2010

An authentication framework for Wireless Sensor Networks using identity-based signatures

Rehana Yasmin
University of Birmingham

Eike Ritter
University of Birmingham

Guilin Wang
University of Birmingham, guilin@uow.edu.au

An authentication framework for Wireless Sensor Networks using identity-based signatures

Abstract

In Wireless Sensor Networks (WSNs), authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate DoS attacks exploiting the limited resources of sensor nodes. Resource constraints of sensor nodes are hurdles in applying strong public key cryptographic based mechanisms in WSNs. To address the problem of authentication in WSNs, we propose an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user. The proposed framework is also evaluated using the most efficient and secure identity-based signature schemes.

Disciplines

Physical Sciences and Mathematics

Publication Details

Yasmin, R., Ritter, E. & Wang, G. (2010). An authentication framework for Wireless Sensor Networks using identity-based signatures. 2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010) (pp. 882-889). Piscataway, New Jersey, USA: IEEE.

2010 10th IEEE International Conference on Computer and Information Technology (CIT 2010)

An Authentication Framework for Wireless Sensor Networks using Identity-Based Signatures

Rehana Yasmin, Eike Ritter, Guilin Wang
Dept. of Computer Science
University of Birmingham, B15 2TT
Birmingham, United Kingdom
Email: {R.Yasmin, E.Ritter, G.Wang}@cs.bham.ac.uk

***Abstract*—In Wireless Sensor Networks (WSNs), authentication is a crucial security requirement to avoid attacks against secure communication, and to mitigate DoS attacks exploiting the limited resources of sensor nodes. Resource constraints of sensor nodes are hurdles in applying strong public key cryptographic based mechanisms in WSNs. To address the problem of authentication in WSNs, we propose an efficient and secure framework for authenticated broadcast/multicast by sensor nodes as well as for outside user authentication, which utilizes identity based cryptography and online/offline signature schemes. The primary goals of this framework are to enable all sensor nodes in the network, firstly, to broadcast and/or multicast an authenticated message quickly; secondly, to verify the broadcast/multicast message sender and the message contents; and finally, to verify the legitimacy of an outside user. The proposed framework is also evaluated using the most efficient and secure identity-based signature schemes.**

I. Introduction

Low cost and immunity from cabling have become strong motivations for many applications of Wireless Sensor Networks (WSNs) like environmental monitoring, disaster handling, traffic control and various military applications [1], [8]. In these applications, sensor devices sense or monitor physical and environmental changes like temperature, pressure, etc. and communicate this data to other nodes over a wireless network. Authentication of this data as well as of the data source is critical, as the data may ultimately be used to assist in some significant situations. In some applications, there are also outside users of the sensor network who are interested in the data collected by the sensor nodes. User authentication is equally important as data collected by the sensor nodes may be confidential, or in some situations only the subscribed users are allowed to access it.

However, the radio links are insecure, facilitating an adversary in intercepting, injecting or modifying communication. Resource limitations of sensor nodes make it difficult to apply strong traditional cryptographic mechanisms to secure the communication. Moreover, WSNs are often deployed in a hostile environment where they are physically accessible by an adversary who can discover cryptographic material e.g., keys, stored on the sensor nodes. In this scenario, it is challenging to enable sensor nodes to accept communication only from the legitimate entities and to distinguish between valid and fake or modified communication.

In this paper, we address the problem of authentication in WSNs, particularly *authenticated broadcast/multicast by sensor nodes* and *outside user authentication*. The problem of *authenticated broadcast/multicast by sensor nodes* is not addressed by the existing authentication schemes for WSNs. Symmetric schemes like μTESLA [21] and its variations [11], [17], [18] proposed for base station broadcast authentication use Message Authentication Code (MAC) and are efficient in terms of processing and energy consumption. However, they suffer from the following issues:

- Provide delayed authentication.
- Very slow for large scale sensor networks.
- DoS attack against storage due to late authentication.
- Not scalable in terms of number of senders.
- Multiple senders cannot broadcast simultaneously.
- If a sensor node wants to broadcast a message, it unicasts the message to the base station, which then broadcasts that message on behalf of that node.

