TECHNIQUES TO PRESERVE DATA ACCESS PRIVACY OF USERS IN WSN :A SURVEY

Merin Jacob
Department of Information Technology
Rajagiri School of Engineering and Technology
Kochi, India
merinjacob89@gmail.com

Sijo Cherian
Department of Information Technology
Rajagiri School of Engineering and Technology
Kochi, India
sijoc@rajagiritech.ac.in

Abstract— Sensor nodes in wireless sensor network are densely deployed to monitor the physical world. In distributed access control user can directly access data from sensor nodes. While accessing data from sensor nodes user details can be caught by sensor nodes. It adversely affects the user privacy. A user does not want the wireless sensor network to associate his details while he accessing data from sensor nodes. The mechanisms that considering the privacy of user is so limited. DP2AC, Priccess are the two mechanisms that protect the privacy of the user. These two approaches consider different techniques to preserve privacy of user access control.

Keywords-*:* wireless sensor network (WSN), access control, authentication, privacy

I. INTRODUCTION

Wireless sensor network is densely deployed with autonomous sensors. Sensor nodes are randomly deployed to monitor the physical world. Its features ensures a wide range of application areas like health ,military ,home ,environment, disaster relief operation and other commercial areas. User can access monitored data from sensor nodes. A user can access data from WSN in three different ways. First, sensor nodes can transmit their data through a base station to an external data logger which centrally handles data queries. Second, users send data queries via base station which in turn forwards query results to users. Third, user can directly access data from the sensor node without the help of base station. These three methods can be categorized in to two that is centralized and distributed. First two methods come under centralized and third one comes under distributed. The distributed is the only feasible option for sensor networks deployed in extreme and hazardous environments such as oceans and animal habitats, where it may be impossible to maintain a stable communication connection between an in network base station and the outside network. So in this paper we are considering techniques which follow distributed access control method. [3][5][9]

Sensor nodes are deployed in an environment where security is very low. So accessing data from sensor node in secured fashion is very critical. While user accessing data from sensor nodes user details can be caught by sensor nodes. It adversely affects the user privacy. A user does not want the wireless sensor network to associate his details while he accessing data from sensor nodes. To sustain in this competitive world user prefers to protect his details. By knowing interests of user, other competitors can beat down the user. The sensed data may be of interest to several users, ranging from individual users to universities, government research centers, industries etc. They do not fully trust each other, due to diversified interests. User's wishes to protect the attributes like data types accessing from nodes, from which node he access data etc.[6][7] For example an oil company interested in accessing data from ocean sensor network, tries to hide its access privacy from others. So there is high demand for protecting user's data access privacy. DP2AC[2]and Priccess [1][4]are two approaches that give importance to users data access privacy.

The three major roles participating in this network are network owner, sensor node and user. Owner is the one who owns the wireless sensor network. He is the one who decides who has the right to access wireless sensor network. The owner plays three major roles 1) authentication: confirms only known user can access service 2) authorisation: users only have access to allowed services 3) management of users and permissions. Initially user has to register with the owner, and then only he can access the sensor nodes. Sensor node responds only when he gets query command from authorised users. This is the basic communication that happening in both DP2AC and Priccess.

Basic requirements that must be followed in privacy preserving access control infrastructure are: 1)user privacy preserving : A user does not want anyone to associate his details while he accessing data from sensor nodes.2)authentication : information must not be accessed by unauthorized users 3)multi-user: multiple users have to be able to interact with the system 4) Efficiency: sensor nodes are low cost entities with limited processing ,energy and memory capacity. so the cryptographic techniques used here must be efficient 5)Protection against network attacks : a network attacker cannot gain access to restricted node services (authorized access only),nor can he modify messages .6)Scalability :the protocol should be efficient in a large scale wireless sensor network 7)Access privileges: access restriction has to be enforced according to the access privilege of the user.8)Freshness : to defend against replay attack there should be certain measures to confirm the freshness of query and response messages.9)Dynamic participation: it must be easy for new users to register in to the network .[8]

