Volume 2, Issue 10, October 2012 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Design an Enhanced Certificate Based Authentication Protocol for Wireless Sensor Networks

M.Rameshkumar
Assistant Professor, Department Of Computer Science and Engineering.
Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College,
Chennai, Tamil Nadu, India.

Dr.C.Suresh Gnana Dhass
Professor & Head of IT Dept,
Park College of Engineering and Technology, Kaniyur,
Coimbatore, Tamil Nadu, India.

Abstract: In wireless sensor networks (WSN's), the broadcast authentication is a critical security service, as it helps users to broadcast the WSN in an authenticable way. µ TESLA and MULTILEVEL µ TESLA are symmetric key based schemes, that have been introduced to provide such services for WSNs, but even they suffer from serious DoS attacks due to the delay in message authentication. Hence in order to overcome the weaknesses presented in the µ TESLA, and such similar schemes, this paper presents several effective key based schemes to achieve immediate broadcast authentication. In order to minimize the scheme overhead regarding the costs on both computation and communication, several schemes, such as hash tree and identity based signature schemes have been adopted. Of the proposed scheme, the quantitative energy consumption analysis is also given in detail. This paper is in all means prepared to solve the important multi sender broadcast authentication hindrance in WSNs.

Keywords: Authentication, DoS attacks, energy consumption.

1. INTRODUCTION

Wireless sensor networks , have authorized data gathering from a vast geographical region , and for a wide range of tracking and monitoring application from both civilians and military domains, unprecedent opportunities is present [1],[2],[28],[29],[38].To the demands of the network users, it is expected that the WSNs would process ,store and provide the sensed data to the users.As the most common communication pattern, it is expected that the network users issue the queries to the network before obtaining the information of their internet. Moreover in wireless sensor and actuator networks (WSNs)[2], commands to the network may be issued by the network users (probably based on the data he/she received from network).

There could be a large number of users in WSNs, which could be either static or mobile. In both cases, mobile clients could be used by the users to query or command the WSNs from anywhere in network. For sure , broadcast/multicast operations are fundamental , in order to realize these network functions.Therfore to ensure broadcast authentication which is for the security purpose is highly important. It is µTESLA that initially addressed the broadcast authentication in WSNs [27]. It is always assumed trustworthy , that user of WSNs is taken or alleged to be one or a few fixed sinks in WSNs.A one way hash function h() has been assumed by this scheme and it also uses the hash pre images as keys in a message authentication code (MAC) which is an algorithm. To begin with, the sensor nodes are preloaded with $K_0=h^n(x)$,where x is the secret held by the sink. After this, the $K_1=h^{n-1}(x)$ is used to generate MACs for all the broadcast messages that are been sent within the time interval 1. The sink broadcast K_1, and sensor nodes verify $h(K_1)= K_0$ at the time interval 2. The authority of messages received during the time interval 1, is then checked using K_1. For the entire hash chain, the delayed disclosure technique is been used and this ultimately demands loosely synchronized clocks between the sink and sensor nodes. µ TESLA is than enhanced in [19], [20], in order to length the limit of the hash chain. The µ TESLA is extended in [21] to support the multiuser agenda at the cost of higher communication overheads per message.It is commonly held at µ TESLA like schemes have the following drawbacks, even in the single user scenario.

1) All the messages received within one time interval have to be buffered by all the receivers.

2) They are subject to wormhole attacks [13], where because of propagation delay of the disclosed keys, the message could be forged. Moreover, here, a more serious weakness of µ TESLA like schemes when they are applied in multi hop WSNs.

This paper, for effective solution public key cryptography is resorted. By designing PKC-based solutions with minimized computational and communication costs, we approach broadcast authentication problem in WSNs under multi user scenario. On one side, we want to achieve immediate message authentication and be immune to DoS attacks in the presence of both the node compromise and user revocation. On the other side, we want to optimize both the computational and communication costs.

Here three various PKC –based approaches and provide in depth analysis on their pros and cons, has been proposed. In all these three proposed approaches, the users are always authenticated, via , public keys. We initially propose, a certificate based proposal, and indicate its inherent weakness on artificate revocation management, when applied in WSNs . In order to distance from certificate revocation problem, we propose a Merkle hash tree scheme manage user public keys. The storage overhead at sensor nodes is a single hash value with L bytes, as in the above proposed way, however, the additional communication overhead per hop is $L*\log_2 N$ bytes , where N is the number of network users. To have a L* m-byte storage overhead , the Merkle hash tree based scheme is further enhance and a $L*\log_2 N/m$-byte communication overhead, where m is the number of hash value that need to be stored by sensor nodes. $L*\log_2 N/m$-bytes additional communication overhead per hop could still be very high , where N is large , since the WSN under consideration is usually very large and hence has many hops.

An approach, called ID-based authentication technique has been proposed, to eliminate the communication overhead. Now this approach makes use of the ID-based cryptography, in which a user's public key is his ID information , an valid user only can have the corresponding private key. Henceforth, in communication, the ID-basede scheme is highly efficient, but still it suffers from high computation cost. Rgarding and with respect both computational and communication cost, the pros and cons of the proposed scheme have been analysed .

2. RELATED WORK

- This paper , points out the serious security weakness inherent to the surfaces or the symmetric key based µ TESLA likes schemes that is in practice.
- This paper has also revisited the problem of multi sender broadcast authentication in WSNs.
- To address the multi sender broadcast authentication in WSNs, the PKC based schemes are been proposed . In this scheme both computational and communication costs are been analyzed well. In order to decrease the cost for this process , several novel cryptographic techniques are been taken into practice, including Merkle hash tree authentication technique and ID-based signature scheme.
- Of the proposed scheme, we analyze both the performance and security resilence. And also a quantitative energy consumption analyses is given in detail.