An extension of μTESLA [7], [15] attempts to enable sensor nodes to broadcast messages to nearby sensor nodes only, however, it inherits the weaknesses of μTESLA. Asymmetric schemes, for example digital signatures, overcome the problems of symmetric schemes but require public keys and certificates on the receiver side to verify signed messages. Moreover, it is more time and power consuming for sensor nodes to sign a message than to compute a MAC. Digital signature based authentication schemes discussed in [6], [23], [24] allow broadcast by powerful senders only and therefore, are not suitable for resource constrained motes.

In *outside user authentication*, the number of outside users of sensor nodes data is also restricted due to the fact that sensor nodes need some user specific information to verify a user request. For example, *RRUASN* [4] requires the public key and certificate of a user on the receiver side, which are sent with every user request (increasing transmission overhead). *DP^{2}AC* [32] uses a token to authenticate a user and stores every used token to control re-usability.

To handle the above mentioned issues, we propose an authentication framework for WSNs, using Identity-based

978-0-7695-4108-2/10 $26.00 © 2010 IEEE
DOI 10.1109/CIT.2010.165

Cryptography and Online/Offline Signature (OOS) schemes, comprised of two authentication schemes; one for quick *authenticated broadcast/multicast by sensor nodes* and another for *outside user authentication*. The first scheme allows every sensor node in the network to broadcast or multicast authenticated messages very quickly without the involvement of the base station. All potential receivers can verify a message sent by any sender node in the network. It also allows sensor nodes on the path from the sender node to the receivers to verify a valid message and drop false injected data. The second scheme enables all sensor nodes in the network to verify the legitimacy of any outside user without storing user specific information. It allows a maximum possible number of legitimate users to access data from sensor nodes in a secure way. This scheme first authenticates a user and then establishes a session key for secure exchange of user queries and sensor nodes data.

The proposed framework uses Identity-based Online/Offline Signature (IBOOS) scheme (an ID-based version of OOS) for the first scheme and Identity-based Signature (IBS) scheme for the second scheme. IBS schemes [26] allow a user to use his identity information such as name, email address etc., which is unique to him, as his public key while the corresponding private key is generated by a private key generator (PKG). It eliminates the need of a certificate signed by a certification authority to extract the public key for the verification of a signed message. A message signed with a user's private key can be verified using his ID.

Online/Offline Signature (OOS) schemes [12] divide the process of message signing into two phases, the *Offline* phase and the *Online* phase. The *Offline* phase is performed before the message to be signed becomes available. This phase performs the most computations of signature generation and results in a partial signature. Once the message is known, the *Online* phase starts. This phase retrieves the partial signature calculated during the *Offline* phase and performs some minor quick computations to obtain the final signature. The *Online* phase is assumed to be very fast, consisting of small computations while the *Offline* phase can be performed by other resourceful device. OOS enables a resource constrained sensor node to sign a message quickly, once it has some critical event to report. IBOOS is the ID-based version of OOS, where a message signed with a signer's private key is verified using signer's ID.

The primary objective of this framework is to design an authentication mechanism which solves the above mentioned authentication problems efficiently in terms of power consumption, processing time and storage overhead. The primary advantage of this research work is that it does not restrict the solution to the existing IBS and IBOOS schemes, rather it provides a general authentication framework which can be reused with new IBS and IBOOS schemes. Once new IBS and IBOOS schemes are available, which are more secure and efficient than the existing IBS and IBOOS schemes, they replace the existing ones to achieve better results. Security and performance of the proposed framework are also evaluated and compared with some existing signature based authentication schemes for WSNs. This paper makes the following main contributions:

- Points out the need of quick authenticated broadcast and/or multicast by all sensor nodes in the network and proposes a secure and efficient solution to this problem without the involvement of the base station. To the best of our knowledge, this is the first attempt to highlight and handle this problem;
- Proposes the use of online/offline signature schemes for sensor broadcast. To the best of our knowledge, this is the first application of online/offline signatures in WSNs;
- Provides a secure and efficient identity-based authentication framework which can also utilize new IBS and IBOOS schemes to achieve improved performance.

Organization: Section 2 discusses motivations, section 3 introduces the cryptographic primitives, section 4 presents our proposed framework, section 5 evaluates its security & performance and section 6 concludes the paper.

II. Authentication in WSN

Authentication in WSNs can be divided into three categories, namely base station to sensor nodes, sensor nodes to other sensor nodes, and outside users to sensor nodes. The problem of authenticated broadcast by the base station has been widely addressed [6], [11], [17], [18], [21]. We focus on the other two categories, i.e., authenticated broadcast/multicast by the sensor nodes and outside user authentication.

