Secured Public key Authentication and Energy Efficient MAC Implementation in Wireless Sensor Networks

Manoj Challa,
Lecturer, Dept of CSE,
C.M.R. Institute of Technology, Bangalore

M .Damodar Reddy,
Associate Professor,Dept of E.E.E,
S.V.U.College of Engineering, Tirupati

P. Venkata Subba Reddy,
Associate Professor,Dept of CSE,
S.V.U.College of Engineering,Tirupati

Jitendra Nath Mungara,
C.M.R. Institute of Technology,
Bangalore.

Abstract
As wireless sensor networks (WSNs) are susceptible to attacks and sensor nodes have limited resources, designing a secure and efficient user authentication protocol for WSNs is a difficult task. Considering that most future large-scale WSNs follow a two-tiered architecture, we propose an efficient and Denial-of-Service resistant user authentication scheme for two-tiered WSNs, which imposes very light computational load and requires simple operations such as one-way hash function and exclusive-OR operations. In addition, there is a growing requirement for preserving user anonymity recently. Thus we introduce pseudonym identity for each user which is concealed in login messages. And through clever design, our proposed scheme can prevent from smart card breach. Moreover, the security analysis on this scheme demonstrates that our proposed scheme enjoys security attributes such as preventing the various kinds of attacks and user anonymity. Finally, performance analysis shows that our proposed scheme is simple and efficient.

1. Introduction

Wireless sensor networks have applications in many areas, such as military, homeland security, health care, environment, agriculture, manufacturing, and so on. In the past several years, sensor networks have been a very active research area. Most previous research efforts consider homogeneous sensor networks, where all sensor nodes have the same capabilities. However, a homogeneous ad hoc network suffers from poor fundamental limits and performance. Research has demonstrated its performance bottleneck both theoretically and through simulation experiments and test bed measurements. Several recent works studied Heterogeneous Sensor Networks (HSNs), where sensor nodes have different capabilities in terms of communication, computation, energy supply, storage space, reliability and other aspects. Security is critical to sensor networks deployed in hostile environments, such as military battlefield and security monitoring.

A number of literatures have studied security issues in homogeneous sensor networks. Key management is an essential cryptographic primitive upon which other security primitives are built. Due to resource constraints, achieving such key agreement in wireless sensor networks are non-trivial. Probabilistic key pre-distribution is a promising scheme for key management in sensor networks. To ensure such a scheme works well, the probability that each sensor shares at least one key with a neighbor sensor (referred to as key-sharing probability) should be high. For the key pre-distribution scheme, each sensor randomly selects its key ring from a key pool of size P. When the key pool size is large, each sensor needs to pre-load a large number of keys to achieve a high key-sharing probability. Most existing sensor key management schemes are designed to set up shared keys for all pairs of neighbors sensors, without considering the actual communication pattern. In many sensor networks, sensor nodes are densely deployed in the field. One sensor could have as many as 30 or more neighbors. The many-to-one traffic pattern dominates in most sensor networks, where all sensors send data to one sink.

Due to the many-to-one traffic pattern, a sensor node may only communicate with a small portion of its neighbors, for example, neighbor sensors that are in the routes from itself to the sink. This means that a sensor node does not need shared keys with all neighbors. A key management scheme only needs to set up shared keys for each sensor and its c-neighbors, i.e., it does not need to set up shared keys for each pair of neighbor sensors. The new scheme can significantly reduce the overhead of key establishment in sensor networks. For example, suppose that a sensor node has 30 neighbors but only sends packets to 2 neighbors (e.g., one primary next-hop node and one backup). Using traditional key management schemes, 30 pair wise of keys need to be established for u, one key for each neighbor. Using c-neighbor concept, only 2 pair wise keys need to be set up for u, one for each c-neighbor. Thus, the new scheme can significantly reduce communication and computation overheads, and hence reduce sensor energy consumption. Public-key cryptography has been considered too expensive for small

