ACCELERATED BROADCAST AUTHENTICATION WITH SIGNATURE AMORTIZATION FOR WSNS

Minnu Meria Mathew[1], Anjitha Mary[2]

[1]*Student, Computer Science & Engineering, ASIET, Kerala, India*
[2]*Assistant Professor, Computer Science & Engineering, ASIET, Kerala, India*

Abstract

Asymmetric Key Cryptography is widely used in broadcasting areas for authentication. But it is considered to be expensive to wireless sensor networks. This proposed system is a novel broadcast authentication scheme based on PKC with signature amortization. This scheme uses single Signature for authenticating a group of broadcast messages. As a result, the overhead is spread over that group of broadcast messages. Moreover, this scheme gives high security and low overhead also. But signature verification in ECDSA slower than signature generation. So, broadcast authentication with ECDSA has also suffered large energy consumption and lengthy verification delay. To reduce, this system uses cooperation among sensor nodes, which helps to accelerate the signature verification. During Signature verification, sensor nodes which have high energy allowed to leave the intermediary results of the signature verification process to their neighbors for accelerating the same. Simulation results show that the overhead of message authentication and the delay of verification of authenticated messages is reduced significantly.

Keywords: *Wireless sensor networks; Broadcast authentication; Cooperative Communication; signature amortization.*

----------***----------

1. INTRODUCTION

Wireless Sensor Network composed of one or more base station and number of sensor nodes that are scattered to monitor environmental and physical conditions like pressure, temperature, humidity. Base stations are the nodes that connects users and sensor nodes. A sensor node has limited power, storage, communication and computation.

WSN is often deployed in hostile situations which is lack of protection of the environment, and extremely vulnerable to attack like any other conventional network. For example, an adversary eavesdropping radio channel, can inject, intercept, modify, and destruct data packets. But the limited resource characteristics and unique application features of it needs some extra security requirements with the typical network requirements.

In WSN, Broadcast authentication is an important security concern, as it supports authenticated broadcasting of messages. Generally, Point-to-point authentication is by symmetric key cryptographic techniques. In this, the secret key with sender and receiver is same by which the cryptographic message authentication code over each message is computed. In sensor networks, broadcast authentication is difficult. The symmetric approaches for point-to-point authentication are not secured enough for broadcast authentication, where sensor nodes are not mutually trusted. In symmetric scenario, compromised receiver node can forge messages from the sender node. So broadcast authentication for WSNs encounters many challenges. Due to the constraints of sensor nodes, the broadcast authentication schemes by conventional Public Key Cryptography (PKC) are too expensive for WSNs due to this reason.

Perrig [9] propose µTESLA as a broadcast authentication scheme for WSNs. µTESLA exploits symmetric scenario to authenticate broadcasted messages. It satisfies limitations of WSNs. S it is efficient. But there is chances for node compromise attacks because of delayed disclosure of secret keys. To boost the performance of µTESLA, number of variants[10] [11] [12] are proposed. But this group of µTESLA have some shortcomings such as maintenance of time synchronization and distribution of the initial parameter. These are achieved by unicast transmission. So it shows heavy overhead. Another shortcoming is delayed authentication.

For the public-key based authentication technique, each message is transmitted along with the digital signature of the message which produced using the sender's private key. Every intermediate forwarder and the last receiver can authenticate by using public key of sender. One of the recent developed technique under public-key cryptographic schemes is elliptic curve cryptography (ECC). It is considered to be more beneficial in terms of memory usage, message complexity, and security resilience.. RSA [16] is a public key cryptography based signature algorithm that widely used for authentication purposes today. ECC [14] also offers equivalent security as compared with RSA at much smaller key sizes. The smaller keys shows savings in memory, bandwidth and computational power usage since constraints of WSNs. So now-a-days ECC become more

attractive for constrained wireless devices. Some other broadcast authentication schemes based on PKC are also existing which are proposed by Ren [16] and Liu[18]. Some works are done for finding the techniques to reduce the overhead of PKc based schemes. The main technique for this is signature amortization proposed by Gennaro[17] which is to sign efficiently digital streams.