A. Authenticated Broadcast/Multicast by Sensor Nodes

There are many critical situations where a sensor node requires to send a quick message. For example:

- In a forest fire alarm application [27], sensor nodes deployed in a forest should immediately inform authorities about the event and the exact location of the event before the fire spreads uncontrollably.
- In a traffic application [5], whenever a sensor node senses an accident (or a traffic jam) on the road it sends an immediate message in all directions to alert other traffic approaching this location.
- Consider the military application scenario discussed in [27], where a troop of soldiers needs to move through a battlefield. Sensor nodes deployed there detect the presence of the enemy and broadcast this information immediately throughout the network. Soldiers, passing near these sensor nodes, use this information to strategically position themselves in the battlefield.

All these scenarios require a message to be sent as quickly as possible. Due to wireless media, transmission and reception of a message consume considerable time. Moreover,

in most cases a message propagates through several hops to reach the desired destinations. Therefore, the signature generation and the verification times should be as small as possible. A delayed message may have undesirable effects. For example, it may help a fire spreading uncontrollably and a traffic jam becoming worse. A delayed message about the presence of an enemy in the battlefield may cause the deaths of soldiers while moving through the battlefield. In all the above situations, message authentication is equally important otherwise a malicious entity may exploit its absence. For example, an adversary may send fake messages to block traffic towards a specific region or to turn traffic towards a specific direction. In battlefield, sensor nodes added by the enemy can disseminate wrong information about enemy's movement, thus deceiving soldiers.

Moreover, in all the above mentioned scenarios, sensor nodes on the path from the sender node to the receiver(s) relay the messages towards destination. Wireless communication allowing an adversary to inject false messages during multi hop forwarding [19] causes sensor nodes to relay false data and deplete their energy. Hence, sensor nodes on the path should be able to authenticate and filter out false messages as early as possible to save relaying energy [33], [34]. Therefore, they are also potential receivers of these messages, arising the need of *authenticated multicast* by sensor nodes. In battlefield application, all sensor nodes in the network are potential receivers of critical information, arising the need of *authenticated broadcast* by sensor nodes.

To summarize, all these scenarios require a secure mechanism which, on one hand, enables all sensor nodes in the network to send an immediate authenticated message to report a critical situation, and on the other hand, enables every receiver to verify this message. For simplicity, both broadcast and multicast are referred as broadcast in the rest of this paper.

B. User Authentication

Sensor nodes data may be confidential and in some situations only the subscribed users, who have paid, are allowed to obtain this data. A user authentication mechanism aims to prevent unauthorized users to access data from sensor nodes. Usually, a mechanism to provide an outside user access to sensor nodes data requires three tasks:

1) *User Authentication* allows only legitimate users of the data to access it.
2) *Access Control* allows a user to access only the data which he is entitled to access.
3) *Session Key Establishment* enables secure exchange of user queries and confidential data between users and sensor nodes.

In *centralized* user authentication, all users are authenticated through the base station. This mechanism is easy to deploy because the base station is a powerful device which can perform complex cryptographic operations. However, this approach has a few drawbacks. Firstly, it makes the base station a single point of failure. Secondly, it causes sensor nodes near the base station to deplete their energy quickly as for every user request, they relay packets between base station and queried sensor nodes. Furthermore, it causes a severe DoS attack where an adversary sends fake request messages causing sensor nodes to relay them towards the base station for verification, increasing network traffic and depleting their energy. User authentication schemes discussed in [10], [16], [29], [30] all suffer from these problems. To avoid this kind of DoS attack, a user should be locally authenticated by the sensor nodes without the involvement of a third entity, i.e., a *distributed* approach. This approach reduces traffic congestion and transmission overhead within the network. However, it puts the burden of authentication on sensor nodes. As sensor nodes are resource constrained devices as compared to the base station, a lightweight user authentication mechanism is needed for sensor nodes to verify authenticity of the users.

