ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

Authentication and Secure Data Access Privacy in Wireless Sensor Networks

Indumathi G, Sylvia Sharon D

Department of Electronics and Communication Engineering, Mepco Schlenk Engineering College, Sivakasi, India.

Department of Electronics and Communication Engineering , Mepco Schlenk Engineering College, Sivakasi, India.

ABSTRACT— An authentication and secure data access privacy in wireless sensor network enforces strict access control so that the sensed data will not be obtained by unauthorized users. A secure data access privacy involves three participants namely, the network owner, all sensor nodes and the network users. The users who want to access the data firstly register to the network owner. A network user signs a query command and then sends the signed query command to the sensor nodes. Users purchase tokens from the network owner whereby to query data from sensor nodes which will reply only after validating the tokens. The signature can be verified by its recipient as coming from someone authorized without exposing the actual signer. It ensures that only authorized users can gain access to read data from the nodes. The paper investigates the security related issues and challenges in wireless sensor networks to identify malicious activities by using a low power FPGA.

KEYWORDS— Authentication, Privacy, Secure Data Access, Wireless Sensor Network.

I. INTRODUCTION

Wireless Sensor Network (WSN) is formed by a large number of networked sensing nodes. In order to model analytically a WSN and it usually leads to oversimplified analysis with limited confidence. Besides, deploying test-beds supposes a huge effort. Therefore, simulation is essential to study WSN. However, it requires a suitable model based on solid assumptions and an appropriate framework to ease implementation on FPGA. However, detailed models yields to scalability and performance issues, in the large number of nodes, have to be simulated using the software ModelSim Altera. Therefore, the trade off between scalability and accuracy becomes a major issue when simulating wireless sensor networks.

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 requests to get authenticated and access the information stored in the sensor nodes. But, it is in-efficient, not scalable, and vulnerable to many potential attacks along the long communication path. On the other hand, in distributed access control [2], the authorized users can enter the sensor field to directly access data on sensor nodes without involving a base station. This approach can avoid weaknesses 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.

In Distributed Privacy Preserving Access control in sensor networks, the owner and users of a sensor network may be different, which necessitates privacy-preserving access control. On the one hand, the network owner need enforce strict access control so that the sensed data are only accessible to users willing to pay. On the other hand, users wish to protect their respective data access patterns whose disclosure may be used against their interests. In [3], the author presents DP^2AC, a Distributed Privacy-Preserving Access Control scheme for sensor networks, which is the first work of its kind. Users in DP^2AC purchase tokens from the network owner whereby token generation ensures that tokens are publicly verifiable yet not linkable to user identities, so privacy-preserving access control is

achieved. A central component in DP^2AC is to prevent malicious users from reusing tokens, for which they propose a suite of distributed token reuse detection (DTRD) schemes without involving the base station. These schemes share the essential idea that a sensor node checks with some other nodes whether a token has been used, but they differ in how the witnesses are chosen. They thoroughly compare their performance with regard to TRD capability, communication overhead, storage overhead, and attack resilience. The efficacy and efficiency of DP^2AC are confirmed by performance evaluations.

In this paper, we propose an access control protocol based on Elliptic Curve Cryptography (ECC) for sensor networks. Our access control protocol accomplishes node authentication and key establishment for new nodes. Our access control protocol cannot only identify the identity of each node but also differentiate between old nodes and new nodes. In addition, each new node can establish shared keys with its neighbours during the node authentication procedure. Compared with conventional sensor network security solutions, our access control protocol can defend against most well-recognized attacks in sensor networks, and achieve better computation and communication performance due to the more efficient algorithms based on ECC than those based on RSA.

A privacy – preserving access control in WSNs should satisfy the following requirements: (1**) User Authentication:** user authentication needs to be enforced for sensor data in WSNs so that the information will not be obtained by unauthorized entities; (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 sender; (3) **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) **Node Compromise Tolerance:** the adversary cannot impersonate any network user by compromising nodes; (5) **Scalability:** the protocol should be efficient even in a large scale WSN with many users and many nodes. (6) **Freshness:** to defend against replay attacks, a node should have the capability of freshness checking for any query message; (7) **Limits of Access Privileges:** access restriction may be enforced for users with different access privileges; (8) **Dynamic participation:** new users can easily join the network, and users can easily be revoked when they are expired. (9) **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. (10) **Efficiency:** Due to the limited energy, processing and storage resources of sensor nodes, a cryptographic technique should be efficient.