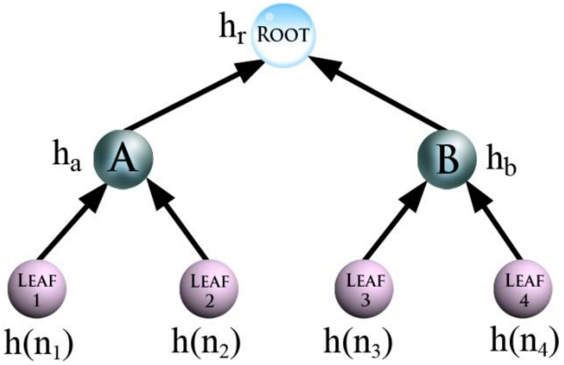


Fig: 1 an Example of Merkle Hash Tree

3. PRELIMINARIES

A. Merkle hash tree techniques: Here we adorn the construction and application of the Merkle hash tree [24] through an example.The date source constructs the Merkle hash tree, assuming that w=4, in order to authenticate data values n1,n2,….,nw. The message hashes, such as h(ni),i=1,2,,3,4, hash the values of the four leaf nodes(eg: SHA-1 [26]). From the child nodes only, the value of each interval node is derived. For instance the value of the node A is ha=h(h(n1)|h(n2)). From the leaf nodes to the root node, the data source completes the levels of the tree recursively. The one that is used to commit to the entire tree to authenticate any subset of the data values n1,n2,n3 and n4 in conjunction with the small amount of auxiliary, i.e., helping authentication information AAI(I.e., $\log_2 N$ hash values with N as the number of leaf nodes) is the value of the root node hr=h(ha/hb). For instance, a user who is assumed to have the authentic root value hr, request for n3 and requires the authentication of the received n3.

Apart from n3, the source sends the AAI:<ha,h(n4)> to the user. The user can then check the authenticity of the received n3 by initially computing h(n3),hb=h(h(n3)|h(n4)) and hr=h(ha|hb) and then checking if the calculated hr is the same as the authentic root value hr. The user accepts n3, only if this check is positive.

B. ID based cryptography:

Identity based cryptography (IBC) is getting extensive attention as a powerful change to traditional certificate based cryptography. The main ideology over here is to make an entity's public key directly derivable from its publicly known identity information. Even though, the idea of IBC dates back to 1984 [34], only recently has its rapid development taken place due to the application of the pairing technique outlined below.

Correctly select two large primes p &q, and let E/Fp indicate an elliptic curve $y^2=x^3+ax+b$ over a finite field Fp. We indicate by G_1 a q-order subgroup of the additive qroup of points of E/Fp and by G_2 a q-order subgroup of the multiplicative group of the finite field Fpi* (i=2,3, or 6). The discrete logarithm problem (DLP) is required to be hard[3] in both G_1 and G_2. For us, a pairing is a mapping ê: G_1 X G_1-> G_2 with the properties listed below,

1.Bilinear: For all P,Q,R,S ε G_1, ê (P+Q,R+S)= ê(P,R) ε (P,S) ê(Q,S). Consequently for all c,d ε Zq*, we have Ê(cP,dQ) =ê(cP,Q)^d = ê(P,dQ)^c= ê(P,Q)^cd,etc..

2. Non degenerate: If P is a generator of G_1, then ê(P,P) ε Fp_2* is a generator of G_2.

3. Computable: There is an efficient algorithm to compute ê(P,Q)for all P,Q ε G_1. It s important to note that, ê is also symmetric i,e., ê(P,Q)= ê(Q,P), for all P,Q ε G_1, which follows immediately from the bilinearity and the fact that G_1 is a cyclic group. Modify Weil [8] and Tate[5] pairing are examples of such bilinear maps for which the Bilinear Diffie-Hellman Problems(BDHP) is believed to be hard[4]. We also see to [5][8] for a more comprehensive description how this pairing parameters should be selected in practice for efficiency and security.

4. ASSUMPTION, OBJECTIVES AND AGENDAS OF SCHEMES AND MOTIVATION OR STIMULANT OF DESIGN

System model: Here we consider a very large, spatially distributed WSN which a fixed sink and a large a,ount of sensor nodes . The sensor nodes in their functionality and capability are not necessarily homogenous. The WSN which under consideration is aimed to offer information services to a large number of network user that roam in the network, in addition to the fixed sink. All these WSN users are having the mobile sinks, vehicles and people with mobile clients, and they are assumed to be more powerful than sensor nodes in term of computation and communicational abilities. For instance the network users could include a number of doctors, nurses, medical equipments (acting as actuators) and etc, in the case of Code Blue [22], where the WSN is used for emergency medical response. Except the replies that reflect the latest sensing results, these networks users broadcast queries/commands through sensor nodes in their vicinity. The network user also directly communicate with sink is always trustworthy but the sensor nodes are subject to compromise. Mean while the users of the WSN may be dynamically revoked due to either membership changing or compromise, and the revocation pattern is not restricted. As the µ TESLA likes schemes, we also assume that the WSN time is loosely synchronized.