III. Cryptographic Primitives

A. ID-based Signature (IBS)

Definition 1. *An ID-based signature (IBS) scheme consists of four algorithms as follows:*

1) ***System Setup (SS):*** *Given a security parameter 1^k, outputs a master secret key SK_{PKG} and system parameters SP.*
2) ***Key Extraction (KE):*** *Given a user's identity ID_i and master secret key SK_{PKG}, outputs a corresponding private key D_{ID_i}, i.e., $D_{ID_i} \leftarrow KE(ID_i, SK_{PKG})$.*
3) ***Signature Generation (Sign):*** *Given a message m and a signing key D_{ID_i}, outputs a signature σ, i.e., $\sigma \leftarrow Sign(m, D_{ID_i})$.*
4) ***Signature Verification (Ver):*** *Given a message m, user's identity ID_i, a signature σ and system parameters SP, returns 1 if the signature is valid or 0 if not. Namely, $0/1 \leftarrow Ver(m, ID_i, \sigma, SP)$.*

B. ID-based Online/Offline Signature (IBOOS)

Definition 2. *An ID-based online/offline signature (IBOOS) scheme consists of five algorithms as follows:*

1) ***System Setup (SS):*** *Same as in Definition 1.*
2) ***Key Extraction (KE):*** *Same as in Definition 1.*
3) ***Offline Signing (OffSign):*** *Given a signing key D_{ID_i} and system parameters SP, outputs an offline signature S, i.e., $S \leftarrow OffSign(D_{ID_i}, SP)$.*
4) ***Online Signing (OnSign):*** *Given a message m and an offline signature S, outputs an online signature σ, i.e., $\sigma \leftarrow OnSign(m, S)$.*
5) ***Signature Verification (Ver):*** *Given a message m, user's identity ID_i, signature σ and system parameters SP, returns 1 if the signature is valid and 0 if not. Namely, $0/1 \leftarrow Ver(m, ID_i, \sigma, SP)$.*

IV. The Proposed Authentication Framework

In this section, we present the proposed authentication framework which is composed of two authentication schemes. The first two phases of both schemes i.e., the *System Initialization* and the *Key Generation* are performed once, before the deployment of the WSN.

A. Authenticated Broadcast by Sensor Nodes

For authenticated broadcast, a message is signed using IBOOS. Some IBOOS schemes [25] allow reuse of a partial signature computed in the offline phase to sign more than one message, which decreases energy consumption. Moreover, OOS allows the offline phase to be performed on some other resourceful device. Hence, it is possible for the base station to perform the complex computations of the offline phase and distribute the partial signature to the sensor nodes. The sensor nodes then only perform small, energy efficient computations of the online phase.

System Initialization: In our scheme, the base station plays the role of PKG, a trustworthy entity, and initializes the system in this phase. Let SK_{BS} be the secret key of the base station. The base station computes the corresponding public key PK_{BS} and sets up the public system parameters SP which include PK_{BS}. The master secret key SK_{BS} is only kept by the base station while SP is made public.

Key Generation: In this phase, the base station computes the secret keys of all sensor nodes corresponding to their IDs using the master secret key SK_{BS}. For a sensor node i with identity ID_i, the corresponding secret key is D_{ID_i} computed as $D_{ID_i} \leftarrow KE(ID_i, SK_{BS})$. IDs, corresponding private keys and system parameters are stored on sensor nodes before deployment. Hence, every sensor node i stores $\{ID_i, D_{ID_i}, SP\}$.

Message Broadcast and Authentication: In this phase, the sensor nodes broadcast authenticated messages which are verified using their IDs. The signature generation of a broadcast message is divided into two phases:

Offline phase: The offline phase is performed by the base station, before the message to broadcast becomes available. The offline signature algorithm runs in this phase on the base station, and performs the most signature computations to calculate the partial signature S as $S \leftarrow OffSign(D_{ID_i}, SP)$. The resulting partial signature S is stored on sensor node i.

Online phase: Whenever a sensor node i senses an event which requires quick reporting, the online phase starts. In this phase, the sensor node i retrieves the partial signature S calculated during the offline phase. The online signature algorithm runs in this phase on sensor node i, and performs very minor and fast computations to obtain the final signature σ over message m as $\sigma \leftarrow OnSign(m, TS, ID_i, S)$, where TS is the current time stamp. The final broadcast message then contains the message m, time stamp TS, identity of the sensor node ID_i and the signature σ i.e., $\{m, TS, ID_i, \sigma\}$.

Authentication: On receiving a broadcast message, receiver first checks the time stamp TS to avoid the verification of a replayed message. If it is a fresh one, the receiver further proceeds with signature verification; otherwise it discards the message. The receiver verifies the signature σ using sender node's identity ID_i and other system parameters as $0/1 \leftarrow Ver(m, TS, ID_i, \sigma, SP)$.