A central component in distributed privacy- preserving access control (DP^2AC) is to prevent malicious users from reusing tokens, for which we propose a suite of distributed token reuse detection schemes without involving the base station. These schemes share the essential idea that a sensor node checks with some other nodes whether a token has been used, but they differ in how the witnesses are chosen. We thoroughly compare their performance with regard to TRD capability, communication overhead, storage overhead, and attack resilience. The efficacy and efficiency of DP^2AC are confirmed by detailed performance evaluations.
Designing a distributed privacy-preserving access control in WSNs is a non-trivial task because wireless networks are vulnerable to attacks and sensor nodes are resource constrained.

A central issue in DP^2AC is detecting reused tokens. Each token in DP^2AC is essentially a random bit string with no relationship to user identities. Malicious users thus may have financial interest in reusing tokens at different senor nodes without worrying about being caught, which would result in substantial financial losses of the network owner if there are many malicious users. The most straight forward solution for token-reuse detection (TRD) is to let each sensor node check with an in-network base station that a token was not spent and otherwise reject the data access request. To do so, the base station need record every token submitted by sensor nodes. This centralized method has several limitations although it can detect every token- reuse attempt. First, the base station is the single point of failure: once compromising the base station, malicious users can freely reuse tokens. Second, if there are many tokens to verify, sensor nodes close to the base station would deplete their energy quickly for relaying TRD requests and replies. Third, the base station may not exist in our target scenarios. So, we propose a suite of Distributed TRD (DTRD) techniques and thoroughly compare their performance with regard to TRD capability, communication overhead, storage overhead, and attack resilience.

We propose simple hash based message authentication and integrity code algorithm for wireless sensor networks. The proposed scheme uses pre-shared secret key which is obtained from Elliptic Curve Diffie Hellmann (ECDH) key exchange algorithm, and is based on modified SHA-1(mSHA-1) hash function which helps to compute message authentication code for given messages. We suggest two scenarios depending on scale of the network, and also analyze security of the proposed algorithm. This algorithm provides both integrity and authenticity of a message with only one hash value.

II. RELATED WORK

Some approaches make use of the simple operations such as one-way hash functions and exclusive-OR operations to enable efficient access control. In addition, the least

privilege scheme can be used to achieve a specific type of access control, in which a user can only access the sensor data at a predetermined physical path in the field. We observe that all these works just focus on designing access control modules for WSNs, but do not pay attention to protecting user's identity privacy when a user is verified by the network for data accesses. DP^2AC is not efficient in three aspects. First, network- wide flooding is required once token-reuse detection runs. Second, for token reuse detection, the protocol needs to store tokens in local memory of every node. Once a token is used, it is permanently stored. Since a node has limited memory capacity. Also, as each token only allows the user to access the nodes once, the number of user queries allowed in DP^2AC is limited. Third, users can only access one node at a time, while majority of actual access requests are targeted to many nodes via broadcast. We have considered using ring signature to achieve distributed privacy-preserving access control.

III. OVERVIEW OF DISTRIBUTED PRIVACY PRESERVING ACCESS CONTROL

Distributed privacy –preserving access control in WSNs 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 of each group. Let assume a user U_i, belongs to the group with the identity gid. The number of group members is assumed to be N. The network owner advertises the group access list pool to all users. In addition, the group access list pool is pre-loaded on each node. U_i wants to send a query command to the nodes in such a way that it remains anonymous, yet the nodes are convinced that the query command is indeed from a member of the group with the identity gid .Even though the network owner controls the whole network and has the privilege to divide users into groups, it cannot determine the actual source of the query command.

A viable approach is for U_i to send the nodes a standard digitally signed message. A digital signature scheme allows a user to sign a message with his private key such that any verifier can verify that the message originated from an authorized user. However, such a signature message will directly reveal U_i's identity. Therefore, a standard digital signature cannot be used to achieve privacy-preserving access control.