Manuscript received August 5, 2012
Manuscript revised August 20, 2012

sensor nodes, because traditional public-key algorithms (such as ECC) require extensive computations and are not suitable for tiny sensors. However, the recent progress on Elliptic Curve
Cryptography (ECC) provides new opportunities to utilize public-key cryptography in sensor networks. The recent implementation of 160-bit ECC on Atmel ATmega128, a CPU of 8Hz and 8 bits, shows that an ECC point multiplication takes less than one second, which demonstrates that the ECC public-key cryptography is feasible for sensor networks. Compared with symmetric key cryptography, public-key cryptography provides a more flexible and simple interface, requiring no key pre-distribution, no pair-wise key sharing, and no complicated one-way key chain scheme. ECC can be combined with Diffie-Hellman approach to provide key exchange scheme for two communication parties. ECC can also be utilized for generating digital signature, data encryption and decryption. The scheme utilizes the c-neighbor concept and ECC public-key cryptography. That is, the scheme set up pair wise keys for each sensor with more than one neighbor. In case the primary next hop node fails, a backup node is used for communications. In addition, if there is a need for two neighbor sensor nodes to set up shared keys later (e.g., in case all backup nodes fail); they can do this with the help from other neighbors. First, we observed the fact that a sensor only communicates with a small portion of its neighbors and utilized it to reduce the overhead of key management. Second, we designed an effective key management scheme for HSNs by taking advantage of powerful H-sensors. Third, we utilized a public key algorithm - ECC for efficient key establishment among sensor nodes.

2. Elliptic Curve Cryptography Algorithm

A message M is encrypted by raising it to the power of e and then taking the result modulo some number N. To decrypt the message, you simply raise the value of the encrypted message C to the power of d and again mod by N. The beauty of ECC is that e and N can be published publicly. Together they, in fact, comprise the public key. The private key, which is not be published, is comprised of d and N.

C = Me mod N

M = Cd mod N

If you're like me, then you are astonished at 1) how simple this system is, and 2) that you can exponentiation messages twice (modulo some number) and leave the original message unaltered. The main question that my skeptical mind came up with when presented with this powerful encryption tool was, "wouldn't it be easy to compute d if you have the values of e and N?" The answer is, of course, no. It turns out that it is very hard to do so. If we choose N to be arbitrarily large, factoring N can take an arbitrarily long period of time. Currently, there are no known polynomial-time algorithms which can perform this task. Factorization has, in fact, been shown to be in the set of problems known as NP. So the security of ECC is essentially provided For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation along with a distinguished point at infinity, denoted (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.) This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

As for other popular public key cryptosystems, no mathematical proof of security has been published for ECC. However, the U.S. National Security Agency has endorsed ECC by including schemes based on it in its Suite B set of recommended algorithms and allows their use for protecting information classified up to top secret with 384-bit keys. While the technology, though some argue that the Federal elliptic curve digital signature standard (ECDSA; NIST FIPS 186-3) and certain practical ECC-based key exchange scheme (including ECDH) can be implemented without infringing them. by the hardness of the factorization problem. If someone figures out a way to factor large numbers fast, then ECC is out of business.

3. System Analysis Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. Public-key cryptography is based on the intractability of certain mathematical problems. Early public-key systems, such as the RSA algorithm, are secure assuming that it is difficult to factor a large integer composed of two or more large prime factors. For elliptic-curve-based protocols, it is assumed that finding the discrete algorithm of a random elliptic curve element with respect to a publicly-known base point is unfeasible. The size of the elliptic curve determines the difficulty of the problem. It is believed that the same level of security afforded by an ECC-based system with a large modulus can be achieved with a much smaller elliptic curve group. Using a small group reduces storage and transmission requirements.

For current cryptographic purposes, an elliptic curve is a plane curve which consists of the points satisfying the equation along with a distinguished point at infinity, denoted (The coordinates here are to be chosen from a fixed finite field of characteristic not equal to 2 or 3, or the curve equation will be somewhat more complicated.) This set together with the group operation of the elliptic group theory form an Abelian group, with the point at infinity as identity element. The structure of the group is inherited from the divisor group of the underlying algebraic variety.

As for other popular public key cryptosystems, no mathematical proof of security has been published for ECC. However, the U.S. National Security Agency has endorsed ECC by including schemes based on it in its Suite B set of recommended algorithms and allows their use for protecting information classified up to top secret with 384-bit keys. While the technology, though some argue that the Federal elliptic curve digital signature standard (ECDSA; NIST FIPS 186-3) and certain practical ECC-based key exchange scheme (including ECDH) can be implemented without infringing them.