If the verification succeeds, the receiver accepts the message; otherwise it discards it. If necessary, it rebroadcasts the message to sensor nodes belonging to the next hop.

Sender Revocation: To revoke a compromised sensor node i, the base station broadcasts its identity ID_i to all other sensor nodes in the network, who store ID_i. If in the future a sensor node receives a message containing ID_i, it simply rejects the message without going through authentication process. An adversary is assumed to compromise only a few sensor nodes in the network. If the adversary compromises majority of the sensor nodes, it will break down all the security mechanisms. Therefore, storing the IDs of few compromised nodes would incur a reasonable storage overhead for sensor nodes. Moreover, the base station can periodically update system parameters and secret keys of all legitimate sensor nodes excluding malicious nodes. However, this update might be costly. Another possible solution is to manually detach these compromised sensor nodes from the sensor network.

B. User Authentication

In order to access data from sensor nodes, a user first registers himself to the base station and obtains his private key and other system parameters. After that, whenever he wants to access data, he sends a signed request to the sensor nodes in his range who verify his signed request locally using his ID. If the verification succeeds, the sensor nodes and the user both compute a session key for further communication. This session key establishment enables the user to send encrypted queries to the sensor nodes and get confidential data from them.

System Initialization and **Key Generation** phases are the same as described in the first scheme.

User Registration: This phase is performed whenever a new user is added to the system. In this phase, a user U with identity ID_U registers with the system. The base station computes his private key D_{ID_U} as $D_{ID_U} \leftarrow KE(ID_U, SK_{BS})$. The user gets his private key and other system parameters from the base station through a secure channel. Hence, every user gets $\{ID_U, D_{ID_U}, SP\}$.

User Authentication: In order to query sensor nodes, a user U sends his signed request to the sensor nodes in his range. Let N be the number of sensor nodes in his range. U's request contains his request message RM, current time stamp TS, identity ID_U, and the signature σ calculated on these parameters using his secret key i.e., $U \rightarrow N$: $\{RM, TS, ID_U, \sigma\}$, where $\sigma = Sign((RM, TS, ID_U), D_{ID_U})$.

On receiving a user request, each sensor node first checks the time stamp TS to filter out a replayed request message. If it is a fresh one, sensor node verifies the signature using U's ID and other system parameters stored on it as $0/1 \leftarrow Ver(RM, TS, ID_U, \sigma, SP)$. If the verification succeeds, it proceeds with session key establishment else it stops further computation and communication.

Session Key Establishment: To provide secure transmission of data from sensor nodes to user, a session key needs to be established. For this purpose, any secure key exchange protocol could be used here. However, an identity based one-pass key establishment protocol is an attractive choice for resource constrained sensor nodes. It reduces the number of messages exchanged during key establishment phase i.e., only one party computes and sends its ephemeral key to the other party, for example, identity based one-pass key establishment protocol presented in [13]. That single message can be combined with user request message (in user authentication phase) which is signed by the user. It further reduces the communication. It also avoids the man-in-the-middle attack. The only message exchanged between the user U and the sensor node A for key establishment will be signed by U and verified by A, which makes it difficult for an intruder to send fake ephemeral key to the sensor nodes on behalf of U.

To establish a session key, U randomly computes its ephemeral key R. U then sends R, together with his signature, to A in authentication phase. If U's signature is valid and user authentication succeeds, both A and U compute session key SK using the key derivation function χ as $SK = \chi(ID_A||ID_U||TS||T_{AU})$, where TS is the time stamp to avoid replayed messages and T_{AU} is a common secret computed by both parties using R and their secret keys as described in [13]. At this point, the session key SK is ready for encrypting data.

