ISSN No: 2454-9614

An Enhanced Privacy Access and Accountable Security Management in Wireless Sensor Networks

S. Mano Shalini[a], M. Navaneetha[a*], M. Shivakumar[a,b]

[a)] Department Of Computer Science and Engineering, V.S.B Engineering College,
Karur,Tamilnadu, India.
[b)] Department Of Computer Science and Engineering, CMRIT,
Bangalore, Karnataka, India.

*Corresponding Author: S. Mano Shalini
E-mail: mailshalu01@gmail.com

Received: 10/11/2015, Revised: 12/12/2015 and Accepted: 07/03/2016

Abstract

With expeditious development and extensive use of wireless sensor networks (WSN), it is essential to enhance the security and privacy of WSN which will diversify its application areas. The major concern is data communication among the sensor nodes, users and vice-versa. The performance of the network can be evaluated by using privacy and security prime factors. The trust among the entities involved in the WSN is rather very limited. On account of this, multiple protocols have been proposed in the recent research by considering factors of accountable access control, sophisticated user privacy, data security, communication security and also to defend against various attacks. This paper presents the overall analysis and review of the recent research works along with the proposed architecture of an integrated approach to privacy and security with its simulated resul*ts.*

Keywords: WSN, Access control, DOS, IAPS, Diffie-Hellman, Group Signature.

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Wireless sensor network refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. The topology of the WSNs can vary from a simple star network to an advanced multi-hop wireless mesh network. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. Users of the wireless sensor networks can access the information at any time from any place and the owners of the WSN are responsible for monitoring and control of the entire scenario. The challenges in WSN are the factors of Energy Efficiency, Responsiveness, Robustness, Self-

Configuration and Adaptation and Scalability, Heterogeneity, Systematic Design, Privacy and Security. Past research in WSN focused mainly on data security **[1]** and access control but the integrated approach of all the issues is still an open challenge. Pin pointing the dishonest users, unlinking the user transactions, privacy and security of the users, and accountable access control between the network owners and users are the key concepts focused on this paper. The additional challenge of temporal privacy **[2]** and location privacy is also focused to gain a better insight to the integrated approach. Addressing the above challenges with an optimal solution can increase the demand of WSN deployment in scattered applications.

The rest of the paper is organized as follows. The comprehensive review of the survey of the literature is elaborated along with its pros and cons in section **2.** Section **3** explains the proposed architecture obtained based on the literature survey. The simulation results and evaluation are analyzed in the section **4**. Section **5** concludes the paper.

2. Literature review

In the literature, various protocols have been proposed to address the security and privacy challenges faced in different aspects of WSN.**[3]** Kui Ren and Wenjing Lou suggested a suite of authentication and key agreement protocols named PEACE, a sophisticated privacy-Enhanced yet Accountable security framework, which enforces a strict access control against the intruders and malicious users. The group signature scheme is tailored with a variation that is proposed in **[4]** for the PEACE protocol. Although the proposed protocol is resistant to different kinds of attacks like DOS attacks, bogus injection attacks but it incurs communication overhead and computational cost in signature generation and verification. The security of an offline trusted third party (TTP) is completely based on assumption and in reality it may result in a compromise of itself.

To address the challenges of data security and physical compromise of sensor nodes**[5]** Shucheng Yu proposed distributed data access control scheme which depends relies on the cryptographic element called Attribute based encryption(AEB).Sensor data attributes are encrypted based on AEB and it focuses on fine-grained access control(FDAC) and is impervious to node compromise and resistant to collusion. Other security problem of data authenticity and integrity is not explicitly addressed.

A complete effort on protecting and preserving user identity when user wants to access data from a network was proposed **[6]** by Daojing He and his fellow members with a prices-privacy preserving access control. A ring signature technique is incorporated into the design of prices protocol and also involves the usage of elliptic curve cryptography. It addresses the authenticity and integrity problem which was not explored in **[5]** but the secure storage of data in sensor nodes is out of scope. Along with, it provides way for the fraudulent network users to launch DOS attacks without disclosing his identity.