ADVISORY MODEL: The advisory goal over here is to inject bogus messages into the network, attempt to receive sensor nodes, and obtain the information of his interest. Appending, Deny of Services (DoS) attacks such as bogus messages flooding, aiming at exhausting constrained network resources, is another important focus of this paper. Also here, it is assumed that the advisory has the ability to compromise better network users and sensor nodes. The advisory hence could exploit the compromise users/ nodes for such attacks. We also consider the following types of attacks,

1) The advisory may directly broadcast bogus messages to the WSN by himself.

2) The advisory may use one or more compromise nodes to propagate bogus messages to the WSN by pretending that the messages are stared by legitimate network users.

3) The advisory may use one or more compromise users to broadcast messages to the WSN. But still we consider that advisory cannot compromise an unlimited number of sensor nodes. Neither can they break any cryptographic primitive on which we base our design. If not it is unlikely for any feasible security solution to be designed.

OBJECTIVES FOR SECURITY PURPOSES: The advisory model, indicated above in which our security objective is straight forward. Initially, user authentication is needed so that illegitimate (i.e.,) legally wrong or such users will be excluded from injecting bogus messages. Secondly, user revocation mechanisms have to be implemented so that sensor nodes could deal with user revocation. Thirdly, the authenticity of any message broadcast by the user should be able to be verified by every receiving node. As an abstract, all messages being broadcast to the WSN should be authenticated so that any bogus ones issued by the unlegalized users and compromised sensor nodes can be efficiently and deterministically rejected of filtered.

DESIGN STIMULANT OR MOTIVATION: With respect to computation capability, bandwidth availability and energy supply, the sensor nodes where assumed to be extremely resource constrained, at the time when µ TESLA was proposed.

Although PKC could provide much simplified solutions with much stronger security strength, the PKC was thought to be forbiddingly computationally expensive. However, recent studies [10], [36] showed that, contrary to widely held believes, PKC with software implementations only is very viable on sensor nodes. For instance, in [36] it was reported elliptic curve cryptography(ECC) signature verification takes 1.61 s with 160 bit keys on ATmegal128 8MHz processor, a processor used for the current crossbow platform[9]. The advantages of transmitting smaller ECC keys and hence smaller messages / signatures will in turn be more significant. Furthermore, next generation sensor nodes are expected to combine ultra-low power circuitry which so called power scavengers such as Heliomote [11],[16], which lets continuous energy supply to the nodes using MEMS- based power scavengers, at least 8- 20 µW of power can be generated [3][23]. Where as the other solar based systems are even able to deliver power up to 100mW for the mica motes [16],[17]. These results indicate that, with the advance of fast growing technology, PKC is no longer in practical for WSNs, although still expensive for the present generation of sensor nodes and its wide acceptance is expected in the near future [10].

5. THE PROPOSED SCHEMES

PKC based solution has the ability to realize immediate message authentication and thus overcome the delayed authentication problem presented in µ TESLA likes schemes, however, the straight forward solution such as certificate based approach can not be directly applied in WSNs due to their high scheme overhead as we analyze below. To achieve a desirable scheme performance we have adopted more advance techniques.

A. The Certificate Based Authentication Scheme: The scheme:- Every user of the WSN is equipped with a public / private key pair(PK/SK), and signed every message he broadcasts with his SK using a digital signature scheme such as RSA or DSA[25], [31]. The sink[6] is also equipped with a public/private key pair and serves as the certificate authority (CA) in order to prove the user's ownership over his public key . The sink issues each user a public key certificate, and such a certificate, to its simplest form, consists of the following contents.

$\mathrm{Cert}_{UID} = U_{ID}$, PK$U_{ID}$, ExpT, SIGSK_{Sink} *{h*(*UID*||ExpT|| PK*UID*)*}*, para,

where *UID* denotes the user's ID, PK*UID* denotes his public key, ExpT denotes certificate expiration time and SIGSK*Sink{h*(*UID*||ExpT||PK*UID*)*}* is a signature signed over *h*(*UID*||ExpT||PK*UID*) with SK*Sink*. Hence, a broadcast message is now of the form as follows:

< *M*, *tt*, SIGSK*UID {h*(*UID*||*tt*||*M*)*}*, Cert*UID* > (*I*)

Here, *M* denotes the broadcast message and *tt* denotes the current time. Then, sensor nodes are enabled to verify the authenticity of the received messages by preloading PK*Sink* before the network deployment. The verification contains two steps: the certificate verification and the signature verification Of the above M denotes the broadcast message and tt denotes the present time .The sensor nodes the enable to verify the authenticity of the received message by preloading PK sink before the network deployment. The verification contains two steps: The certificate verification and the verification of the signature

ANALYSIS:

From much severe vulnerability this straight forward scheme suffers. It is inefficient to support the user in revocation in the scheme. Sensor nodes have to receive K store a certificate revocation list (CRL), in order to support user revocation and also certificate revocation. The CRL request a storage space linear to the total number of revoked certificates at each sensor nodes. But still, this is practically infeasible due to the stringent storage limitation of sensor, especially given a large number of users or a highly dynamic membership changing scenario. For instance, it is assumed that a public key is 20 byte long, a CRL having only 1,000 revoked certificates is atleast of size 19.5 KB even in the simplest format (i.e containing only the public key). It is also obvious that resorting to the sink on demand for CRL verification is inefficient either, because this could introduce too much communication cost. Embedding validity interval into the certificate does not really help decrease the storage overhead much, since the revocation pattern is not available. Next, to authenticate each message, instead of one signature verification operations, one is taken. This is because; usually the certificate must be authenticated in the first place.