4. System Model

We consider a large spatially distributed WSN, consisting of a fixed sink(s) and a large number of sensor nodes. The sensor nodes are usually resource-constrained with respect to memory space, computation capability, bandwidth, and power supply. The WSN is aimed to offer information services many network users that roam in the network, in addition to the fixed sink(s). The network users may include mobile sinks, vehicles, and people with mobile clients, and they are assumed to be more powerful than sensor nodes in terms of computation and communication abilities.

The network users could consist of a number of doctors, nurses, medical equipment (acting as actuators) and so on where the WSN is used for emergency medical response. These network users broadcast queries/commands through sensor nodes at their vicinity, and expect the replies that reflect the latest network information. The network users can also communicate with the sink or the backend server directly without going through the WSN if necessary. We assume that he sink is always trustworthy but the sensor nodes are subject to compromise. At the same time, the users of the WSN may be dynamically revoked due to either membership changes or compromise, and the revocation pattern is not restricted. We also assume that the WSN is loosely synchronized.

5. User Authentication in WSN

Simple Authentication with respect to the two primitive operations of authentication: (1 authenticate (V, I) is invoked by the prover P whenever P would like to be authenticated by V using identity associate (P, I) is invoked by the verifier whenever it has established the relation between P and some identity I. Intuitively, an authentication protocol is correct if the identity associated to P by V is the "real" identity of P. If P is dishonest or claims to have a fake identity this is indicated by a special value which is supposed to be distinct Menaces define the term entity authentication as the process whereby one party is assured the identity of a second party involved in a protocol. We call the two players involved prover P and verifier V. The verifier is requested by the proper to establish a correct relation between a particular identity and the prover. There can be multiple prover having the same identity, e.g., Alice's PDA, her workstation or her mobile phone can all be associated with the identity of Alice. We assume that a prover has at most one identity. We denote the set of all identities by I. We now formally define the properties of authentication protocols. These properties are defined from any value in I. Authentication is successful if V invokes associate (P, I) with some more precisely, a protocol solves authentication if it guarantees two properties (Validity) An honest verifier V invokes associate (P, I) with only if P in fact has identity I. (Termination) If P invokes authenticate (V, I) and if V is honest then V will eventually invoke associate. We call a protocol which satisfies the above two conditions a simple authentication protocol. Simple authentication is not sufficient in wireless sensor networks if failures and active adversaries are taken into account. If we require that a proper (i.e., a user) always authenticates to some particular sensor, then this becomes impossible if that sensor fails. However, if we don't care which sensor the proper uses for authentication, then taking control of a single sensor is sufficient for an active adversary to gain access to the entire system. What is needed is a more robust notion of authentication.

6. Distribution Mode

WSN the more hops between two communicating ends exist, the poorer the traffic performance becomes and the more energy consumption is required. To overcome these problems, we introduce the major idea of distribution mode is to deploy the cluster heads as the sub-base-stations because a cluster head is more powerful than normal sensor nodes. The distribution mode includes the following steps:

- Each cluster head manages to establish the shared key with its neighbouring cluster heads after deployment. There are several ways to do this. One could embed those keys in advance if the topology is known at deployment, or use the basic protocol described in the above sections, *via* the base station. (As this is a one-time operation, the overheads may be acceptable.)
- Sensor node keeps two base station identifiers (IDs): one is a real base station ID; the other is a sub-base-station (the cluster head) ID. Initially, the ID of sub-base-station is a real base station.
- After deployment, the first round for a mobile node to establish the shared key with the nearest cluster head uses the basic protocol, too.
- When the mobile node moves, use the basic protocol to establish the shared key with the new cluster head, *via* the sub-base-station (old cluster head) rather than the real base station.
- After successfully establishing the keys, the sensor node updates the ID of substation.
- For security reasons, each sensor node must reset its sub-base-station ID to the real BS

7. Proposed Methods and Works

Several recent works studied Heterogeneous Sensor Networks (HSNs), where sensor nodes have different capabilities in terms of communication, computation, energy supply, storage space, reliability and other aspects. In this project, we present an efficient authentication that only needs small storage space. The scheme achieves significant storage saving by utilizing.