Further research focused on privacy preserving access control suggested by Rui Zhang **[7]** which was an extended research of proposed in **[5]**. Rui Zhang presents a Distributed Privacy-Preserving Access Control scheme

DP2AC which is a token based approach as it involves the purchase of token from network owners and the sensor nodes in turn respond to the users upon validating the tokens. The backbone of this protocol relies on the use of blind signature concept in token verification. Even though it resulted in better result with token reuse detection (TRD) which uplifts the privacy access some diverse attacks are still an open challenge. **[8]**Daojing contributed with SeDrip, a secure, lightweight protocol for secure data discovery and dissemination. This is particularly resistant to DOS attacks which was the demerit in **[6][7].**The past research targeted on data dissemination and resulted in Drip,DIP **[9]** and no importance to security mechanisms was imposed. The design of SeDrip was based on signed Merkle hash tree and is further enhanced with a digital signature to ensure the authentication of the disseminated data and message specific puzzle approach to resist against the adversaries launching the Denial-Of-Service (DOS) attacks. It incurs computational cost and overhead as it involves multiple techniques put forth together.

Specific to a particular application perspective **[10]** Hongzhi Guo, and Zhi Sun suggested a new self-contained wireless sensor framework based on magnetic induction (MI) technique, which enabled the real-time and in-situ monitoring in oil reservoirs. The existing challenges such as high path loss, infeasibility in radiating wireless signals and short lifetime of the system were concentrated in his proposal with a two-layered architecture, micro wireless sensors forming the first layer and the base station forming the second layer. The transfer of energy and information between the two layers takes place by means of dipole antenna possessing the high transmission power. The transfer is bi-directional both uplink and downlink to be suitable for use in the application. The entire framework still fails as it covers only limited coverage area and lacks energy efficient networking.

[11] Baojiang Cui proposed a key management protocol in order to enhance security and protect from WSN from various attacks. As single keying mechanism cannot successfully meet the security needs, **[11]** suggested four kinds of key establishment (Individual key establishment, Pair-wise key establishment, cluster key establishment and group key establishment) to be derived from initial master key and the entire protocol is based on diffie-hellman algorithm. The master key protection, key revocation mechanism and the authentication mechanism is based on one-way hash function. The proposed protocol enhances the survivability of nodes, defends against attacks like Sybil attacks, HELLO flood attack, sinkhole attack and wormhole attacks. Although the protocol enhances the network security it can be further improved by avoiding the storage of master key in the sensor nodes which will produce critical effects to the entire network if a single node is captured.

In **[12]** Developed a novel protocol named APAC-Accountable and privacy enhanced access control similar to one proposed in **[6] [7].**It enforces strict access control, user privacy protection and auditing of misbehaving and malicious users. It includes a trust and key management model among the law authority, network owners and group of users. This fig.1 illustrates the management of key between the entities as there is no trusted third party involved in this concept and the trust between the entities is also limited. It works based on the principle of separation of duties.

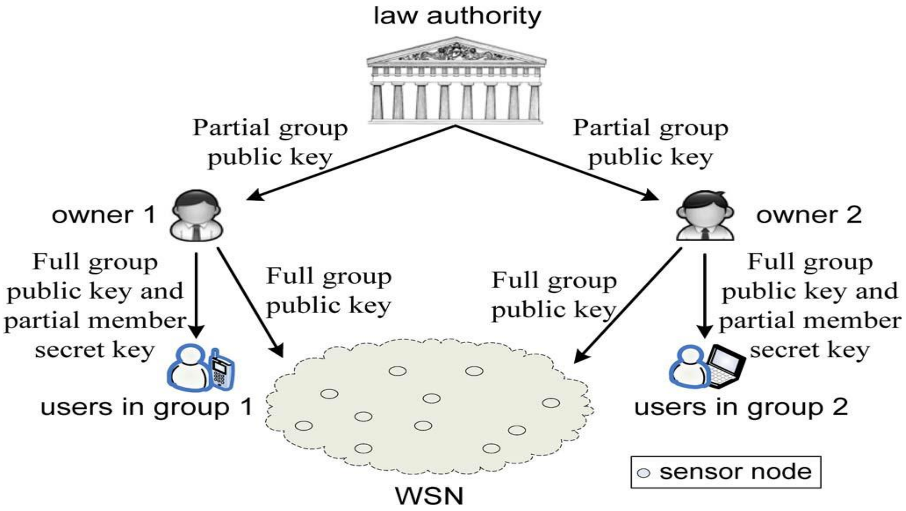


Fig.1 **[12]** Trust and key management model of APAC.

