CA). The sensor nodes are used to sense conditions in their local surroundings and report their observations to network users based on various query commands. The network users (e.g., soldiers) use access devices such as PDAs or laptop PCs to access the sensed data.

2. Trust Model:

Malicious network owner model: We suppose that the network owner charges users for accessing sensor data, thus enforcing strict access control. The network owner is trusted to provide the appropriate amount of data commensurate with users' payments. This coincides with the typical assumption about service providers. However, the network owner may for various purposes be interested in users' identities and data access patterns (e.g., who are interested in what kinds of data at what locations and times).

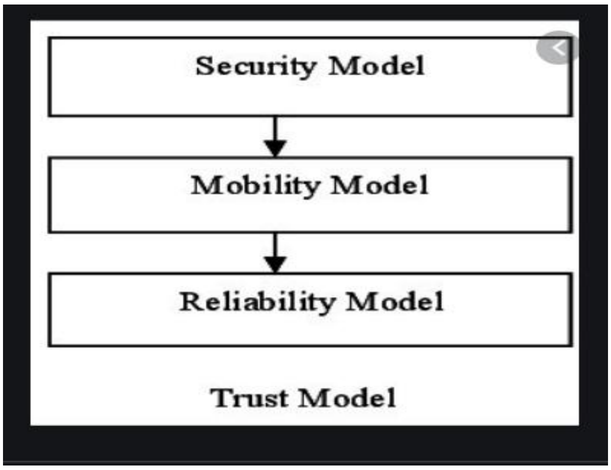


Fig 2. Trust Model.

3. Adversary Model:

An adversary can launch both outside and inside attacks. In outside attack, the adversary may leaves drop, copy and replay the transmitted messages in the WSN. Therefore, for a practical threat model we consider an adversary that is able to eavesdrop all network communications, as well as inject bogus messages or forge non-existing links in the network by launching a wormhole attack. As an inside attack, we assume that the adversary may compromise and control a number of sensor nodes subject to his choice. Additionally, we consider two sybil attacks: one is that the network owner could add a user to a group in which other users are impersonated by the network owner, this would remove the anonymity of this user. The other is that by presenting multiple identities, a malicious user can control a substantial fraction of the system and thereby undermine the security.

III. PRICESS: THE PROTOCOL

1. Overview of Distributed Privacy-preserving: Access Control

A system over view of distributed privacy-preserving access control in WSNs. It mainly involves three kinds of participants, the network owner, all sensor nodes, and the network users. The users who want to access the network firstly register to the network owner. Then the network owner divides all users into groups. Network users in the same group have the same access privilege. At the same time, the network owner maintains a group access list pool, which contains the identity and other information (e.g., access privileges) of each group.

2. Overview Of Pricess:

Pricess consists of six phases: system initialization, user query generation, sensor node verification, establishing secure channels between the network user and sensor nodes, new user joining phase, and user revocation phase.

3. System Initialization:

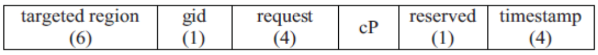
In the system initialization phase, the network owner and all users create their public and private keys.Then the network owner divides all users into groups and maintains a group access list pool. The group access list pool is pre-loaded on the corresponding sensor nodes before they are deployed.

4. **User Query Generation:**

After system initialization, network users can enter the network to access the senor nodes if a user has a new query, he will need to construct the query command and the ring signature and then send them to the sensor nodes.

5. Sensor Node Verification:

In the sensor node verification phase, if the query verification passes the the sensor nodes respond to the users query command. The new user joining phase is invoked whenever a user wants to join the network while user revocation phase runs whenever a user is to be revoked.



targeted region (6)	gid (1)	request (4)	cP	reserved (1)	timestamp (4)

Fig 3. User Query Generation.

IV.SECURITY ANALYSIS

1. User Authentication:

In order to pass the signature verification of sensor nodes, each user has to register to the CA and the network owner, then the network owner relegates him to a group according his access privilege. To send a valid message {*Que*, *σ*}, a network user needs to sign the query command *Que* with his private key and the public keys of allchosen group members.

2. User Privacy-Preserving:
As before, the use ring signature can ensure user privacy-preserving.More specifically, ring signature can lead to desirable user privacy-preserving property. We assume that m group members in the group have been chosen to generate the ring signature.

3. Integrity Protection of Query Command:
In Priccess, an authorized network user uses a ring signature technique to authenticate the query command Que.The sensor nodes know the public keys members and thus can verify.

4. Node Compromise Tolerance:
Only the public key of the network owner and the group access list pool are pre-loaded on every node. Therefore, even if an adversary compromises some nodes, the adversary just obtains the public key of the network owner and the group access list pool. Without the private key of a network user, the adversary cannot impersonate any network user by compromising nodes.

5. Freshness:
The use of the timestamp included in que can ensure the freshness of the message and replay attacks instead of timestamp.

6. Limits of Access Privileges:
The network owner can restrict each network user's activities by group division.

V.CONCLUSION

In this paper, we have proposed a novel protocol to achieve privacy-preserving access control for WSNs. The security analysis and experimental results show that our approach is feasible for real applications. To achieve privacy-preserving access control, the network owner in Priccess cannot determine the identity of the actual signer of a query command.

Thus, without the assumption that users are rational, a dishonest user may launch DoS attacks without exposing his identity. For example, a dishonest network user can exploit the benefits of distributed privacy- preserving access control and keeps sending query commands to sensor nodes for preventing its competing users from accessing sensor data.In general, the network owner should have measures to identify dishonest users and defend against their attacks. To achieve this, we can also rely on reports from sensor nodes. For example, if a dis- honest user launches some unknown attacks on sensor nodes, the network owner can identify which particular user group (the one including the dishonest users) launched the attack by analyzing the access records periodically submitted by each node. Then, the network owner can defeat users' misbehavior through some ways (e.g., revoking the user group).

REFERENCES

[1] B. Carbunar, Y. Yu, L. Shi, M. Pearce, and V. Vasudevan,"Query privacy in wireless sensor networks, "in Proc. IEEE SECON, pp.203–212,2007.

[2] R.Zhang, Y.Zhang, and K.Ren,"DP2AC:distributed privacy preserving access control in sensor networks, " in Proc.IEEE INFOCOM,2009.

[3] D.He, J.Bu, S.Zhu, M.Yin, Y.Gao H.Wang, S.Chan, and C. Chen, " Distributed privacy- preserving access control in a single-owner multiuser sensor network, "in Proc.IEEE INFOCOM Mini-Conference, 2011.

[4] A.Liu and P.Ning,"Tiny ECC:a configurable library for elliptic curve cryptography in wireless sensor networks" in Proc ACM/IEEE IPSN,2008.

[5] P.Li, C.Xu, H.Xu, L.Dong and R.Wang, "Research on data privacy protection algorithm with homomorphism mechanism based on redundant slice technology in wireless sensor networks," in China Communications, vol.16, no.5, pp. 158-170, May 2019.

[6] A.Karakaya and S.Akleylek, "A survey on security threats and authentication approaches in wireless sensor networks," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, 2018, pp.1-4, doi: 10.1109/ISDFS.2018.8355381.

[7] K.Z.Turakulovich and S.L.Tokhirovich, "Analysis of Security Protocols in Wireless Sensor Networks," 2019 International Conference on Information Science and Communication Technologies (ICISCT), Tashkent,Uzbekstan,2019,pp.14,doi:10.1109/ICISCT 47635.2019.9012015.