Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

An Accountable Access Control with Enhanced Privacy in Wireless Sensor Networks

R. MayaDevi[1], J.Albert Simon[2]
[1]M.E student, [2]AssociateProfessorDepartment of CSE
Sardar Raja College of Engineering, Tamilnadu, India

Abstract---- Security and privacy are the major concern in today's world, among any users and owners of different entities. In general, anyone would be aware of his/her own data privacy from other users, including the owners and the one who misbehaves has to be identified. Wireless Sensor Networks pays a great responsibility in monitoring and controlling of environments. However many remote authentication protocols have been proposed, each leads to a challenging factor of security and scalability. By enforcing a novel based approach which ensures strict access control using APAC protocol, which meets the above challenges. This protocol also ensures that it doesn't rely on third party, so feasibility can be achieved on sensor platforms. Performance evaluation demonstrates that the proposed protocol outperforms all the other existing schemes in terms of computational cost.

Keywords--- Access control, Wireless Sensor Network, Security, Privacy, Feasibility.

I. INTRODUCTION

Recently, with the terrific development in sensors and its desirable feature has attracted worldwide. This sensing technology shows a promising futuristic application in both terrain and for mass public.[1] The basic idea of any sensor is to observe tiny sensing devices that are capable of sensing each and every minute changes in the environment especially in communication with each other where the communication is done wirelessly. In today's world people are more concerned about security, mainly privacy preserving techniques. This attractive feature of Wireless Sensor Network has engrossed many researchers to work on access control.[1][2]

Due the significant advancement in Wireless Sensor Network (WSN) it has become feasible to provide to such access control to the user's and their satisfaction needs. However, due to the natural loss of sensor node the network might be affected by malicious attacks in hostile environment, this could lead to the destruction of some sensor node by the dishonest user which would make the entire network useless.[3] In such case, the misbehaving user might be able to get the access control so that all the secrets would be revealed to him.Obviously, many schemes have been proposed to the sensor network, but all these were focused on protecting the external attacks and no such results were provided for the accurate internal protection.

It is important to enforce network access control to handle intruders, even though it is critical to avoid invasion of user's privacy. In large scale WSN, the owners and users may come different entity and the individual needs would be different, they may be particular about their data to be confidential and even they don't want the owner to interfere in it.[7] For example: Panda hunter problem.

The above case requires the following in order to be aware of the dishonest user namely user authentication, user privacy preserving, Integrity, Access privileges, Freshness, Availability of secure channels, Compromise tolerance.[2] Generally. The data access control follows two main approaches Centralized access and Distributed access control, where the distributed privacy access control plays a vital role and has drawn its attention recently. The only distributed privacy preserving approach is done by using APAC protocol.[3] The intent of the APAC protocol is to ensure authorized user, secondly, it pinpoints the dishonest user, Finally, it satisfies all the above requisites and making it more practical.