User Revocation: User revocation can be divided into two cases; firstly, to revoke a user whose access time period has been expired, and secondly, to revoke a malicious user. These two cases can be treated differently. To handle the first case, at the time when base station calculates the secret key for a user U, the expiry time ET of the user can be used as a parameter to calculate the secret key. After his access time period expires, his secret key will automatically expire. If he now sends a signed request, it will not pass verification. In the second case, the base station issues an authenticated revocation list containing malicious user's ID. Sensor nodes store it until the malicious user's expiry time is passed. Thus, if next time that user attempts to access data from sensor nodes, the sensor nodes reject his request without going through authentication process. After his access time expiration, his secret key will expire and he will not be able to successfully authenticate himself to the system. In WSN, the case of the malicious users is not very common. Therefore, storing IDs of malicious users until their expiry time will not impose an unreasonable storage overhead on sensor nodes. To efficiently handle storage, user's access period can be kept short so that sensor nodes do not store malicious users' IDs for a long time. After that time period only the private keys of the legitimate users are updated for next time period. The duration of this period depends on how frequently the event of the malicious users occur.

Although some figures would help to improve the readability of framework, space limitation does not allow it.

C. Instantiation of the Proposed Framework

There are many IBS and IBOOS schemes available, for example, based on ECC and RSA signatures. Verifying RSA signature is efficient for sensor nodes [14] since we can set small verification exponents. This fact can be utilized in user authentication scheme, where sensor nodes only verify a signed user request. However, RSA based signatures are large, resulting in a considerably increased message size. ECC based signatures are equally useful for signing and verification of messages and have short signature sizes. Therefore, for WSN, ECC based signatures are considered more efficient than RSA signatures. To instantiate the proposed authentication framework, we have selected the most secure and efficient ECC based signature schemes from the available IBS and IBOOS schemes. Keeping in mind the security and efficiency requirements, an IBS scheme given in [6] is selected for user authentication scheme while two different IBOOS schemes given in [25] and [31] are selected to evaluate sensor broadcast scheme.

ID-based Signature (IBS) Schemes: ID-based signature schemes are suitable for the proposed user authentication scheme. IBS scheme in [6] presents an ID-based signature which is actually an improvement over **BNN-IBS** [2] to reduce the signature size. Security of this signature scheme depends on *Elliptic Curve Discrete Logarithm Problem*.

ID-based Online/Offline Signature (IBOOS) Schemes: ID-based online/offline signature schemes are suitable for the proposed sensor broadcast authentication scheme. An IBOOS scheme in [25] presents a method to convert any underlying signature scheme into an online/offline signature scheme. The Offline signature in this scheme can be securely reused to sign more than one message. This signature scheme is proved to be existentially unforgeable. Its security depends on *Discrete Logarithm Problem*. Unlike [25], an IBOOS scheme presented in [31] provides a direct online/offline signature scheme, which does not require another underlying signature scheme. This signature scheme is existentially unforgeable under adaptive chosen message attacks.

V. Evaluation

A. Security Analysis

This section analyses the security achieved by the proposed authentication framework.

Authentication: Authentication is achieved as only the legitimate broadcast senders and the outside users with valid secret keys can sign a message.

Verification: Every sensor node can verify a broadcast message by any sender and authenticity of any outside user.

Integrity: Provides message integrity as any changes made in the contents of the messages during transmission are detected through signature verification.

Freshness: Replayed data can be distinguished through timestamp, providing freshness of data.

Session Key: After successful user authentication, session key establishes a secure communication between the user and the sensor nodes.

Now we consider some usual security threats and show how our proposed framework counters them:

1) *Active attack:* The proposed framework employs secure digital signature schemes providing strong authentication and message integrity, and making it impossible for an intruder to sign or modify a valid message sent by another legitimate sender. Time stamp prevents replay of a broadcast message or a previous successful authentication message by a valid user.
2) *DoS attack:* The proposed sensor broadcast scheme provides authentication without any delay. Hence, it prevents DoS attack faced in μTESLA. In user authentication scheme, a user is locally authenticated by the sensor nodes, and not by the base station, which avoids the DoS attack caused by fake intruder's requests.
3) *Node Compromise Attack:* In symmetric key schemes, where a single key or a subset of keys are used by more than one sensor node to calculate a MAC for a message, a compromise of a single node enables an intruder to impersonate all sensor nodes sharing that MAC key(s). In our scheme, an intruder can only impersonate the compromised node. Furthermore, with revocation process he will not be able to successfully broadcast further messages in the network.
4) *False Data Injection Attack:* The proposed sensor broadcast scheme enables all sensor nodes on the message path, during multi-hop forwarding, to verify and filter out false injected data earlier.

B. Performance Analysis

This section evaluates the performance of the proposed authentication framework.