PAC protocol involves verification of new user joining the network, receiver verification, key establishment and user revocation and tracing and includes the group signature schemes with a redesign of key generation and tracing phases. Although this approach produces better results it still lacks its importance in the source location privacy and also the privacy of some temporal information.

2.1 Summary of literature review

From the above survey it is reviewed that some of the protocols like PEACE, APAC does not provide resistant to attacks even though the other parameters of security and privacy is preserved. This gives way to the proposal of an integrated approach to privacy and security with an enhanced mechanism of integrating some additional aspects of privacy factors that defends against some important attacks like DOS, wormhole attack and other similar attacks which is explained in the next section.

3. Proposed Architecture

In this section, an idea of integrated approach to privacy and security (IAPS) is proposed based on the above survey and its reviews. Based on the analysis of the literature, different protocols were enforced which contributed to one aspect but compromises in other factor, the outcome of which is the integration of strict access control to data, security mechanism enforcement, user privacy, privacy to temporal information and spatial privacy. Strict access control is to provide control over the data from intruders and malicious users. Security mechanism is mainly enforced to prevent the data from attacks like Denial of service, bogus injection attack, Wormhole attacks and many of its kind. User privacy focuses to hide the association between the user identity and the data the user accesses. It also enforces privacy among the different group of users accessing the wireless sensor networks by means of tailoring some aspects of the group signature scheme. The IAPS involves the enhancement of APAC **[12]** by including the adaptive buffering algorithm called RCAD (Rate-controlled adaptive delaying) **[2]** that forwards data based on buffer saturation.

This hides the time of origin of the data packet. Further enhancement can be done by introducing the concept of source and sink location privacy to protect from the local eavesdropper. Apart from the content of the message, privacy should also be enforced on the contextual information such as location of the sink, time of origin of packet and such details. The overall architecture is presented in the following figure where the IAPS can be implemented to enforce security and privacy parameters in wireless sensor networks.

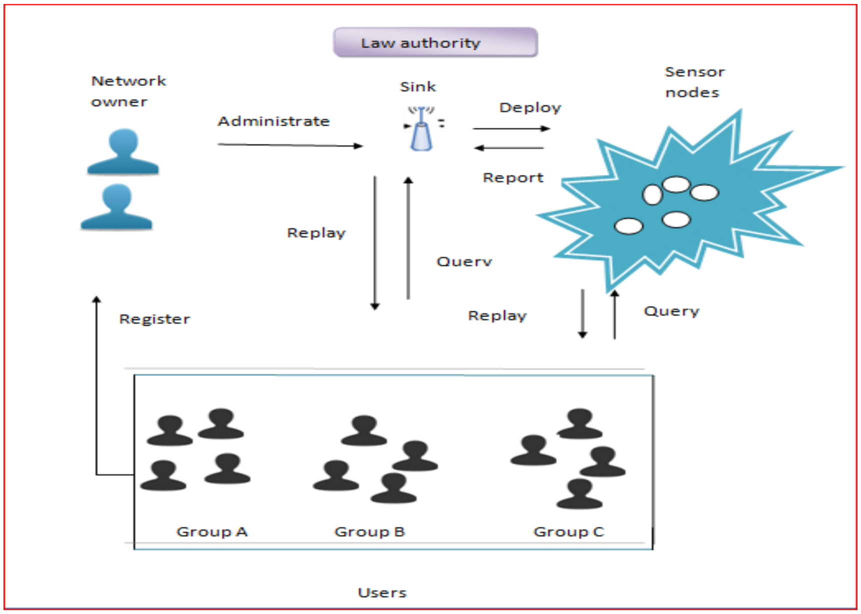


Fig. 2 Architecture

3.1 Network Architecture

WSN consists of many users, a large number of resource-constrained sensors and a sink one or more network owners and an off-line law authority. The sensors report their sensed data to the sink (administrated by one or more network owners) and users in response to queries. After registering to one or more network owners, network users use access devices such as smart phones or Laptop PCs to access the sensed data by sending queries to the sink or the targeted nodes. The network owners bootstrap the keying materials for access devices to enforce the access control policy. According to the agreement, each network owner has specific access privilege of his/her own.