- The fact that most sensor nodes only communicate with a small portion of their neibours
- An efficient public-key cryptography
- A sensor only communicates with a small portion of its neighbors and utilized it to reduce traffic conjestion.
- We utilized a public key algorithm for authentication among sensor nodes.

Node's private key is stored by itself, it can't be revealed even BS is under attack. Based on the difficulty even if the attacker got node's public key, he can't get its private key. And the private key is a random number selected by node itself, when the private key is untrusted, the node can reselect a random number for private key and register in system.

In authentication process, the attacker can get kA and kB by cracking the private key or intercepting SA and SB for attacking. But the above problems are all based on the difficulty of solving; the attacker cannot attack by the above way. So, this scheme can resist passive attack. Now that the attacker cannot get node's private key, even if SA and SB are falsified in communication process, the attacker cannot disguise himself as one side to accomplish authentication with the other side. So, this scheme can resist active attack. The node needs to check the other's ID hash value before authentication. Because the node's ID is the unique one which cannot be forged, this scheme can resist man-in-the-middle attack. In authentication phase, this scheme uses the random number to accomplish authentication, so it can resist replay attack. Hash function is a kind of one-way irreversible function, so any attacker cannot decrypt it. And nodes store the ID hash value which can conceal the node's real identity.

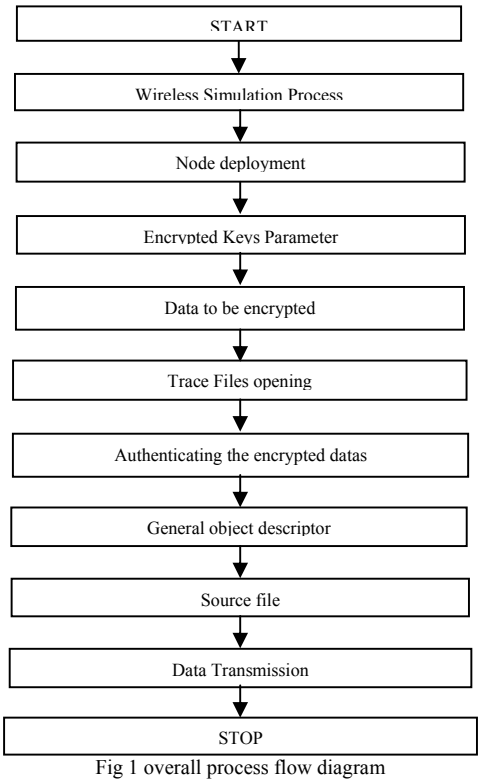

Fig 1 overall process flow diagram

In this authentication system, ECC multiplication is the primary operation mode, so its efficiency directly determines the performance of the system. Therefore, it can effectively enhance the performance of the system to use the fast algorithm for ECC multiplication and less multiplication in this scheme, sensor node only stores the other node's ID hash value which decreases the consumption of the node memory space, and provides the condition for the expansibility of the network. Considering the limited sensor node traffic, the node traffic is 3 times in the communication process designed in this scheme. Compare with the primary scheme, this

protocol leave out the tedious calculation for public and private keys, which makes the scheme simpler. And without additional digital signature, this scheme avoids additional communication overhead. Based on the low consumption of node storage and communication traffic and the high efficiency ECC multiplication algorithm, the 3 times node multiplication in this scheme is more reasonable. Overall process flow as shown in fig 1.

8. Simulation result

The following graph represents performance analysis security authenticated protocol in the Time domain Representation. The graph is plot between Data rate in the Y axis and Time in the X axis. The gradual decrease in the time shows the Stability of the system with the increasing Data rate. As shown in fig 2.

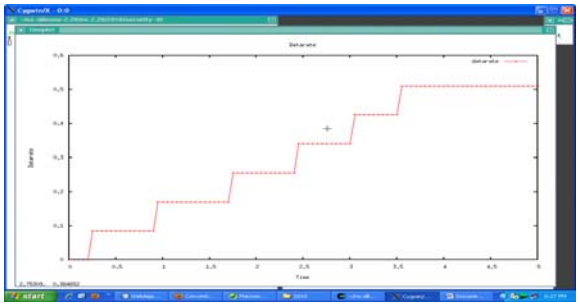

Fig 2 Relation between Time and Data rate

The following graph represents performance analysis security authenticated protocol in the Time domain Representation. The graph is plot between Delay in the Y axis and Time in the X axis. The gradual increase in the Delay shows the increasing performance abased on the Quality of service parameters. As shown in fig 3.