II. DP2AC:DISTRIBUTED PRIVACY PRESERVING ACCESS CONTROL

DP2AC is a novel token-based approach to achieve distributed privacy-preserving access control in single-owner multi-user sensor networks. In DP2AC, user purchases token from network owner. Using this token it can access sensed data from sensor network. Once validating the token, the sensor node provides the user with an appropriate amount of requested data. DP2AC is processed in three phases initialization, withdrawal and spending phase. In initialization phase network considers about security parameters .DP2AC is based on blind signature. so by blind signature the actual signer of the query will not be known. This blind signature depends on RSA. Network owner creates RSA public key and private key. < n, e > is the public key and <d> is the private key. Here, n is the product of two distinct random primes p and q; e, $1 < e < \phi$, is co prime to $\phi = (p-1)(q-1)$; d, $1 < d < \phi$, satisfies $ed = 1 \bmod \phi$. The modulus n is at least 1024 bits long for sufficient security. By keeping <p, q, d> as confidential to himself, he publishes the public key. Prior to network deployment, each sensor node is preloaded with the public key. By using TESLA protocol it broadcasts public key to all sensor nodes. Purchasing of token is done in withdrawal phase. Network user needs to buy some tokens from the network owner to access the sensors. Each token in DP2AC consists of a λ bit random integer and also signature of network owner will be present. λ is a system parameter partially determining DP2AC's correctness.

Tokens can be purchased in many ways. Consider as an example user Alice who can purchase a token from the network owner through the following procedures:

i) Alice picks a λ bit random integer m, $0 \le m \le 2\_-1 \le n - 1$, as well as a random secret integer k satisfying $0 \le k \le n-1$ and gcd(n,k) = 1.

ii) Alice sends $m^* = h(m)k^e \bmod n$ along with her payment information to the network owner, where $h(\cdot)$ denotes a good hash function such as SHA-1.

iii) The network owner returns $\sigma^*_m = (m^*)^d \bmod n$ to Alice after verifying her payment information.

iv) Alice computes $\sigma_m = k^{-1} \sigma^*_m \bmod n$, which is the network owner's RSA signature on h (m).

v) Alice records the pair $<m, \sigma_m>$ as token.

The network owner is trusted to return a correct σ^*_m. It is easy to see that σm is a valid RSA signature on h (m), $\sigma_m = k^{-1} \sigma^*_m = k^{-1} h(m)^d k^{ed} = k^{-1} h(m)^d k = h(m)^d \bmod n$. Due to the blinding factor k, the network owner cannot derive h(m) and σ_m from m* . In other words, the network owner cannot link it to Alice.

Each token corresponds to a financial value and based on that appropriate amount of sensed data can be purchased. By using different RSA public and private key pair multi-denomination token can be made. For each denomination different pairs are used. Although unable to precisely associate individual tokens with the identities of their holders, the network owner may still narrow down the holder of a particular token to the users who purchased tokens. Because of this number of token buyers will be reduced. So to overcome this tusted third party was introduced. User can relay on trusted third party to purchase token. So here payment information is not directly submitting to network owner. Third phase of DP2AC is token spending where the user spend token to access data from sensor node. After receiving token it undergoes two verification processes. First verification process is a standard RSA signature verification. If it is true it goes under second verification process. Second verification process is to ensure that the token is not used before. Only then the sensor node provides appropriate amount of requested data. The owner of the token will not be known to sensor node.

User can access sensor node only when he has token. Tokens are generated with the owner's public key. Then only authorized user can access the sensor network. Sensor can't identify the owner of the token. So it follows privacy preserving access control. A sensor node has to permanently store the entire tokens that he had already processed. By that he can avoid token reuse. In order to achieve privacy-preserving access control, the use of blind signatures in token generation ensures that tokens are publicly verifiable yet unlinkable to user identities.