3.2 Trust and Key Management Model of IAPS

The trust and key management model adopted users who have registered to the same network owner are organized in a group, among which the network owner acts as the group manager. Our protocol does not assume the existence of a trusted third party, and is therefore more practical. The above key management scheme is based on the separation of duties principle and has several salient features. First, from network access control point of view, each authorized user is assigned a member secret key to generate a legitimate access credential, i.e., the signature of a fresh query. The legitimacy of this access credential is verified by the sink and each node through group public key. Thus, centralized and distributed access security is guaranteed. Second, it divides group private key and the identities of users among two autonomous entities the group manager and the law authority.

3.3 IAPS Protocol

IPAS consists of four phases - system setup and new user joining phase, query generation and verification phase, key establishment phase and user revocation and tracing phase.

✓ *System setup and new user joining phase*

It involves the generation of partial group keys by the law authority and also the generation of Full group public key by the network owner .It includes the authentication of new user by the generation of partial member secret key to the group manager and also sends to network owner (secure transmission)

✓ *Query Generation and Verification phase*

This phase involves the creation of appropriate query request and generation of group signature and a collision-resistant hash function is applied along with timestamp. It includes the sending query request to targeted nodes/sink and also receiver verification and response is done if timestamp, group validity and group public key is valid.

✓ *Key Establishment Phase*

In this phase a session key is established between a user and the sink to protect data communication against attacks. It is implemented by using an Elliptic Curve Diffie-Hellman (ECDH) technique which is based on mutually authenticated key exchange.

✓ *User Revocation and Tracing phase*

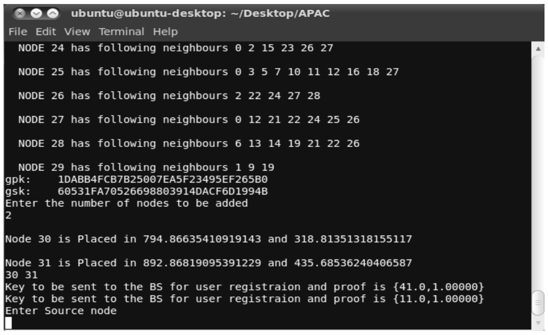
In this phase the network owner sets the minimum subscription period of the network service. Upon the expiration of each minimum subscription period, each unrevoked user and sensor node will await the User Revocation Message from the network owner. The law authority decides to track the particular attacker that is responsible for a certain network access. Once tracked it communicates to the network owner via secure channel

3.4 Analysis and Evaluation

The performance of proposed system is highly efficient compared to the existing system. Security evaluation is done by analyzing its fulfilment of the security requirements i.e., correctness, enforceability, anonymity, unlink ability, traceability. The following four metrics to evaluate IAPS, namely, memory overhead, execution time of each operation of IAPS, message overhead, and energy overhead.

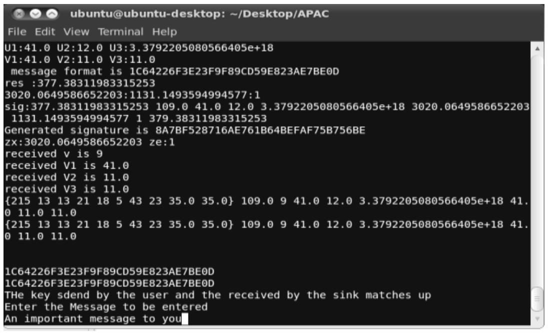
4. Simulation Results and Evaluation

In this section, we use simulation to evaluate the performance of our techniques in terms of throughput, End to end delay and packet delivery ratio. We use the following four metrics to evaluate IAPS, namely, memory overhead, execution time of each operation and energy overhead. The memory overhead refers to the amount of data space consumed by the real implementation. For our purpose, the simulation code was written in OTCL, and we assume error free and collision-free packet transmissions.