This paper proposes a novel broadcast authentication scheme based on PKC with signature amortization for WSNs. This scheme uses only single signature by ECDSA to authenticate a group of broadcast messages. So, the overhead is amortized over that group of broadcast messages. However, this system shows low overhead and high security. Security of this system is strong as typical broadcast authentication schemes by PKC. No time synchronization is required for this scheme and also it can achieve immediate authentication. Thus, shortcomings of µTESLA can be overcome. But ECDSA shows signature verification delay since its signature verification is much slower than signature generation. To overcome this, we propose a scheme with cooperative communication. For this, the network forms clusters with cluster head, which have high energy in that group. Each cluster head releases intermediate results of computation to the neighbours of that cluster.

2. PROPOSED BROADCAST AUTHENTICATION SCHEME

The proposed scheme uses ECDSA for authentication, which is based on Public Key Cryptographic technique. It also **uses** a signature amortization technique for reducing the overhead and allows the network to function efficiently. This scheme exploit one signature to authenticate a group of messages. The one and only signature is used to authenticate the authenticator in first Extended Block ($EBlock_0$). The authenticator in $EBlock_0$ is used to authenticate next extended Block $EBlock_1$ that has a group of b broadcast messages and one authenticator. The authenticator in $EBlock_1$, is used to authenticate $EBlock_2$ that has authenticator and another group of *b* broadcast messages. This process till $EBlock_k$. From this brief, this is clear that the all messages authenticated by single signature.

WSN applications require low power, less memory space and bandwidth. ECC is best for this application because of its speed and security. But ECDSA needs an addition point and two multi scalar for verifying signature in WSNs, that because decrease signature verification speed, in the result, it has also incurred problems such as long verification delay and high energy consumption. To reduce these problems, here use cooperation among sensor nodes for accelerating the verification of a single signature. In this, system allow some sensor nodes that are selected by clustering to release the intermediary multiplication results in signature verification stage to their neighbours during the verification process. The overall idea of proposed system shown in Fig.1. The message authentication stage is performed by three steps:

Step 1 generating extended blocks step
Step 2 broadcasting extended blocks step
Step 3 verifying extended blocks step.

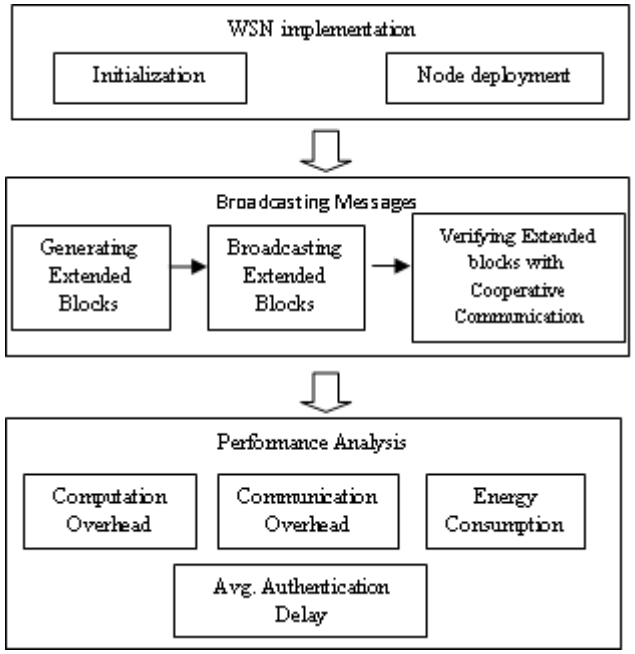

Fig-.1. Overall System

2.1 Extended Block generation

All broadcast messages in *M* is divided into p blocks $Block_1,...,Block_p$. Every block $Block_k$, $1 \le k \le p$, contains *b* messages. These blocks together form a vector $B = [Block_p]_{Ti=1,...,p}$ that shown in equation (1), here $n = pb$.

$$B = \begin{bmatrix} Block_1 \\ \cdot \\ \cdot \\ Block_k \end{bmatrix} = \begin{bmatrix} m_1 & \cdots & m_b \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ m_{(k-1)(b+1)} & \cdots & m_{kb} \end{bmatrix} \quad (1)$$

The p messages in each row of B are concatenated into a long string. Here considering $Block_k$, so concatenation is denoted by $CON(Block_k)$.