IV. OVERVIEW OF PRIVACY PRESERVING ACCESS CONTROL

In this paper, a ring signature technique is introduced to the design of privacy- preserving access control. In particular, U_i sends a query command to the sensor nodes through a ring signature algorithm. The ring signature allows a user U_i from a set of possible signers to convince the verifier that the signer of the signature belongs to the set but the identity 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. Obviously, the ring signature technique can remedy the security issues of the group signature application. But a ring signature scheme was not originally designed for distributed privacy- preserving access control; a direct application of ring signature technique is still unable to meet requirements like (3) and (6)-(9). To address these issues, some additional mechanisms are incorporated into the design of the proposed protocol.

Privacy preserving access control 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.

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. In the user query generation phase, if a user has a new query, he will need to construct the query command and the ring signature and send them to the sensor nodes. In the sensor node verification phase, 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 scope. Additionally, in privacy preserving access control, we choose Elliptic Curve Cryptography (ECC) because ECC has a significant advantage over RSA due to its computational efficiency, small key size, and compact signatures.

V. SYSTEM SETUP

A. System setup for Authentication in WSN

The system setup for Authentication in WSN consists of three kinds of participants, the network owner, sensor nodes and the network user is shown in Figure 1.

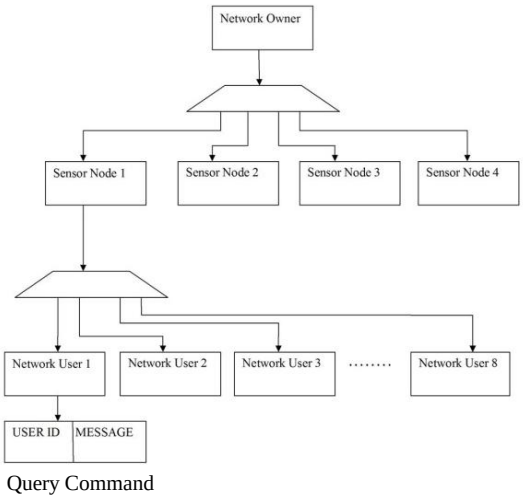

Fig. 1 System Setup for Authentication in WSN

A query command consists of unique user Id and message is generated by a network user which is sent to the network owner. The network 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 of each group. A user belongs to the group with the identity are assumed. The number of group member is assumed to be N. The network owner advertises the group access list pool to all users. In addition, the group access list pool is pre-loaded on each node. The user wants to send a query command to the nodes in such a way that it remains anonymous, yet the nodes are convinced that the query command is indeed from a member of the group with the identity.

B. *System Setup for a Single Node*

The System Setup for a single sensor Node is shown in Figure 2.

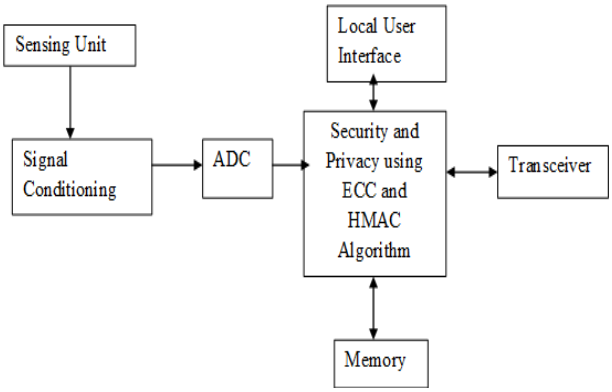

Fig 2 System Setup for a Single Sensor Node

The sensing unit generate an input signal which is sent to the ADC where continuous analog signal is sampled and converted into digital bit stream. The obtained serial data stream is transmitted using wireless sensor transmitter. The data travels through the wireless medium and also a local user interface is created. The transmitted signal is received by means of wireless receivers operating in the same frequency as the transmitter. The obtained received bit stream is given to the FPGA kit to perform the Elliptic Curve Cryptography algorithm to provide an authentication of data. The ECC algorithm is simulated and implemented using the ModelSim - Altera 6.4a Quartus II 9.0 starter Edition with verilog as the source language. The register transfer level schematic(RTL), power utilization, resource utilization such as number of adders, subtractors, multipliers, slices, flip flops for the algorithm are measured by means of the Xilinx PlanAhead 13.2 version tool. This algorithm is implemented in the FPGA Virtex 5 kit using Xilinx Integrated Software Environment (ISE) Design Suite 13.2 version.