Broadcast by Sensor Nodes: Unlike μTESLA, in our proposed sensor broadcast scheme, a sensor node can broadcast a message itself without the involvement of base station.

Quick Broadcast: An online/offline signature scheme performs the most time consuming offline phase of message generation beforehand. It enables sensor nodes to sign and broadcast a message quickly once the message is known.

Storage Efficiency: As sensor nodes do not store IDs and corresponding public keys of all broadcast senders and outside users for verification, it provides storage efficiency.

Computation Efficiency: In sensor broadcast, by performing the offline phase on base station, the sensor nodes are only left with the online phase computation which is very efficient in terms of time and energy consumption.

Communication Efficiency: ID-based schemes do not require a broadcast sender or an outside user to send public keys/certificates with all messages, thus reducing communication overhead.

Multiple Senders: ID-based signatures handle public keys/certificates issue. Therefore, the proposed framework allows multiple broadcast senders and outside users.

Scalability: New sensor nodes and outside users can be added to the WSN easily at any time. Preloaded with ID, secret key and public parameters, new sensor nodes can broadcast messages as well as verify messages by any other broadcast sender. New users simply need to register themselves to the base station and get their secret information corresponding to their IDs.

C. Discussion

This section gives a rough-and-ready estimation of applying our proposed authentication schemes on sensor nodes and comparison with other existing digital signature based authentication schemes for WSN. We assume the capabilities of standard MICA2 mote [9], a popular choice among research community. Figures in Table 1 and Table 2 are computed considering only the expensive operations of pairing, point multiplication, exponentiation and ECDSA & RSA signature costs, based on the actual experimental results of these operations for MICA2 given in [14], [22] and [28]. A point multiplication operation on MICA2 takes 0.81s [14]. For MICA2, active power consumption is 30mW [22]. Therefore, computation of one point multiplication operation consumes 0.81*30 = 24.3mWs. According to [28], computing a pairing operation on MICA2 takes 2.66s and consumes 62.73mWs. Signing and verifying an ECDSA takes 0.89s and 1.77s and consumes 26.96mWs and 53.42mWs, respectively [22]. One RSA signature verification with 1024 bit key size takes 0.47s and consumes 14.05mWs [22].

For **broadcast authentication schemes**, we only consider computation cost and message size. Transmission cost is proportional to the message size. Assuming number of sensor nodes N = 65,000, message m = 20 bytes, timestamp TS = 2 bytes and ID = 2 bytes, Table 1 gives a comparison with existing signature based schemes. Existing authentication schemes assume broadcast senders as powerful devices, however for comparison purposes, we estimate the cost of applying these schemes to ordinary sensor nodes. **CAS** and **DAS** in [24] propose ECDSA to sign a message. **CAS** requires signer's public key and certificate to be sent with every message, increasing message size. The receiver verifies two ECDSA signatures for every message; one to verify certificate and other to verify message. **DAS** requires

Table I
COMPARISON OF PROPOSED BROADCAST AUTHENTICATION SCHEME WITH EXISTING BROADCAST AUTHENTICATION SCHEMES.

Schemes	Signature Scheme	Energy Cost (Offline) mWs	Energy Cost (Online) mWs	Computation Time (Online) s	Storage Overhead (KB)	Message Size (bytes)
Existing Broadcast Authentication Schemes						
CAS [24]	ECDSA	0	26.96	0.89	0	148
DAS [24]	ECDSA	0	26.96	0.89	(0.022N =) 1441	84
IDS [23]	Pairing based	0	87.09	3.47	0	108 [24]
IMBAS [6]	BNN [2]	0	72.90	2.43	0	107
Proposed Broadcast Authentication Scheme						
Proposed	IBOOS [25]	τ*	5.62	0.19	0	64 + ρ*
Proposed	IBOOS [31]	48.60	ε*	ε*	0	84

τ* and ρ* show the computational cost and the signature size of underlying signature scheme respectively and ε* shows negligible cost

all sensor nodes to store public keys of all senders. For N = 65,000, public key size = 22 bytes, every sensor node is required to store 1441KB which is beyond the storage capabilities of sensor nodes. Signature generation in **IDS** [23] comprises one pairing and one point multiplication while in **IMBAS** [6] three point multiplications as expensive operations.