III. PRICCESS

This protocol was introduced in order to compensate disadvantages in the DP2AC.DP2AC was not so efficient by many aspects.1) network wide flooding is required once token-reuse is run.2) local memory is needed for storing the token. After using token it has to be stored permanently in order to identify the attacker. So it is impractical.3) with one token user can access only once. So number of queries allowed in DP2AC is very limited.4) at a time only one node can be accessed by a user. These limits leaded the way to establish Priccess protocol.

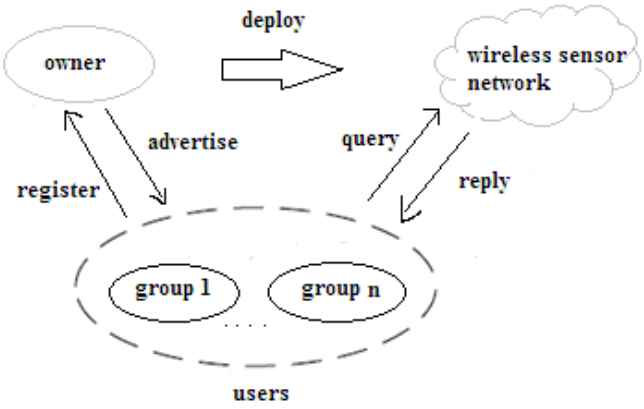

Fig 1: Priccess protocol

The main participants in this protocol are network owner, sensor node, network users. In fig 1: we can see the involvement of all these participants. Initially user registers with the owner. Owner is the one who responsible for grouping the user according to their access privileges. Network users in the same group have the same access privilege. Access privilege for each user will be different. For example, in a battle field a soldier only needs to access the data related to his task but a rank officer often requires information gathering for an overall manoeuvre, so access privilege for rank officer will be greater compared to soldier. [10]The network owner maintains group access list pool which contains user identity and his access privilege. In this protocol, initially the network owner submits its public key and identity information to the CA. And the CA verifies the identity of the network owner upon registration and then generates a public-key certificate for it. The certificate consists of the network owner's public key and identity information plus other information (e.g., an indication of the period of validity of the certificate, some information about the CA), with the whole block signed by the CA. every network user, and also registers with the CA through submitting its public key and its identity information. The CA verifies the identities of each user and then generates a public-key certificate for each user. Each certificate consists of the network user's public key plus other information (e.g., an indication of the period of validity of the certificate, some information about the CA), with the whole block signed by the CA. The user delivers its public key certificate payment information and targeted access privilege to the network owner. Fig 2 gives an idea about the certification process between the user, owner and the certification authority. Owner groups the user according to the access privilege. Group access list pool contain group id which is to identify the group, next content is group access privilege mask .its a bit map where each bit represent specific information. eg: first parameter .'1' indicates light parameter available for all members in this group. Group access list pool also includes group member's public key and public key expiration time. This group access list pool will be advertised to all users.

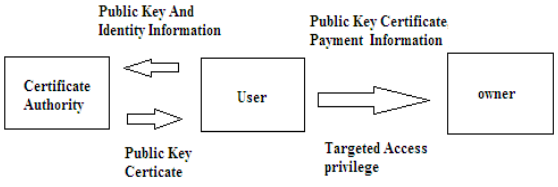

Fig 2: Initialization phase

After initialization phase, user sends query to sensor nodes. the query includes targeted region which is to specify the specific region of nodes to where we are sending, time stamp which is to resist the replay attacks and it contain the request in detail. User sends its query to sensor node after performing ring signature algorithm. The query is signed by a subset of group to convince the verifier that the signer of the signature is authorized

one in a specific group but its identity is not disclosed. Thus it protects the anonymity of the signer. 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. 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 size r with probability greater than 1/r.

By receiving the message from user sensor node first checks its timestamp. Then it checks its request and group id. The verification of timestamp is to confirm whether it has undergone any replay attacks. After all these verification it checks the validity of the signature. If all went true, it gives response to user. Using elliptic curve Diffie Hellmann key exchange secure channel is implemented between network user and sensor nodes. By this mechanism it protects the integrity of query and response command transferring between user and sensor node. When a new user registered, the owner sends new user joining message to all other network users in a group who having same access privilege. When a user tries to revoke, the network owner needs to sign a user revocation message and it then advertise by using its private key. After getting this message it deletes the details of that specified user. By this it proves that a user can dynamically participated without any difficulties.