VI. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic Curve Cryptography is an approach to public-key cryptography, based on elliptic curves over finite fields
An elliptic curve is defined by the equation,

$$y^2 + xy = x^3 + ax + b$$

A. *Elliptic curve cryptography algorithm*

ECC is faster, and occupies less memory space than an equivalent RSA system. This means that it is suitable for constrained environments, especially in smartcards, where fast operations are necessary. Though the industry has been excruciatingly slow in adopting the new technique, RSA Security in an article on their website has implicitly agreed that ECC is the way to the future. The difference in the key-sizes between ECC and RSA will grow exponentially to maintain the same relative strength as compared to the average computing power available.
The architecture of an elliptic curve cryptography algorithm is shown in Fig 4.

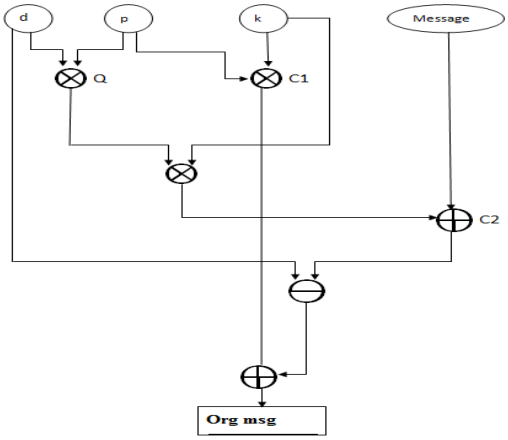

Fig 4 Architecture of an Elliptic Curve Cryptography Algorithm

Let d be the private key and p is a point on the curve where q=d*p is the public key. k denotes a random variable from 0 to n-1.where c1 and c2 are the two cipher texts generated through encryption process. In decryption process the encrypted cipher text is again decrypted to get back the original message.

VII. HASH MESSAGE AUTHENTICATION CODE(HMAC).

HMAC is a mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, e.g., MD5, SHA-1, in combination with a secret shared key. The cryptographic strength of HMAC depends on the properties of the underlying hash function.

A.HMAC Algorithm

The architecture of HMAC algorithm is shown in Fig 5.

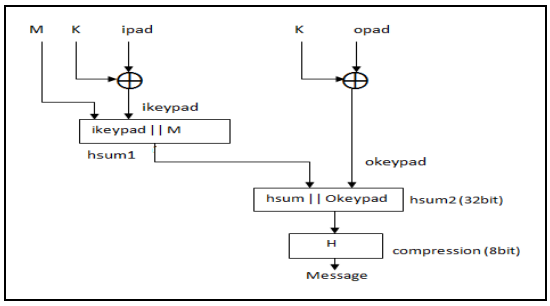

Fig 5 Architecture of HMAC Algorithm

The authentication key K can be of any length up to B, the block length of the hash function. Applications that use keys longer than B bytes will first hash the key using H and then use the resultant L byte string as the actual key to HMAC. In any case the minimal recommended length for K is L bytes (as the hash output length).

The two fixed and different strings ipad and opad are defined as follows

(the 'i' and 'o' are mnemonics for inner and outer):

ipad = the byte 0x36 repeated B times

opad = the byte 0x5C repeated B times.

To compute HMAC over the data `text' perform

H(K XOR opad, H(K XOR ipad, text))

VIII. EXPERIMENTAL TESTBED AND IMPLEMENTATION SETUP

We have implemented Privacy preserving access control on a real world experimental test- bed. Our implementation has the network owner, network user and sensor side programs. We use HMAC as the one-way hash function and ECC as the data encryption algorithm. In addition, the key size of ECC is set to 160 and 192 bits respectively. Also 160- bit ECC key length is considered secure enough for now and immediate future.

Power utilization output of secure data access privacy on FPGA, as shown in Figure 6.