B. THE AUTHENTICATION SCHEME BASED ON THE BASIC MERKLE HASH TREE:- Now, we propose a Merkle hash tree based authentication scheme, which is highly storage efficient, having observed the CRL problem inherent to the first scheme.

SCHEME INITIALIZATION:- All the public keys of the current network users are collected by the sink and constructs a Merkle hash tree .Here we have constructed N leaves with each leaf correspondingly user ID and the public key of the user (i.e) h(Uid,PKuid). The values of the internal nodes are determined with the same methodology as in section-2-A hr, this is how the value of the final root node of the hash tree is denoted. Then, the sink per loads/ broadcasts each sensor node with this value before network deployment or during the network operation time. But then, if the network operation time is broadcasted during hr, then the hr should be signed by the sink to prove its authenticity. Obviously, in this case, sensor nodes should be preloaded with the sink's public key. Meantime, each user should obtain its AAI in accordance to his corresponding leaf node's location in the Merkle hash tree. From a leaf node to the root (not including the root), let T denote all the nodes. Then A is defined s the set of nodes corresponding to the siblings of the nodes corresponding to the siblings of the nodes in T and AAI further corresponds to the values associated with the nodes in A. Ofcourse, AAI is (L*$\log_2$N) bytes, where the hash value is L bytes in length.

MESSAGE AUTHENTICATION: The form of a message sent by a user ID would be <M,tt,SIGSKuid{h(Uid||tt||M)}, Uid,PKuid,AAIuid> Each and every node verifies such a message in 2 steps . Initially the PKuid is verified using AAIuid that is attached in the message and hr that is stored by itself. With the final value equal to hr as we demonstrated in section -2-A, the verification operation is a chain of hash operations.

A different final value other than hr suggests the invalidity of the correspondinging public key. Next the sensor nodes verifies SIGSKuid{h(Uid||tt||M)} using PKuid. Upon user revocation and for addition, the sink updates the Merkle hash tree and get a new hr. Using SKsink,the new hr is assigned by the sink. Moreover , each present user also obtains his updated AAI_{UID} from the sink.

ANALYSIS:- In this scheme, to prove the binding to his public key, a user does not need a certificate. Instead , a Merkle hash tree technique is used. A revoked or invalid user public key will never pass the verification, as long as the user holds the up-to-date root node value hr. henceforth, the certificates are no longer necessary or required and can be eliminated, in this scheme. Moreover, the user revocation problem (i.e certificate revocation problem) is now decreased to the problem of updating sensor nodes a single hash value hr, that which requires storage space of only L bytes. Here the assumption is that SHA-1[26], is used,L=20 bytes. But then, the scheme is communication inefficient when N becomes large. The reason for this is that , the size of AAI grows logarithmically with N. So hence, here, we assume L=20 bytes, when N=1,024 and also|AAI|=260 bytes when N=8,192.

C. THE AUTHENTICATION SCHEME BASED ON ENHANCED MERKLE HASH TREE: In the latter scheme, the storage overhead is only one hash value(i.e)L bytes, but the communication overhead is in no way inferior than L*$\log_2$N bytes. So, between the storage and communication overheads a compromise is been made(i.e) to reduce the size of AAI, we increase the number of stored hash values.

Through a diagrammatic representation, we represent how to do it via an example. In fig 1, hr is made public and stored by the authenticator. Hence forth, the user corresponding to leaf node n3 must have AAI:<ha,h(n4)>. But still , if both ha and hb are made public and stored by the authenticator, the corresponding AAI new contains h(n4) only. So it is very obvious that, by trimming down the Merkle hash tree constructed in the above scheme, we can have a set of smaller Merkle hash trees.

The size of the AAI can be reduced to the height of the smaller trees multiplying L bytes , if each sensor node is loaded with all the values of the root nodes corresponding to these smaller trees. In fact, the communication overhead is reduced by K*L bytes, if we remove K levels of the original Merkle tree. However, the storage cost increases to 2^k *l bytes. If we require sensor nodes to store all the leaf values, the scheme is reduced to the trivial memorize-all-keys case, which demands N*L bytes storage space.

ANALYSIS: The value of K is obviously limitless, since sensor nodes are storage constrained. Here, it is given that, m=2^k hash values can be stored by each sensor node, the size of AAI is now L*$\log_2$ N/M bytes. If in case, N=1,024 and M=32, this is 100 bytes; and if N is increased to 8,192 this is 160 bytes. If M is made to be 64, then the size of AAI will be 80 bytes, given N=1,024 and 140 bytes, given N=8,192. When compared to this above basic scheme, this result is much improved to the earlier one, where N=8,192, the message overhead in this enhanced scheme is 120 bytes less than that of the basic Merkle hash tree based scheme. This gain comes at the cost of increased storage overhead, which is new 64*20=1,024 bytes=1.25KB. So hence, this scheme is still inefficient of communication when N is large.

D. ID – BASED AUTHENTICATION SCHEME: In this section, we propose an ID based authentication scheme. Just different to the Merkle hash tree schemes, the proposed ID based authentication scheme requires sensor nodes to memorize the revoked user ID only, and adopt an automatic public update technique.