$$CON(Block_k) = m_{(k-1)b+1}||...||m_{kb},\ 1 \le k \le p \quad (2)$$

Then, $CON(Block_k)$ is padded with authenticators in each block indicated as $PAD(CON(B_k))$ which shown in equations (3) where d_{k+1} is authenticator. Block $Block_k$ and digest d_k+1 comprise an extended block $EBlock_k$.

$$PAD(CON(Block_k)) = CON(Block_k)||d_{k+1},\ 1 \le k \le p \quad (3)$$

Algorithm

1. Splitting-up broadcast messages into p blocks $Block_1 \ldots Block_p$
2. Initialize d_{k+1} and k=1…p
3. Perform the following steps
3.1 Concatenate messages in $Block_k$ to generate $CON(Block_k)$

3.2 Pad CON ($Block_k$) with digest d_{k+1} to generate Pad (CON ($Block_k$))
3.3 Compute the digest of result in step 3.2 using a collision resistant hash function H
3.4 Let $EBlock_k$ = [$Block_k$ d_k+1]
3.5 Decrement k
4. Repeat step 3 till i greater than or equal to 1
5. Sign the digest with senders private key PR_s to generate $EBlock_0=d_1 \| E(PR_s,d_1)$
6. Let EBlock= $[EBlock_i]_{i=0..p}$

2.2 Extended Block Broadcasting

$EBlock_k$'s authentication is based on $EBlock_{k-1}$. Thus, $EBlock_{k-1}$ should reach before $EBlock_k$ and so on. So this is by the sequential broadcast with reliability. A receiving node that receives a message *mj*, then it first confirms that *mj* is in current extended block $EBlock_k$. Then secondly it also confirms that the previous extended block $EBlock_{k-1}$ has received and authenticated. If $EBlock_{k-1}$ has not authenticated yet, then wait for short period for completion of its authentication. After completing authentication of block $EBlock_k$, the message m_j will broadcast. The receiver node accepts message m_j and broadcasts an acknowledgement that indicates all missed messages in that block. Hence the overhead for acknowledgement of each message is reduced. That is, here one acknowledgement is used to specify the missed messages in one extended block. But it may leads to large acknowledgement size.

2.3 Accelerated Verification of Extended Block

The signature verification process is accelerated by releasing few intermediate computation results in the WSN by the sensor nodes. This WSN authentication scheme performs better compared to other authentication schemes. Nodes that communicate through cooperative communication transmit data packets with each other. In WSNs, sensor node are distributed spatially and the nature of communication is generally broadcast through wireless medium. Hence, cooperative communications in WSNs can enhance the performance, especially network reliability.

2.3.1 Clustering

For implementing co-operative communication, it is needed to arrange the nodes into clusters. Each cluster has a cluster head, which has high energy in that cluster. Clustering means grouping the sensor nodes into clusters. The cluster formation is done by two steps where the the first step is group the nodes geographically and second step is Cluster-Head selection form the cluster-Member nodes. The Cluster-Head which is the higher level in clusters periodically transmit here it is intermediate results to the members of the cluster. Thus, the signature verification becomes easier and faster for each node. All the time, the Cluster-Head nodes send data to member nodes. Thus it always spend large amount of energy than member nodes. In some cases, the energy of Cluster Head is completely used. So it cannot be act as Head for long. As a solution for this energy starvation of some nodes, it is need to periodically re-elect a node which has highest energy in that cluster as new Cluster-Head. The fig 3 shows the flow diagram of CH selection.

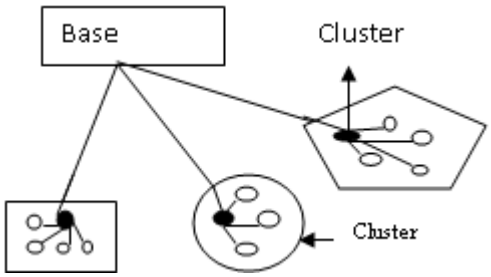

Fig- 2 Cluster model

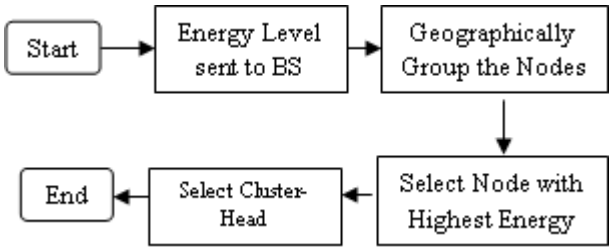

Fig -3 Flow diagram of CH selection

2.3.2 Accelerated Verification

In WSNs, the broadcast authentication schemes based on PKC techniques provides strong security and immediate message authentication than the same based on symmetric-key approaches. But the schemes used public-key Cryptographic techniques, verification of signature is much slower than the schemes that based on symmetric-key cryptographic techniques. Due to this, when large number of message are there for authenticated broadcast, a number of messages might wait for signature verifications.