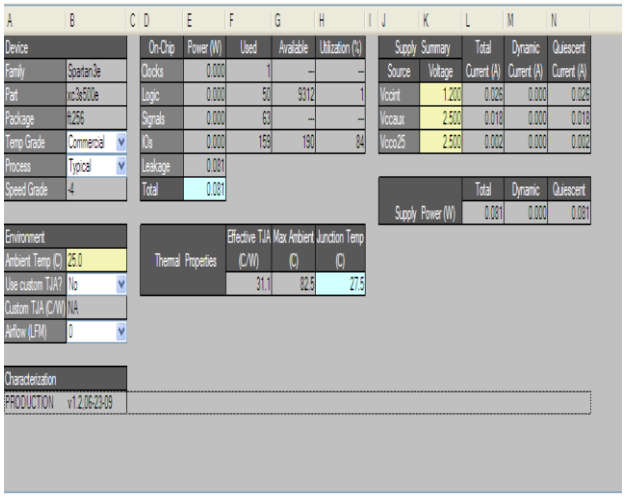

Fig 6 Power Utilization on FPGA

Due to increasing computation required for higher bit encryption, more transistors are required on board the smart card to perform the operation. This leads to an increase in area used for processor. Using ECC, the number of transistors can be cut back on since the numbers involved are much smaller than an RSA system with as similar-level security. Also, the bandwidth requirements for both of the systems are the same when the messages to be signed are long, but ECC is faster when the messages are short. This is more relevant, since PKC is used to transmit mostly short messages.

From [3], the occurrence of leakage power is found to be about 0.9 mw using RSA algorithm in Active mode. Using ECC algorithm in our proposed work on FPGA platform, we found the leakage power of about 0.081 mw only. The leakage power is very low when compared to RSA algorithm.

TABLE I

RESULTS OF FAST IMPLEMENTATIONS AND LEAKAGE POWER IN ACTIVE MODE OF ECC COMPARED TO RSA

Function	ECC 163 –bit	RSA 1024 –bit
Key Generation	3.8ms	4708.3ms
Sign	2.1ms(ECNRA) 3.0ms(ECDSA)	228.4ms
Verify	9.9ms(ECNRA) 10.7ms(ECDSA)	12.7ms
Leakage Power	0.081mw(Active mode)	0.900mw(Active mode)

IX. HARDWARE IMPLEMENTATION

The hardware architecture of secure data access privacy, as shown in Figure 7.

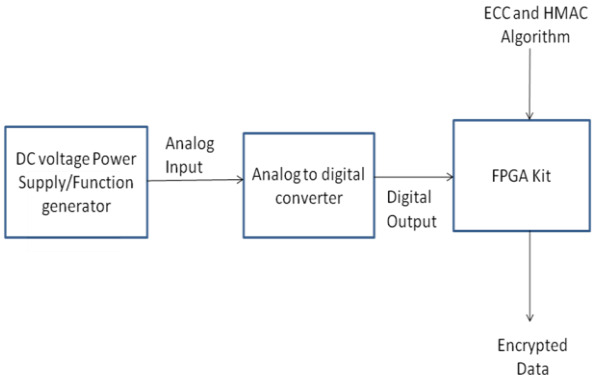

Fig. 7 Hardware architecture

DC Voltage Power Supply or Function Generator is used to produce the frequency and voltage in terms of analog signal. This analog signal is further converted to digital signal by means of analog to digital converter. This digital output acts as an input data to the FPGA kit, where we dumped verilog coding for ECC and HMAC algorithm. Finally, we get back the encrypted data in FPGA kit.

X. EVALUATION RESULTS

We present evaluation results of privacy preserving access control by means of four metrics: message overhead, the execution time, message complexity and energy consumption.

Firstly, we consider the message overhead of privacy preserving access control without considering packet headers. There are two cases as follows. One case is that we do not need to establish secure channels between the network user and sensor nodes. The message overhead of privacy preserving access control is (20×m+36) bytes. For the second case that we need to establish secure channels between the network user and sensor nodes. The message overhead of privacy preserving access control is (20×m+56) bytes.