Now upon user revocation, the sink only needs to broadcast the corresponding user IDs to the sensor nodes. Each sensor node stores a local copy of such revoked IDs only within the current interval and dumps them afterwards. The scheme works as follows,

SCHEME INTIALIZATION: Regarding to the network deployment, we assume that the sink does the following operation;

- Generate the pairing parameters (p,q,E/Fp,G_1,G_2,ê), as described P of G_1,
- Choose two cryptographic hash functions H_1 map-to-point hash function, mapping strings to non-zero elements in G_1 and h_1 mapping arbitrary inputs to fixed length outputs. E.g, SHA -1[26].
- Pick a random number k ε Zq* as the network master secret and set Ppub=kP.
- Preload each sensor node with the public system parameters (p,q,E/Fp,G_1,G_2,ê,H,h,P,Ppub).
- Preload each user Uid with the private key SKUid=kH(Uid||v_1).

MESSAGE BROADCAST AUTHENTICATION: Here, we assume that, to broadcast a message M, the user Uid, first obtains its private key as SKUid=kH(Uid||vi), where vi is the current time interval. Uid then picks a random αεZq* and computes θ=ê(P,P) Uid further computes, Ux,y=h(M||tt||θ)SKUid and σx,y=Ux,y+αP.

Let c=h(M||tt||θ) < σx,y,c> is the signature on message m. The broadcast message is now of form, <Uid,tt,M, σx,y,c. (111).

On receiving message (111), each se3nsor node verifies its authenticity in the following way,

It checks the current time tt' and determines whether or not the received message is fresh.

Here, we take δ as the predefined message propagation time limit. Then, we should have $tt'-tt<=\delta$. If so, the sensor node further computes, $\theta'=\hat{e}(\sigma x,y,P)\hat{e}(H(Uid||vi), Ppub)^{c}$, using the current time interval vi. If the message is authentic, we will have,

$$\theta'= \hat{e}(\sigma x,y,P)\hat{e}(H(Uid||vi),Ppub)^{-c}$$
$$= \hat{e}(cSKUid+\alpha P,P)\hat{e}(H(Uid||vi),kP)^{-c}$$
$$= \hat{e}(cSKUid+\alpha P,P)\hat{e}(kH(Uid||vi),P)^{-c}$$
$$= \hat{e}(SKUid,P)^{c}\hat{e}(P,P)^{\alpha}\ \hat{e}(SKUid,P)^{-c}$$
$$=\theta$$

Therefore, if$h(M||tt||\theta')=h(M||tt||\theta)$, a sensor node considers the message authentic. If the above verification fails, a sensor node considers the message a fabricated or replayed one, and a simply dump it.

ANALYSIS: The pros of the ID based authenticated scheme are two-fold: Initially it eliminates the existence of certificate or the helping authentication information. Therefore, the resulted message size can be reduced.

Next, it requires much smaller storage space to support user revocation. Since now only the revoked user IDs have to be stored.

It is assumed that, a WSN supporting up to 65,535 users, then two bytes are enough for the length of a user ID.

Now only 2,000 bytes=1.95 KB storage space is needed for accumulating the same 1,000 revoked users. But still, the cons of the ID based authentication scheme are also there, since it has a very high computation cost due to the pairing operation involved.

6. QUANTITATIVE PERFORMANCE COMPARISON

In this section, we present a quantitative comparison with respect to the above proposed schemes. We start from analyzing the message sizes providing by different schemes, since the message size is directly related to the energy consumption on message propagation.

A MESSAGE SIZE: The certificate based authentication scheme: the total message size of form(1) equals to,

$|M|+|tt|+|S|GSKUid\ \{h(Uid||tt||M\}|+|CertUid|$, where 1.1 denotes the size of '.' In bytes, In its simplest significantly larger than that of the message in WSNs generally. As in [36], CertUid is atleast 86 bytere, even if ECDSA is used [39]. The total message size of form(1) is then 148 bytes, assuming M20bytes, tt two bytes, and that ECDSA is used.

$|M|+|tt|+|S|GSKUid\ \{h(Uid||tt||M\}|+|Uid|+|PKUid|+|AAIUid|$.

Assume that SHA-I IS USED, UID is two bytes and all the other settings remain the same as latter; we have the total message size equal to (20+2+40+2+20+20*log2N)=84+20*log2N bytes. The total message size of form (II) is further reduced to 82+20*log2N/M, as AAI is now (L*log2N/M) bytes, for its enhanced scheme as presented in section III-C.

If N is increased to 8,192, this is 244 bytes. If m is made to be 64, then the total message size will be 164 bytes, given N=1,024 and 244 bytes given N=8,192. Note that, RSA-1024 is obviously, not achieve here, since total message size of form(II) will be 280+20*log2N/M bytes in this case.

THE ID BASED AUTHENTICATION SCHEME: The total message size of form (111) equals to $|Uid|+|tt|+|M|+|\sigma x,y|+|h(M||tt||\theta)|$.Then we have to find the size of the signature. The second part of the signature i.e., $|h(M||tt||\theta)|$ is is a hash value which should be 20 bytes given SHA-1 is used. $|\sigma x,y|$ is variable. The bilinear map $\hat{e}$ used is the Tate pairing[5]. The elliptic curve E is defined over Fp. The order q of G_1 and G_2 is a 160-bit prime. According to [8], inorder to deliver an equivalent level of security to that of 1024- bit RSA, p should be a 512-bit prime, if G_2 is a q ordered subgroup of a multiplicated group of a finite field F^*p^2. p could be of 340-bit,given the finite field F^*p^3 and 160-bit given the finite field F^*p^6. Therefore the total message of form(111) is 44+|p| bytes, ranging from 64 to 108 bytes.