By using the cooperation among sensor nodes, this issue of slower signature verification of ECDSA can be reduced. This is by randomly release the intermediary computation results *(iR)* of signature verification to their neighbours. Cluster-Head releases the results in this system. Then many sensor nodes which are the cluster-Members use the received intermediary results to verify signature.

Generally every sensor nodes independently perform the same verification procedure during the broadcast authentication. Every node needs to calculate two scalar multiplications denoted *iR1* and iR2. It leads to high energy consumption. Thus, some sensor nodes that have high energy which selected as Cluster-Heads allow to release some intermediary results to their neighbous. So the member nodes in a cluster does not need to calculate the two scalar multiplications. Only one value is calculatedindependently and other got from Cluster Head. Hence the overall signature verification time can be reduced noticeably. And also, the overall energy consumption of network will be decreased drastically. This is shown in Figure 4.

When a Cluster-Head releases its intermediary multiplication results (iR), all its neighbouring nodes which are Cluster-Members accelerate the signature verification by

just computing one elliptic curve point addition and one scalar multiplication. When the sensor nodes utilize two scalar multiplications as intermediary computation values for verification, there is a chance for receiving fake from an attacker. To prevent this attack, the sensor nodes are permitted to use at most only one intermediate value (iR1 or iR2) from the neighbouring nodes.

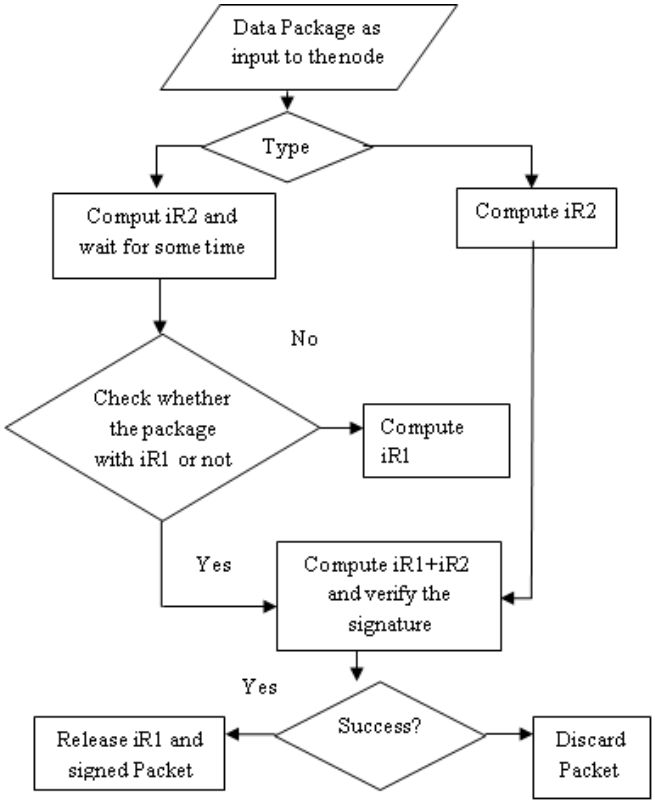

Fig-4 Enhanced scheme for ECDSA signature Verification

3. PERFORMANCE ANALYSIS

Accelerated Authentication scheme for WSN is implemented using JiST simulator (Java in Simulation Time). This JiST simulator is high performance discrete event simulation engine which runs on Java Virtual Machine. Its capabilities are similar to NS2 and Glomosin, but JiST is able to simulate much larger network. During experiments, performance metrics such as Throughput, Signature Verification delay, Routing Overhead, Communication and Computation Overhead and Energy Consumption are considered.