ubuntu@ubuntu-desktop: ~/Desktop/APAC
File Edit View Terminal Help

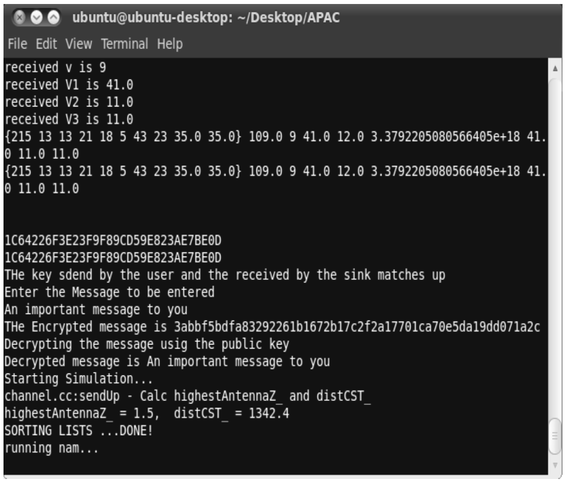
```
  NODE 24 has following neighbours 0 2 15 23 26 27

  NODE 25 has following neighbours 0 3 5 7 10 11 12 16 18 27

  NODE 26 has following neighbours 2 22 24 27 28

  NODE 27 has following neighbours 0 12 21 22 24 25 26

  NODE 28 has following neighbours 6 13 14 19 21 22 26

  NODE 29 has following neighbours 1 9 19
gpk:    1DABB4FCB7B25007EA5F23495EF265B0
gsk:    60531FA70526698803914DACF6D1994B
Enter the number of nodes to be added
2

Node 30 is Placed in 794.86635410919143 and 318.81351318155117

Node 31 is Placed in 892.86819095391229 and 435.68536240406587
30 31
Key to be sent to the BS for user registraion and proof is {41.0,1.00000}
Key to be sent to the BS for user registraion and proof is {11.0,1.00000}
Enter Source node
```

Fig 3. (a) Generation of group private key and group session key


ubuntu@ubuntu-desktop: ~/Desktop/APAC
File Edit View Terminal Help

```
U1:41.0 U2:12.0 U3:3.3792205080566405e+18
V1:41.0 V2:11.0 V3:11.0
 message format is 1C64226F3E23F9F89CD59E823AE7BE0D
res :377.38311983315253
3020.0649586652203:1131.1493594994577:1
sig:377.38311983315253 109.0 41.0 12.0 3.3792205080566405e+18 3020.0649586652203
 1131.1493594994577 1 379.38311983315253
Generated signature is 8A7BF528716AE761B64BEFAF75B756BE
zx:3020.0649586652203 ze:1
received v is 9
received V1 is 41.0
received V2 is 11.0
received V3 is 11.0
{215 13 13 21 18 5 43 23 35.0 35.0} 109.0 9 41.0 12.0 3.3792205080566405e+18 41.
0 11.0 11.0
{215 13 13 21 18 5 43 23 35.0 35.0} 109.0 9 41.0 12.0 3.3792205080566405e+18 41.
0 11.0 11.0


1C64226F3E23F9F89CD59E823AE7BE0D
1C64226F3E23F9F89CD59E823AE7BE0D
THe key sdend by the user and the received by the sink matches up
Enter the Message to be entered
An important message to you
```

Fig 3. (b) Signature generation and receiver verification and addition of new nodes to the network


ubuntu@ubuntu-desktop: ~/Desktop/APAC
File Edit View Terminal Help

```
received v is 9
received V1 is 41.0
received V2 is 11.0
received V3 is 11.0
{215 13 13 21 18 5 43 23 35.0 35.0} 109.0 9 41.0 12.0 3.3792205080566405e+18 41.
0 11.0 11.0
{215 13 13 21 18 5 43 23 35.0 35.0} 109.0 9 41.0 12.0 3.3792205080566405e+18 41.
0 11.0 11.0


1C64226F3E23F9F89CD59E823AE7BE0D
1C64226F3E23F9F89CD59E823AE7BE0D
THe key sdend by the user and the received by the sink matches up
Enter the Message to be entered
An important message to you
THe Encrypted message is 3abbf5bdfa83292261b1672b17c2f2a17701ca70e5da19dd071a2c
Decrypting the message usig the public key
Decrypted message is An important message to you
Starting Simulation...
channel.cc:sendUp - Calc highestAntennaZ_ and distCST_
highestAntennaZ_ = 1.5,  distCST_ = 1342.4
SORTING LISTS ...DONE!
running nam...
```