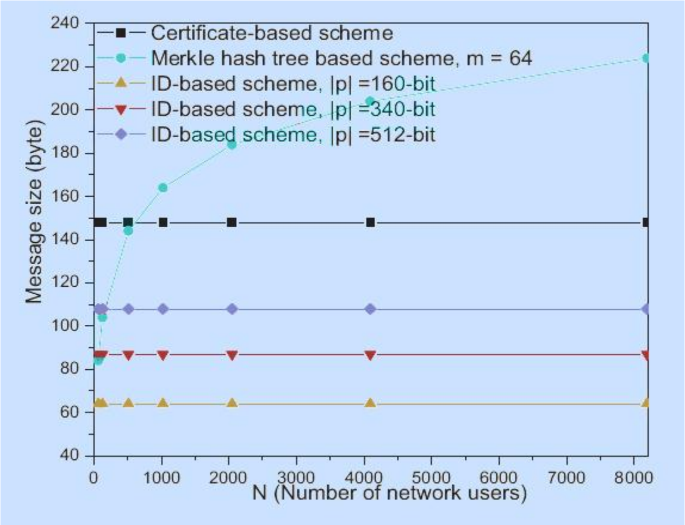


Fig:2 Message sizes with regard to number of network users.

In the fig. the ID- based scheme as the smallest message size as compared to others, when N is larger than 500. At the same time this message size is independent to the number of network users. However, the computational cost is very high. Also the certificate-based scheme as a constant message size of 146 bytes which is also independent to N. Furthermore, Merkle Hash tree based scheme is efficient only when N is upto several hundreds. Therefore this scheme is unsuitable for supporting larger number of users.

B. ENERGY CONSUMPTION ON MESSAGE BROADCAST: In the subsection, to quantify the impact of message length regarding in broadcast in WSNs, we evaluate the energy consumption due to broadcast of messages of different size. We denote by Etr the hop-wise energy consumption for transmitting and receiving one byte. As reported[36], a Chipcon CC1000 radio used in Crossbow MICA2DOT motes consumes 28.6 and 59.2 µJ to receive and transmit one byte respectively, at an effective data rate of 12.4kb/s. We assume a packet size of 41 bytes, 32 for payload and 9 bytes for header[36]. The header, ensuing a 8 byte preamble, consisting of source, destination, length, packet ID, CRC and a control byte[36].

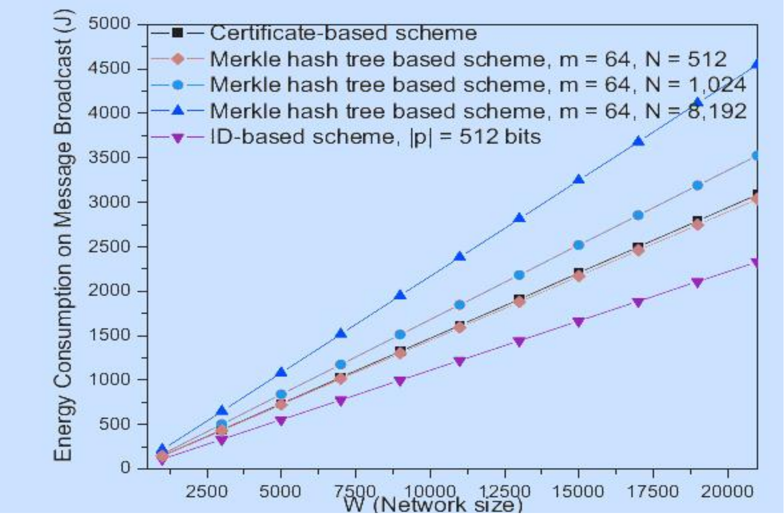


Fig:3 Energy Consumption on Message Broadcast with regard to network

For a certificate based scheme, CertUid is at least 86 bytes [36], even if ECDSA-160 is used. The total message size of form (1) is then 148 bytes, assuming M=20 bytes and tt=2 bytes therefore there 5 packets in total in which 4 of them are 41 bytes long and one is 29 bytes long therefore there should be 233 bytes of transmission. Hence, hop-wise energy consumption on transmitting message (1)=233*59.2µJ=13.79mJ and on receiving = 233*28.6µJ=6.66mJ. To broadcast a message to the whole WSN, when the simple flooding technique is used, each sensor notes should atleast retransmit once and receive w'(neighborhood density) times the same message. Hence, the total energy consumption on message broadcast will be W*(13.79+6.66*w')mJ. The above illustrates the broadcast energy consumption assuming w'=20 clearly ID based schemes offers a much lower energy consumption compared to others. Merkle Hash based scheme outperforms of the certificate based scheme, when N is no more than 512.

C. ENERGY CONSUMPTION ON COMPUTATION: Now we calculate the computation overhead of the proposed schemes in terms of energy consumption. In certificate based schemes, it is mainly due to the verification of two ECDSA signatures. In Merkle hash based scheme it is due to verification of one ECDSA signature and a number of hash operations. In the ID-based scheme, it is due to the verification of ID based signatures.