Volume 4 Issue V, May 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

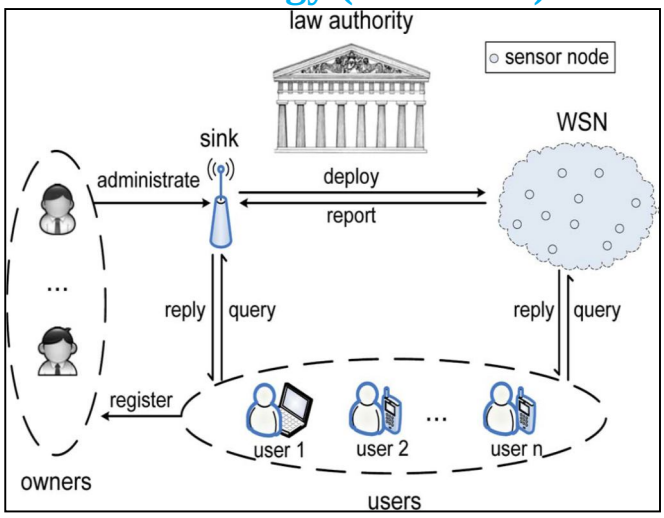

Fig.1 WSN network architecture

II. RELATED WORKS

Privacy issue has been widely explored moreover in all fields. Many techniques have been proposed for achieving privacy preservation in sensor network.[1][4] Yet, a large number of attacks are possible in WSN either internally or externally such as: Denial of Service, Sybil attacks, eaves dropping, attacks against privacy and so on. The earlier works were focused on communication security and data security, some techniques have been proposed to provide privacy over the data collection and transmission through WSN such as DP^2AC and the ring signature.[4] These two techniques were able to hide the users identity henceforth guarantees privacy.[5] However, they are faced with some security weakness. It has been reported that DP^2AC is not efficient in providing the token uniformly; it is not fine grained since each query command cannot be signed by the network user, therefore an intruder might get the access easily and gets authorized to modify the query command according to his wish.[6] Then comes the ring structure which makes both the computation complexity and makes anonymity strength depend on the size chosen and moreover, it is not designed with user authorizability.[8] Clearly, a practical access control should not restrict the user at any cause.

III. SYSTEM ANALYSIS AND DESIGN

A. *Objectives*

The proposed APAC access control satisfies the following design objectives.[9][10]

1) Network model: The WSN consists of number of users, resource constrained sensors and a sink. WSN reports the sensed data to the sink and the user in response to their queries.
2) Anonymity: Except the user and the owner is unable to trust to a particular protocol to a particular identity.
3) Mutual authentication: The user and the owner authenticate each other to verify their identities.
4) Trust and Adversary models: The user needs to pay for their data usage to the network. In case of severe attacks, law authority is enforced which acts as an independent third party. However, both of them should be prevented from user privacy. An adversary could be either an insider or outsider. The outsider may be of eaves dropping, injecting bogus messages into network, where an insider would intrude the control over number of users and nodes according to his/her choice.

B. *System model*

The proposed system consists of the following contributions in order to preserve the privacy for user access control.

1) The characteristics of multi-user-multi-owner has to be identified.
2) A novel based APAC protocol has been proposed to meet the requirements, which would exploit the group signature technique, which ensures dynamic participation.
3) Finally, the proposed protocol which is supposed to be the first implemented privacy preserving access control on the WSN platform.