Total consumed energy: Overall energy consumed in the network by all nodes.

Te=Σ Ce, where Te is total consumed energy, Ce is overall energy by all nodes

End-to End delay: Time taken to transfer a packet from source to destination node.

End-to-end delay = (Σ recv pkt – sent pkt / Σ recv pkt)*100, where recv pkt is no. Of received packets, sent pkt is no. Of sent packets

Overhead: Overall consumption for completing a process. It calculated as a ratio of the correct packets to the total received packet.

$$\text{Overhead} = \Sigma \text{ RTR pkt} / \Sigma \text{ recv pkt}$$

Table 1 shows the parameter used to simulate the proposed system. The Results of the simulation are shown in the Table 2 and Table 3, which shows the Energy Consumption, Average Verification Delay, Communication Overhead and Computation Overhead with the different no. Of nodes by setting up the no of clusters as 4 and different number of clusters or cluster heads for a sensor network 100 sensor nodes respectively.

Table-1 Simulation Parameters

Sl. No.	Parameter	Value
1	Number of nodes	150 (varied)
2	Simulation Area	1000m ×1000m
3	Traffic Type	CBR
4	MAC Type	802.11 MAC Layer
5	Packet Size	512 bytes
6	Node Initial Energy	100J
7	Transmission Power	0.007
8	Reception Power	0.007

Table-2 Simulation Results (here, no of clusters=4)

No of Nodes	Energy Consumption (J)	Communication Overhead	Computation Overhead	Avg Verification Delay
20	11	230	338	15
30	11	250	354	18
40	13	300	374	20
60	14	348	413	27
80	16	412	445	34
100	17	468	489	42
130	21	490	538	42

Table-3 Simulation Results (here, no of nodes = 100)

No of Clusters	Energy Consumption (J)	Communication Overhead	Computation Overhead	Avg Verification Delay
2	23	380	514	53
3	25	412	503	48
4	17	468	489	42
5	19	547	498	37
6	22	554	493	33
7	21	587	482	35
8	20	598	479	38

In this work, the performance analysis is carried out in a sensor network that simulated using JiST by varying parameters i.e. number of nodes, while keeping other parameters constant and also with different number of clusters. Four PKC based authentication schemes, i.e. RSA, ECDSA, ECDSA with Signature Amortization and Accelerated ECDSA Authentication with Signature Amortization are considered in the comparison. Figure 5, 6, 7 and 8 shows the simulation graphs for different number of nodes verses Energy Consumption, Communication Overhead and Computation Overhead, Average Verification Delay respectively.