In Priccess, Elliptic Curve Cryptography (ECC) is chosen because ECC has a significant advantage. Some features are low computation overhead, small key size, and compact signatures. [11] The network owner can restrict each network user's activities by group division. In order to pass the signature verification of sensor nodes, each user has to register to the CA and the network owner, and then the network owner relegates him to a group according his access privilege. A network user needs to sign the query command with his private key and the public keys of all chosen group members. By this it enforce strict user authentication. The use of ring signature ensures user privacy-preserving. No one can know the actual signer of a ring signature, even if all of the private keys of the parties of the ring are known. An actual signer can deny that he has made a ring signature, even if his private key is known. An authorized network user uses a ring signature technique to authenticate the query command. The sensor nodes know the public keys of all group members, and thus can verify the message Therefore, an adversary cannot modify the query command .Thus it protects the integrity of the message. Only the public key of the network owner and the group access list pool are pre-loaded on every node. So by compromising nodes adversary will be getting only the public key of the network owner and the group access list pool. Without getting private key of the user the adversary can't impersonate the user .so by compromising nodes it can't impersonate users. The usage of timestamp in query ensures the freshness of the message. Thus it follows all requirements of privacy preserving access control.

IV. CONCLUSION

User access the WSN in order to get the monitored data from sensor nodes. Everyone concentrates on authentication of each user, but most probably everybody miss to concern about to protect the privacy of user. Here we introducing two schemes DP2AC and priccess that concern about the privacy preserving access control. In DP2AC, user purchases token from network owner. Using this token it can access sensed data from sensor network. Once validating the token, the sensor node provides the user with an appropriate amount of requested data. Because of different reasons this scheme was not so efficient. Priccess is a new approach that overcomes the disadvantages of DP2AC. In priccess users who have same access privileges are assigned to same group. When user sends query on behalf of group to sensor node, so node will not be able to identify the identity of user. The signature can be verified by the node as coming from someone authorized without exposing the real signer. Thus it protects the privacy preserving access control.

V. REFERENCES

[1] Daojing He, Jiajun Bu, Sencun Zhu,Sammy Chan and Chun Chen, "Distributed Access Control with Privacy Support in Wireless Sensor Networks", IEEE transaction on wireless communication, october 2011

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

[3] H. Wang and Q. Li, "Distributed user access control in sensor networks," in Proc. IEEE/ACM DCOSS, pp. 305–320, 2006

[4] 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

[5] D. He, Y. Gao, S. Chan, C. Chen, and J. Bu, "An enhanced two-factor access control scheme in wireless sensor networks," Ad Hoc & Sensor Wireless Networks, vol. 10, no. 4, pp. 361–371, 2010

[6] K. Ren, W. Lou, K. Kim, and R. Deng, "A novel privacy preserving authentication and access control scheme for pervasive computing environment,"in IEEE Transactions on Vehicular Technology, 2006

[7] B. Carbunar, Y. Yu, L. Shi, M. Pearce, and V. Vasudevan, "Query privacy in wireless sensor networks," in SECON '07, San Diego, CA, USA, June 2007, pp. 203–212.

[8] Jef Maerien,Sam Michiels,Christophe Huygens,Danny Hughes and Wouter Joosen "Access control in multi-party wireless sensor networks "iMinds-DistriNet, KU Leuven,3001 Leuven ,Belgium

[9] Archana Bharathidasan,Vijay Anand Sai Ponduru"Sensor Networks:An Overview " Department of computer science University of California,Davis,CA 95616

[10] H. Wang, B. Sheng, and Q. Li, "Elliptic curve cryptography based accesscontrol in sensor networks," Int'l J. Security and Networks, vol. 1, no.3-4, pp. 127–137, 2006.

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