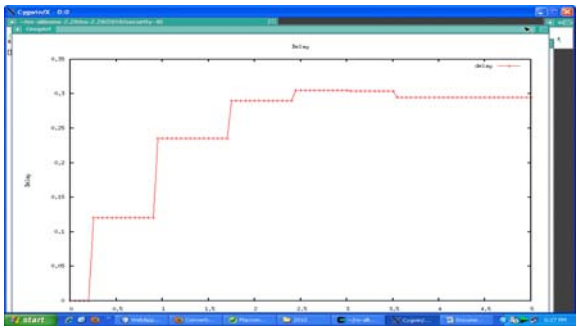

Fig 3 Relation between time and delay

The following graph represents performance analysis security authenticated protocol in the Time domain Representation. The graph is plot between Packets received in the Y axis and Time in the X axis. The graph is plotted for no of packets. Since this effective data transmission is performed by the no of packets transferred. As shown in fig 4.

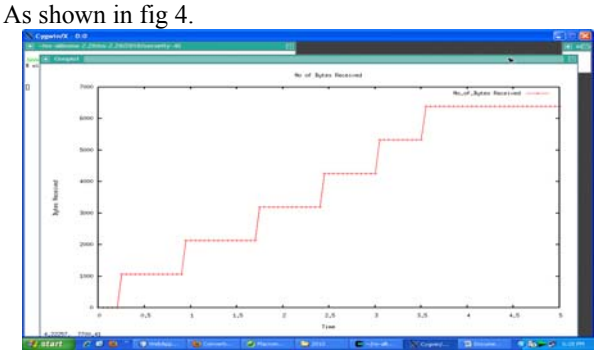

Fig 4 Relation between time and packets received

The following graph represents performance analysis security authenticated protocol in the Time domain Representation. The graph is plot between No of bytes received in the Y axis and Time in the X axis. No of packets is further this integrated for individual Analysis and represented by means of no of bytes. as shown in fig 5 ,5 a ,5b ,5c and 5d.

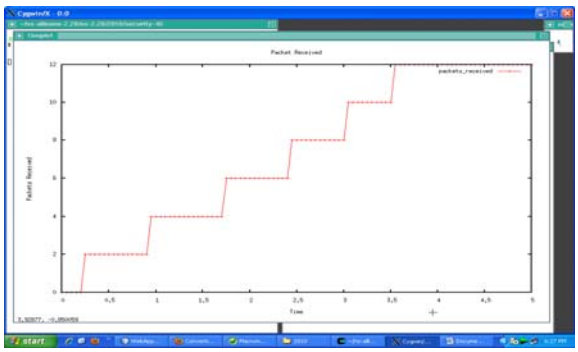

Fig 5 Relation between time and number of bytes received

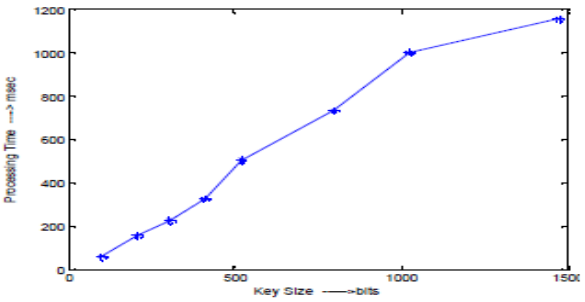

Fig 5a Processing Time versus key size for implicit certificate generation process

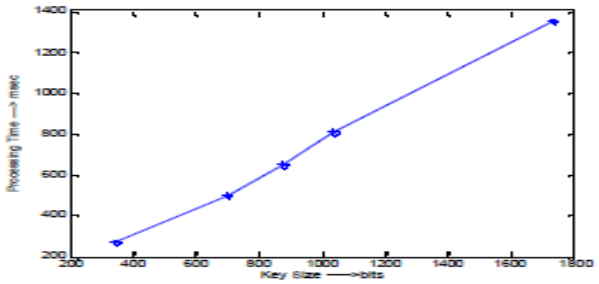

Fig 5b Processing curve versus key size for Elliptic curve digital signature algorithm