Second, the execution time for user query generation phase when the number of chosen group members (m) and the key size of ECC (l) vary. For example, the execution time is 45.3 ms in the case that m=10 and l=160. The execution time is 212.4 ms in the case that m=50 and l=160.Thus the verification time on sensor nodes is independent of the scale of a WSN. But, the execution time is directly proportional to the number of chosen group members (m).

The message complexity of privacy preserving access control is independent of the size of a WSN (i.e., the total number of sensor nodes). To estimate the energy consumption of signature verification we use the formula E = U * I * t, where U is the voltage, I is the current and t is the time duration. Thus it is linear to the execution time.

XI. CONCLUSION AND FUTURE WORK

This paper presents Authentication and Secure data access privacy in wireless sensor network in communication system. The system setup consists of an ADC, transmitter, receivers and FPGA kit. The transmitter and receiver operate in the same frequency. The analog input signal is given to the ADC, which has eight bit resolution that converts the analog sample into digital bits. The ECC and HMAC privacy access algorithm having the source code in Verilog language is simulated using ModelSim and implemented using PlanAhead and Xilinx design suite.

The system implements a novel algorithm, called Elliptic Curve Cryptography algorithm, to obtain secure data access privacy in FPGA platform. In order to achieve Privacy Preserving access control this algorithm adopts various approaches to enhance their performance.

After implementing the algorithm in the kit, the performance is measured in terms of bit error rate. Also, resource and power utilization during synthesis and after implementation is measured. The FPGA Editor is used to improve the performance by manually configuring the logic blocks and input-output blocks. This work can be further enhanced by decreasing the leakage power during transmission and reception of data, so that the proposed ECC and HMAC algorithm for Authentication and Secure Data Privacy can be used in more applications.

REFERENCES

[1] Daojing He, Jiajun Bu, Senchun Zhu, Sammy Chan and Chun chen, "*Distributed Access Control with Privacy Support in Wireless Sensor Networks",* IEEE Transactions on Wireless Communication, Vol.10, No.10,October 2011.

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

[3] M.Das, "*Two-factor access control in wireless sensor networks*," IEEE Trans. Wireless Communication., vol. 8, no. 3, pp. 1086–1090, 2009.

[4] 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

[5] Le, Xuan Hung ,"*An energy efficient access control scheme for wireless sensor networks based on elliptic curve cryptography*", Journal of Communications and Networks, Volume:11 , Issue: 6 , Dec. 2009

[6] H. Song, S. Zhu, W. Zhang, and G. Cao, "*Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks,"* ACM Trans. Sensor Networks, vol. 4, no. 4, pp. 1–34, 2008.

[7] R. Zhang, Y. Zhang, and K. Ren, "*DP^{2}AC: distributed privacy preserving access control in sensor networks,"* in Proc. IEEE INFOCOM, 2009.

[8] 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.

[9] 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.

[10] M. Li, W. Lou, and K. Ren, "*Data security and privacy in wireless body area networks,"* IEEE Wireless Commun., vol. 17, no. 1, pp. 51–58, 2010.

[11] K.-F. Ssu, C.-H. Chou, H. Jiau, and W.-T. Hu, *"Detection and diagnosis of data inconsistency failures in wireless sensor networks,"* Computer Networks, vol. 50, no. 9, pp. 1247–1260, 2006.

[12] D. Janakiram, V. A. Reddy, and A. V. U. P. Kumar, *"Outlier detection in wireless sensor networks using Bayesian belief networks,"* Communication System Software and Middleware (Comsware), pp. 1–6, 2006.

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

[14] X. Lin, R. Lu, H. Zhu, P.-H. Ho, X. Shen, and Z. Cao, "ASRPAKE: an anonymous secure routing protocol with authenticated key exchange for wireless ad hoc networks," in Proc. IEEE ICC, 2007.

[15] D. He, L. Cui, H. Huang, and M. Ma, "*Design and verification of enhanced secure localization scheme in wireless sensor networks,"* IEEE Trans. Parallel and Distributed System., vol. 20, no.7, pp. 1050–1058, 2009.

[16] K. Sun, P. Ning, and C. Wang, "*TinySeRSync: secure and resilient time synchronization in wireless sensor networks*," in Proc. ACM CCS, pp. 264–277, 2006