Fig 3. (c)Encryption and decryption of message between the communicating nodes

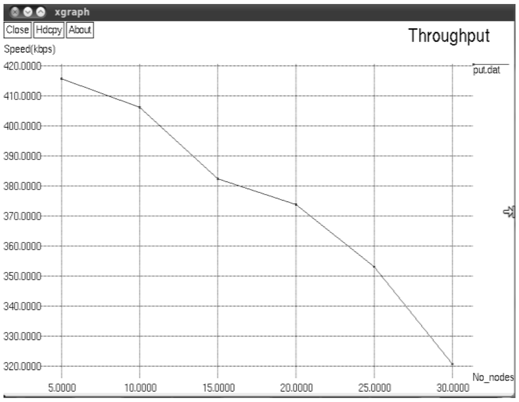


Fig 3.(d)Graph showing the end to end delay when the number of node increases

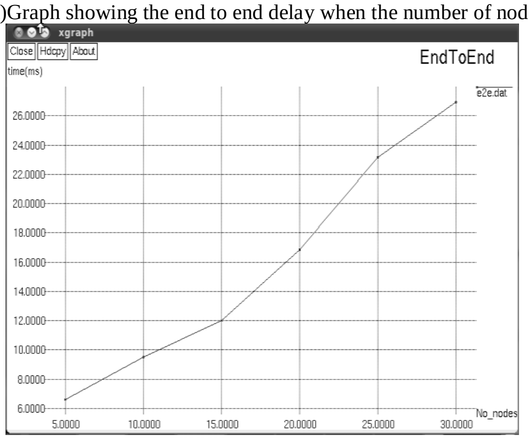
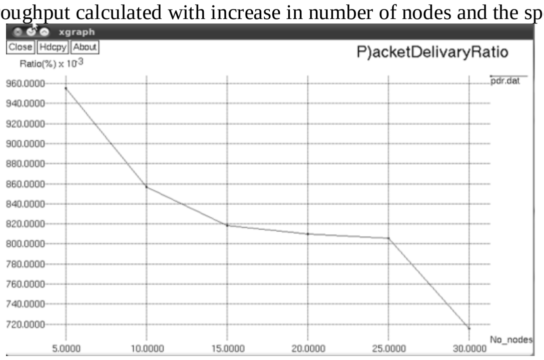


Fig 3. (e) Throughput calculated with increase in number of nodes and the speed of data transmission



5. Conclusion

In this paper, an in-depth analysis is done by considering multiple approaches developed with importance given to security and privacy issues in accessing a WSN. The deployment of WSN in multiple fields of application can be effective only when it is secure and defends against attacks from malicious users and also when user privacy is preserved. Focusing on authenticity, integrity, access control and other security vulnerabilities multiple proposals has been portrayed in the literature along with better experimental results.

References

[1] Daojing He, Sammy Chan, Shaohua Tang, and Mohsen Guizani" Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks",in IEEE 2013.

[2] Pandurang Kamat, Wenyuan Xu, Wade Trappe, Yanyong Zhang,"Temporal privacy in wireless sensor networks"in IEEE 2007

[3] Kui Ren1 and Wenjing Lou2, "A Sophisticated Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks" in IEEE 2008

[4] D. Boneh and H. Shacham, "Group signatures with verifier-local revocation," in ACM conference on Computer and Communications Security (CCS), 2004, pp. 168–177.

[5] Shucheng Yu, Member, IEEE, Kui Ren, Member, IEEE, and Wenjing Lou, Senior Member, IEEE," FDAC: Toward Fine-Grained Distributed Data Access Control in Wireless Sensor Networks",IEEE transactions on parallel and distributedsystems,2011

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

[7] Rui Zhang, Student Member, IEEE, Yanchao Zhang, Senior Member, IEEE, and Kui Ren, Senior Member, IEEE," Distributed Privacy-Preserving Access Control in Sensor Networks",IEEE transactions on parallel and distributed systems,2012

[8] Daojing He, Sammy Chan, Shaohua Tang, and Mohsen Guizani," Secure Data Discovery and Dissemination based on Hash Tree for Wireless Sensor Networks",IEEE transactions on wireless communications,September 2013

[9] K. Lin and P. Levis, "Data discovery and dissemination with DIP," inProc. 2008 ACM/IEEE IPSN, pp. 433–444.

[10] Hongzhi Guo and Zhi Sun ,"Channel and Energy Modeling for Self-Contained Wireless Sensor Networks in Oil Reservoirs",IEEE transactions on wireless communications,April 2014

[11] Baojiang Cui,ZiyueWang, Bing Zhao, Xiaobing Liang, and Yuemin Ding3,"Enhanced key management protocols for wireless sensor networks" Hindawi Publishing Corporation,September 2014

[12] Daojing He, Sammy Chan, and Mohsen Guizani,"Accountable and privacy-Enhanced access control in wireless sensor networks"IEEE transactions on wireless communications,January 2015