Assuming |p|=512-bit, |q|=160-bit and the embedded degree of E/Fp=2. We assume that the sensor CPU is a low-power high performance 32 bit INTEL PXA255 processor at 400MHz. It's active and idle modes are 411 and 121 mW respectively. It was reported in [7] that it takes 752 ms to compute the Tate pairing with the similar parameters as ours on the 32 bit ST11 smartcard microprocessor at 33MHz. Therefore, The computation of the Tate pairing on PXA255 roughly needs 33/400*752 = 62.04ms appx and Ep is 25.5mJ appx. To verify the ID based signature wise one exponentiation in G_2, one MapToPoint hash function evaluation, and two evaluations takes the most running time of the signature verification operation. Lacking of specific energy cost data of the MapToPoint hash operation on embedded processors, we use energy consumed on pairing evaluation for the sake of simplicity, which ranges from Ep to 2Ep it is reported in[4] that it takes 92.4ms to verify a ECDSA-160 signature with the similar parameters on a 32-bit a ARM microprocessor at 80 MHz therefore energy consumption roughly is 7.6mJ.

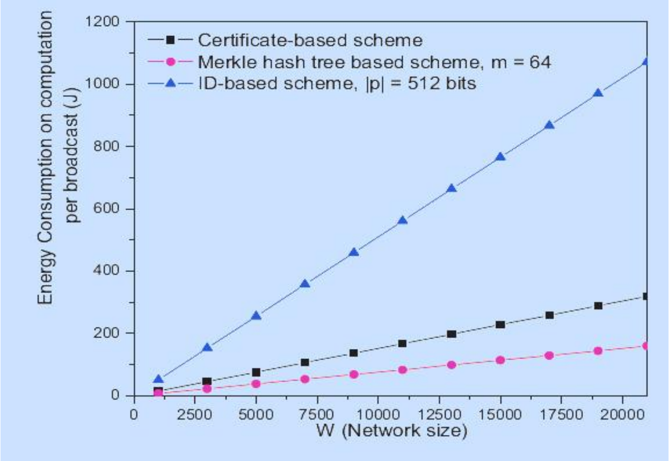
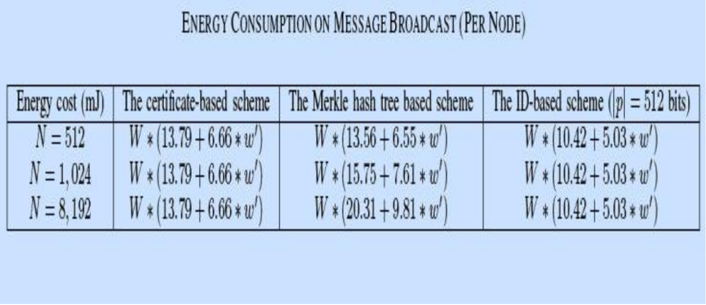


Fig:4 Energy Consumption computation on regard to network size.

In the above fig. it gives the energy consumption on computation when the message is broadcast under different message forms. First, for a message broadcast, energy cost on propagation is much higher than that of computation. Second the ID-based scheme incurs a much higher computation cost compared with others. ID-based scheme is still relatively efficient especially when W is large. An emerging technique, ID-based cryptography is under rapid development. Its computation cost can be expected to decrease. Moreover, the computation cost can be further saved by batch verification of multiple signatures when applicable [37].



ENERGY CONSUMPTION ON MESSAGE BROADCAST (PER NODE)

Energy cost (mJ)	The certificate-based scheme	The Merkle hash tree based scheme	The ID-based scheme ($\|p\| = 512$ bits)
$N = 512$	$W * (13.79 + 6.66 * w')$	$W * (13.56 + 6.55 * w')$	$W * (10.42 + 5.03 * w')$
$N = 1,024$	$W * (13.79 + 6.66 * w')$	$W * (15.75 + 7.61 * w')$	$W * (10.42 + 5.03 * w')$
$N = 8,192$	$W * (13.79 + 6.66 * w')$	$W * (20.31 + 9.81 * w')$	$W * (10.42 + 5.03 * w')$

The next generation of sensors such as Intel Mote 2[15] is expected to use even more powerful processor. Hence, ID-based scheme can have a good application potential in the near future. Third, when W < 500, the Merkle hash tree based scheme is overall best choice. Fourth, when W is large it still remains to find a satisfying scheme. We leave this as our future work.

7. CONCLUDING REMARKS:

In this paper, we first dealt with the problem of multi sender broadcast authentication in WSNs. We found that symmetric- key based solution, µTESLA are insufficient for this problem by identifying serious security vulnerability: the delayed authentication can lead to severe DoS attacks, due to the stringent energy and bandwidth constraints in WSNs. We suggested several effective PKC-based schemes to address the proposed problem. Both computational and communication costs are minimized. We also analyzed its performance and security resilience. A quantitative energy consumption analysis was given in detail. We believe that this paper can serve as the start point towards fully solving the important multisender broadcast authentication problem in WSNs.

REFERENCES

[1] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102-16, Aug. 2002.

[2] I. Akyildiz and I. Kasimoglu, "Wireless sensor and actor networks: Research challenges," *Ad Hoc Networks*, vol. 2, no. 8, pp. 351-367, 2004.

[3] R. Amirtharajah and A. Chandrakasan, "Self-powered signal processing using vibration-based power generation, " *IEEE J. Solid-State Circuits*, vol. 33, pp. 687-695, 1998.

[4] M. Aydos, T. Yanik, and C. Koc. "An high-speed ECC-based wireless authentication protocol on an ARM microprocessor," in *Proc. 16th Computer Security Applications Conf.*, 2000, pp. 401-409.

[5] P. Barreto, H. Kim, B. Bynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proc. CRYPTO'02, Ser. LNCS*, vol. 2442, pp. 354-368, Springer-Verlag, 2002.