C. *Proposed protocol*

Volume 4 Issue V, May 2016
ISSN: 2321-9653

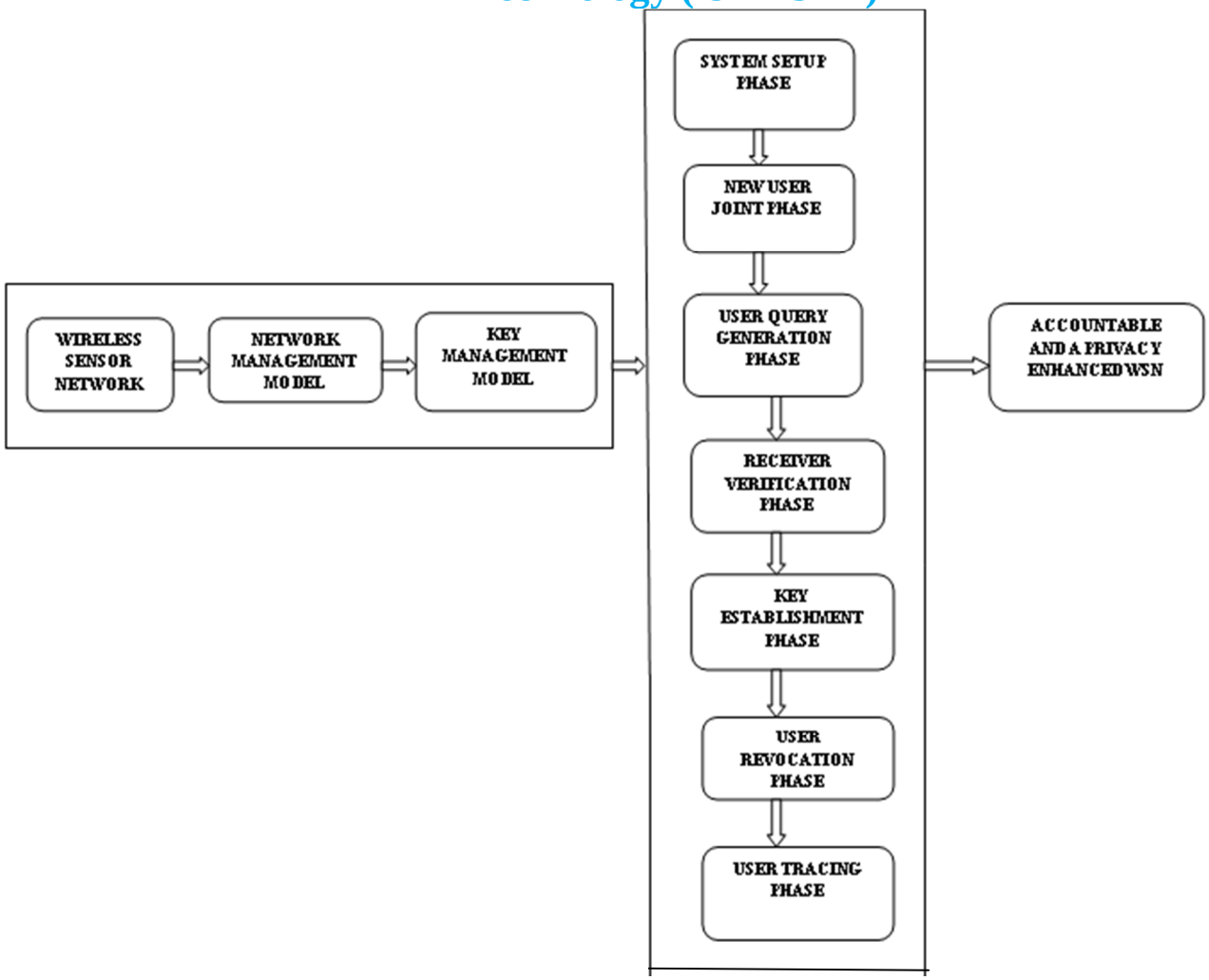

Fig. 2 Architecture of the proposed method

To achieve the goal of the proposed protocol a novel user revocation and key exchange mechanisms are incorporated. The APAC protocol involves seven phases namely: system setup phase, new user joint phase, user query generation phase, receiver verification phase, key establishment phase, user revocation phase and user tracing phase.

1) System setup phase: Each owner generates the partial public and private keys.
Randomly select an lQ-bit prime Q and an lP -bit prime P. Let F be an element of order Q in Z.
choose XG, XH ∈ ZQ and set G = FXG mod P, H = FXH mod P.
Send partial group public key {Q, P, F, G,H} to network
owners, possibly via an open wireless channel, and keep partial group private key XG secretly.

2) New user joining phase: This phase is invoked whenever the user wants to join the network.
Select a random number xi ∈ ZQ and compute Yi =Gxi mod P.
Upon receipt of the message, Choose a random le-bit number ei such that Ei = 2lE +ei is prime.
Compute wi = wE
Choose a random number, to send back the group.
Transmit back to the user via secure channel.

3) User Query Generation Phase: If a user has a query he/she has to construct the query using the group signature and then send it to the sensor nodes.
Select a random number r ∈ {0, 1}ln/2 and R ∈ ZQ.

Compute u = h mod n, U1 = FR mod P, U2 =GR+xi mod P =GRY I mod P, and U3=HR+e i mod P.

Choose rx ∈ {0, 1} lQ+lc+ls , rr ∈ {0, 1}ln/2+lc+ls , re ∈ {0, 1}le+lc+ls and RR∈ZQ and compute v=ureg − rxhrr mod n, V1 = FRR mod P V2=GRR+rx mod P, V3 =HRR+re mod P.

Generate a challenge c = h (gpk, u, v, U1, U2, U3, V1, V2, V3, h (req_ grpj)) and set zx = rx + cxi, zr = rr + c(−ri − rEi), ze=re + cei, and ZR=RR + cR.

4) Receiver Verification Phase: If the query passes, then the sensor responds to the user query.

Check that ze ∈ {0, 1}le+lc+ls and zx ∈ {0, 1}lQ+lc+ls . Set v= (aw) −cg−zxhzruc×2lE+ze mod n, V1=U1−cFZR mod P, V2=U2 −cGZR+zx mod P, V3=U3 −cHZR+ze mod P.