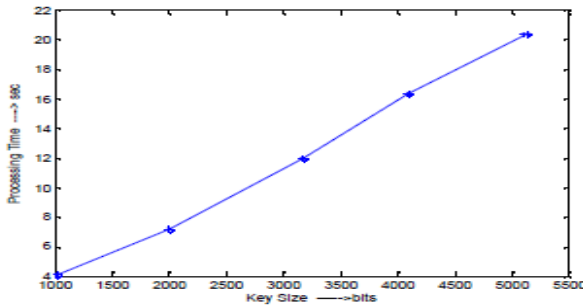

Fig 5c Processing time versus key size for ECC

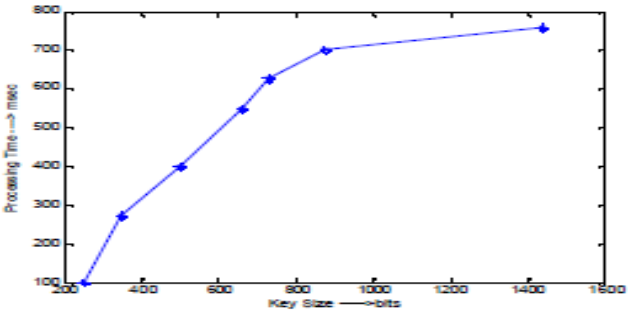

Fig 5d Processing time versus Hybrid key establishment protocol

Conclusion

In this paper, we studied the problem of broadcast authentication in WSNs. We pointed out that symmetric-key-based solutions such as µTESLA are insufficient for this problem by identifying a serious security vulnerability inherent to these schemes: the delayed authentication of the messages can easily lead to severe energy-depletion. We then came up with several effective ECC public-key-based schemes to address the problem. Both computational and communication costs of the schemes are minimized through a novel integration of several cryptographic techniques. Moreover, since the public key operation is expensive, it is also important that sensor nodes can be resistant to the local jamming attacks. Under such attacks, the adversary may simply broadcast random bit strings to the sensor nodes within his transmission range. If these neighbor sensors have to perform the expensive signature verification operation for all received messages, it will be a heavy burden on them. It obviously suffers from this type of attacks, as the signature verification operation has to be performed for every received message. However, such an attack can be effectively mitigated. This is because in both schemes, a sensor node first verifies the authenticity of the attached user public key through hash operations, so it performs signature verification operation for a bogus public key only quantitative energy consumption analysis, as well security strength analysis were further given in detail, demonstrating the effectiveness and efficiency of the proposed schemes.

References

[1] D. Liu and P. Ning, "Multi-level mTESLA: Broadcast authentication for distributed sensor networks," ACMTransactions inEmbedded Computing Systems (TECS), vol. 3, no. 4, (2004).

[2] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, S. Moulton, and M. Welsh, "Sensor Networks for Emergency Response: Challenges and Opportunities," In IEEE Pervasive Computing, (2004) .

[3] K. Ren, K. Zeng, W. Lou, and P. Moran, "On Broadcast Authentication in Wireless Sensor Networks," Accepted, IEEE Transactions on Wireless Communications.

[4] A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Shantz. "Energy Analysis of Public-Key Cryptography on Small WirelessDevices," IEEE PerCom, March (2005) .

[5] I.F Akyildiz, W. Su, Y. Sankarasubramaniam, E.Cayirci, "Wireless Sensor Networks: a Survey,"Computer Networks, Vol. 38, (2002) , pp. 393-422.

[6] A. Perrig, J. Stankovic , and D. Wagner, "Security inWireless Sensor Networks", Communication of ACM Vol. 47, No. 6, (2004) , pp. 53-57

[7] L. Hu, and D. Evans, "Secure Aggregation for Wireless Networks," Workshop on Security and Assurance in Ad hoc Networks, Orlando, USA, (2003) .

[8] D. D. Hwang, B. C. C. Lai, and I. Verbauwhede,"Energy-Memory-Security Tradeoffs in Distributed Sensor Networks," ADHOC-NOW, Vancouver, British Columbia, Canada, (2004) .

[9] H. Chan, Perrig, and A. D. Song, "Random Key Pre Distribution Schemes for Sensor Networks,"Symposium on Security and Privacy, IEEE, Oakland,California, USA, (2003)