[6] P. Barreto, B. Lynn, and M. Scott, "On the selection of pairing-friendly groups in selected areas in cryptography," in *Proc. SAC'03, Ser. LNCS*, vol. 3006, pp. 17-25, Springer-Verlag, 2004.

[7] G. Bertoni, L. Chen, P. Fragneto, K. Harrison, and G. Pelosi1, "Computing state pairing on smartcards," White Paper, STMicroelectronics, 2005 [Online].

[8] D. Boneh and M. Franklin, "Identify-based encryption from the weil pairing," in *Proc. CRYPTO'01, Ser. LNCS*, vol. 2139, pp. 213-229, Springer-Verlag, 2001.

[9] Crossbow Technology Inc, "Wireless sensor network," 2004 [Online].

[10] W. Du, R. Wang, and P. Ning "An efficient scheme for authenticating public keys in sensor networks," in *Proc. 6th ACM International Symposium Mobile Ad Hoc Networking Computing (MobiHoc)*, 2005, pp. 58-67.

[11] G. Gaubatz, J. Kaps, and B. Sunar, "Public keys cryptography in sensor networks–Revisited," in *Proc. 1st European Workshop Security Ad-Hoc Sensor Networks (ESAS)*, Aug. 2004, vol. 3313, pp. 2-18.

[12] F. Hess, "Efficient identity based signature schemes based on pairings," in *Proc. SAC'02*, Aug. 2002, pp. 310-324.

[13] Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: A Defense against wormhole attacks in wireless ad hoc networks," in *Proc. IEEE INFOCOM*, 2003, pp. 1976-1986.

[14] Intel Corp., "Intel PXA255 processor electrical, mechanical, and thermal specification,"

[15] Intel Corp., "Intel mote 2 overview,"

[16] A. Kansal, D. Potter and M. Srivastava, "Performance aware tasking for environmentally powered sensor networks," in *Proc. ACM Joint International Conf. Measurement Modeling Computer Syst. (SIGMETRICS)*, 2004, pp. 223-234.

[17] A. Kansal and M. Srivastava, "An environmental energy harvesting framework for sensor networks," in *Proc. ACM/IEEE Int'l Symposium Low Power Electronics Design (ISLPED)*, 2003, pp. 481-486.

[18] T. Kerins, W. Marnane, E. Popovici, and P. Barreto, " Efficient hardware for the tate pairing calculation in characteristic three," in *Proc. Workshop Cryptographic Hardware Embedded Syst. (CHES'05)*, Aug./Sep. 2005, pp. 412-426.

[19] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks," in *Proc. 10th Annual Network Distributed Syst. Security Symposium (NDSS'03)*, 2003, pp. 263-276.

[20] D. Liu and P. Ning, "Multi-level mTESLA: Broadcast authentication for distributed sensor networks," *ACM Trans. Embedded Computing Systems (TECS)*, vol. 3, no. 4, pp. 800-836, 2004.

[21] D. Liu, P. Ning, S. Zhu, and S. Jajodia, "Practical broadcast authentication in sensor networks," in *Proc. 2nd Annual International Conf. Mobile Ubiquitous Syst.: Networking Services (MobiQuitous 2005)*, July 2005, pp. 118-132.

[22] 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," *IEEE Pervasive Computing, Special Issue on Pervasive Computing for First Response*, 2004, vol. 3, no. 4, pp. 16-23.

[23] S. Meininger, J. Mur-Miranda, R. Amirtharajah, A. Chandrakasan, and J. Lang, "Vibration-to-electric energy conversion," *IEEE Trans. Very Large Scale Integration (VLSI) Systems*, vol. 9, pp. 64-76, 2001.

[24] R. Merkle, "Protocols for public key cryptosystems," in *Proc. IEEE Symposium Research Security Privacy*, Apr. 1980, p. 122.

[25] National Institure of Standards and Technology: Proposed Federal Information Processing Standard for Digital Signature Standard (DSS). Federal Register, vol. 56, no. 169, pp. 42980-42982, 1991.

[26] NIST, "Digital hash standard," Federal Information Processing Standards Publication 180-1, Apr. 1995.

[27] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and D. Tygar, "SPINS: Security protocols for sensor networks," in *Proc. 7th Annual International Conf. Mobile Computing Networks (MobiCom'01)*, July 2001, pp. 521- 534.

[28] K. Ren, W. Lou, and Y. Zhang, "LEDS: Providing location-aware end-to-end data security in wireless sensor networks,"in *Proc. IEEE INFOCOM*, 2006, pp. 1-12.

[29] K. Ren, K. Zeng, and W. Lou, "A new approach for random key pre-distribution in large scale wireless sensor networks," *J. Wireless Commun. Mobile Computing (WCMC)*, vol. 6, no. 3, pp. 307-318, 2006.

[30] K. Ren, K. Zeng, W. Lou, and P. Moran, "On broadcast authentication in wireless sensor networks," in *Proc. WASA 2006, LNCS*, Aug. 2006, vol. 4138, pp. 502-514,.

[31] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp.120-126, 1978.

[32] M. Scott, "Computing the tate pairing," in *Proc. RSA Conference (CTRSA' 05)-Cryptographers' Track*, Feb. 2005.

[33] M. Scott, N. Costigan, and W. Abdulwahab, "Implementing cryptographic pairings on smartcards," in *Proc. Cryptographic Hardware Embedded Syst.-CHES 2006: 8th International Workshop, LNCS*, Oct. 2006, vol. 4249, pp. 134-147.