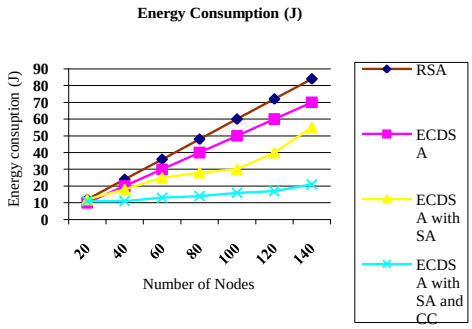

Fig-5 Comparison on the basis of Energy Consumption

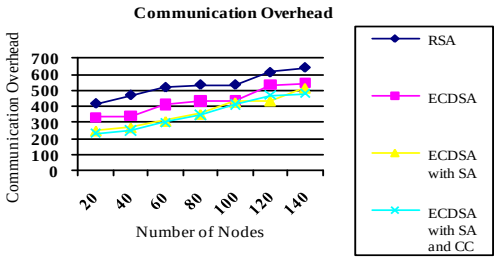

Fig-6 Comparison on the basis of Communication Overhead

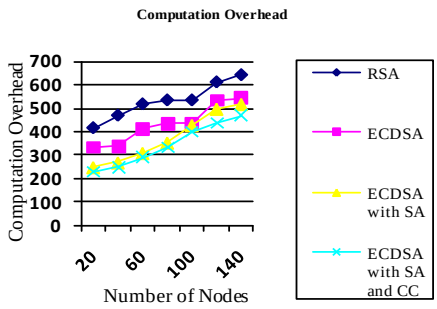

Fig-7 Comparison on the basis of ComputationOverhead

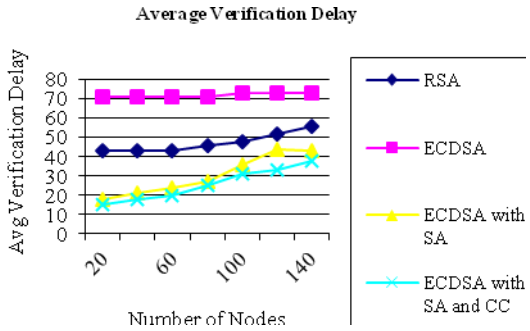

Fig-8 Comparison on the basis of Avg Verification Delay

4. CONCLUSION

PKC-based broadcast authentication schemes specially signature-based schemes for WSNs have more attention in recent years since it shows strong security and immediate message authentication. As compared with others, verification of public-key cryptographic signatures consumes higher amount of energy and this process is also slow. The proposed scheme is an efficient broadcast authentication, which accelerating the verification process of PKC based signatures in WSNs by exploiting the cooperative communication between sensor nodes. It reduces overall energy consumption. From the simulation Results, the overhead of this system is less than the typical signature-based schemes. Besides this, the proposed system uses less energy than others. By accelerating the verification of signature, this scheme reduces the signature verification delay also.

REFERENCES

[1]. Akyildiz , W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag., vol. 40, no. 8, pp. 102–114*, 2002.

[2]. S Patil, Dr Vijaya Kumar, S. Sinha snd R. jamil "A Survey on Authentication Techniques for WSN" IJAER Vol. 7,no.11,2012

[3]. Z Li and Guang Gong "A Survey on Security in Wireless Sensor Networks"

[4]. T Kavitha and D Sridharam "Security Vulnerabilities in Wireless Sensor Networks: A Survey" JIAS, 031-044, 2010

[5]. Y.Wang, G.Attebury and B. Ramamurthy "A Survey of Security Issues in Wireless Sensor Networks" , IEEE ,Vol.8, No.2, 2006

[6]. M Luk, A Perrig and B Whillock "Seven cardinal properties of sensor network broadcast authentication" ACM , pp. 147-156, 2006

[7]. G. Sharma,S. Bala and Anil K V " Security Framework for Wireless Sensor Networks-Review" ScienceDirect, 978-987, 2012

[8]. A. Perrig, R. Canetti, J. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," in *Proc. 2000* IE*EE Symposium on Security and Privacy, pp. 56–73.*

[9]. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS:security protocols for sensor networks," *Wireless Networks, vol. 8, no.5*,pp. 521–534, 2002.

[10]. D. Liu and P. Ning, "Multilevel *μTESLA: broadcast authentication for* distributed sensor networks," *ACM Trans. Embeded Computing Syst.*,vol. 3, no. 4, pp. 800–836, 2004.
[11]. P. Ning, A. Liu, and W. Du, "Mitigating DoS attacks against broadcast authentication in wireless sensor networks," *ACM Trans. Sensor Networking, vol. 4, no. 1, pp. 1–35, 2008.*
[12]. T. Kwon and J. Hong, "Secure and efficient broadcast authentication in wireless sensor networks," *IEEE Trans. Computers, vol. 59, no. 8, pp.* 1120–1133, 2010.
[13]. F. Amin, A.H.Jahangir and H.Rasifard " Analysis of Public Key Crptography for Wireless Sensor Networks Security" World Academy of Science, 2008
[14]. Asha Rani and M Sinha "Elliptic Curve Cryptography(ECC) for security in Wireless Sensor Networks" , IJERT
[15]. G S Quirino, ARL, Ribeiro and E D Moreno " Asymmetric Encryption in Wireless Sensor Networks" INTECH , 2012
[16]. K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," *IEEE Trans. Wireless Commun., vol. 6,* no. 11, pp. 4136–4144, 2007.
[17]. J. M. Park, E. Chong, and H. Siegel, "Efficient multicast packet authentication using signature amortization," in Proc. 2002 IEEE Symposium on Security and Privacy, pp. 227–240.
[18]. An Liu and Peng Ning "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks" IEEE, 2008
[19]. Y Liu , J Li and M Guizani "PKC Based Broadcast Authentication using Signature Amortization for WSNs" IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 11, NO. 6, JUNE 2012