Check if the challenge c is correct: c? =h (gpk, u, v, U1, U2, U3, V1, V2, V3, h (req_ grpj))

5) Key Establishment Phase: The user and the sink share a session key for communication.

6) User Revocation Phase: This phase is involved to revoke the user by the user revocation message. An example of User Revocation Message is “Owner j asks to delete a user with (Ei, wi)”.

User tracing phase: Whenever a network owner observes certain network access being accessed and suspicious, it finds the corresponding access request message Que = {req, grpj, σ} from the network. There are also hybrids WSNs which consists of addition to resource-poor sensor nodes, includes some small number of resource-rich collector nodes, each serving as a temporary repository of the user access records.

IV. SECURITY ANALYSIS

A. Authentication

The proposed protocol achieves the property of user authentication unforgibily, by offering the user to register to at least one network owner, so that the network distributes the user with a secret key. Therefore the intruder cannot get authorized.

B. Integrity protection

The APAC protocol achieves the property of integrity protection, which access the authorized user to use a group signature technique. The sink has the public key and thus it verifies the user.

C. Privacy protocol against adversary

In APAC, the user and the owner have no knowledge about the private key, by anonymity both the user and owner can neither link a group signature. Hence communication is identified only through selecting fresh random numbers.

D. Privacy against law authority

APAC allows late binding between secret keys and the network users. It is the duty of the network owner to generate secret keys and then assigning them to each user without the involvement of any law authority. This satisfies two requirements 1) It reveals only nonessential attribute information 2) It is sufficient for user accountability and limiting the user from respective network.

V. CONCLUSION

This paper discusses about the security weakness of the existing protocol techniques and proposes an enhanced secured access control through APAC protocol that achieves user’s privacy preservation. The computational cost is much higher than the other existing techniques. Therefore the proposed protocol uses a pairing free method for session key generation which improves the performance of the designed protocol. This paper has also reported the evaluation results of APAC in an experimental network of resource limited sensor nodes, which show that APAC is efficient and feasible in practice.

REFERENCES

[1] H. Guo and Z. Sun, “Channel and energy modeling for self-contained wireless sensor networks in oil reservoirs,” IEEE Trans. Wireless Commun., vol. 13, no. 4, pp. 2258–2269, Apr. 2014.
[2] S. Ruj, A. Nayak, and I. Stojmenovic, “Distributed fine-grained access control in wireless sensor networks,” in Proc. IEEE IPDPS, 2011, pp. 352–362.
[3] J. Hur, “Fine-grained data access control for distributed sensor networks,” Wireless Netw., vol. 17, no. 5, pp. 1235–1249, Jul. 2011.
[4] S. Yu, K. Ren, and W. Lou, “FDAC: Toward fine-grained distributed data access control in wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 4, pp. 673–686, Apr. 2011.
[5] G. Bianchi, A. T. Capossele, C. Petrioli, and D. Spenza, “AGREE: Exploiting energy harvesting to support data-centric access control in WSNs,” Ad Hoc Netw., vol. 11, no. 8, pp. 2625–2636, Nov. 2013.

[6] Taking the Pulse of the Planet: EPA's Remote Sensing Information Gateway. [Online]. Available: http://www.epa.gov/geoss/
[7] D. He, S. Chan, S. Tang, and M. Guizani, "Secure data discovery and dissemination based on hash tree for wireless sensor networks," IEEE Trans. Wireless Commun., vol. 12, no. 9, pp. 4638–4646, Sep. 2013.
[8] S. Rahman, N. Nasser, and T. Taleb, "Secure timing synchronization for heterogeneous sensor network using pairing over elliptic curve," Wireless Commun. Mobile Comput., vol. 10, no. 5, pp. 662–671, May 2010.
[9] J. Deng, R. Han, and S. Mishra, "Secure code distribution in dynamically programmable wireless sensor networks," in Proc. IPSN, 2006, pp. 292–300.
[10] H. Lu, J. Li, and H. Kameda, "A secure routing protocol for cluster-based wireless sensor networks using ID-based digital signature," in Proc. IEEE GLOBECOM, 2010, pp. 1–5.