The proposed broadcast authentication scheme using first IBOOS [25] allows the secure reuse of offline signature, computed on base station. The only cost a sensor node bears in message signing is the cost of the online phase which is two scalar exponentiations in group G. Computing one scalar exponentiation (of the form B^t) in G requires roughly t squaring and $t/2$ multiplications in G (Chap 14, Algorithm 14.79, [20]), where t is the bit length of exponent. For simplicity, we assume computing one squaring is equivalent to one multiplication (squaring can be almost twice as fast as multiplying distinct elements [20]). For $t = 160$, one exponentiation requires 240 multiplications. One multiplication on MICA2 takes 0.39ms [14] and consumes 0.0117mW [22]. Therefore, one exponentiation takes 0.09s and consumes 2.81mW. These results further can be improved by applying fixed-base exponentiation and fixed-exponent exponentiation algorithms, and finding the exact cost of squaring on MICA2 motes. For 160 bits ECC, the message size is 64 bytes plus ρ (ρ is size of underlying signature). Using second IBOOS [31] requires two point multiplications in offline phase, while only integer addition and multiplication operations (which are very efficient for sensor nodes in terms of time and energy consumption) in the online phase. Therefore, the time and energy cost of the online phase is almost negligible. For 160-bit ECC, the signature size is 60 bytes. Table 1 shows that the proposed sensor broadcast scheme using IBOOS schemes consume less energy and time in broadcasting a message as compared to applying existing authentication schemes to the sensor nodes.

In **user authentication** schemes, two existing schemes provide distributed user authentication, **RRUASN** [3] and **DP^{2}AC** [32]. In **RRUASN**, authentication by sensor nodes involves verification of two ECDSA signatures as expensive operations. **DP^{2}AC** involves one RSA signature verification and verification of token reusability. An issue with this scheme is the communication overhead per user request and storage overhead. Every used token is stored on more than one sensor nodes in the network. Assuming a token size = 10 bytes and number of used token T =10,000, the overall storage overhead will be 100,000 bytes which is considerable for resource constrained sensor nodes. Verification cost involves energy and time costs to verify RSA signature plus transmission energy (TE) and transmission time (TT) costs of sending a token to a set of sensor nodes for reusability checking. The proposed outside user authentication scheme based on IBS [6] involves one signature verification consisting of three point multiplications by the sensor nodes during the authentication phase. Table 2 shows that the proposed user authentication scheme consumes less energy and time as compared to RRUASN and eliminates the storage and communication overhead of DP^2AC. It also provides session key establishment.

Table II
COMPARISON OF PROPOSED USER AUTHENTICATION SCHEME WITH EXISTING USER AUTHENTICATION SCHEMES.

Schemes	Signature Scheme	Energy Cost (mWs)	Verification Time (s)	Storage Overhead	Session Key
Existing Distributed User Authentication Schemes					
RRUASN [3]	ECDSA	106.84	3.54	0	No
DP^{2}AC [32]	RSA	14.05 + TE	0.47 + TT	10T bytes	No
Proposed Distributed User Authentication Scheme					
Proposed	IBS [6]	72.90	2.43s	0	Yes

D. Impact of Applying PKC on Sensor Nodes

Application of PKC operations on sensor nodes does not affect node's life time drastically, if the number of public key operations is smaller or spread over time [22]. Broadcast of a message by a sensor node is not a very frequent event in considered applications. For example, in case of a fire alarm application, a message is sent by the sensor node only when a fire is set up anywhere. Signing a message occasionally, only in critical situations, is not very expensive for sensor nodes. With 2AA batteries in ordinary MICA sensor motes, the available energy is 6750,000mWs [22]. If only 2% of this energy i.e., 135,000mWs, is available for signing broadcast

messages, a sensor mote can sign 24,021 messages applying first IBOOS scheme and 2,778 messages applying second IBOOS scheme during the life time of the batteries. This number of broadcast messages is big enough for the above mentioned applications. With the same available energy, a sensor node can sign 1,550 messages in **IDS** scheme and 1,852 messages in **IMBAS** scheme which shows that our proposed sensor broadcast authentication scheme gives better results than applying existing broadcast authentication schemes to the sensor nodes.

VI. Conclusions and Future Work

The main contribution of this research work is an authentication framework which provides two features; quick authenticated broadcast by sensor nodes and user authentication. Existing broadcast authentication schemes in WSNs do not handle the problem of authenticated broadcast by sensor nodes. The proposed ID-based Online/Offline Signature (IBOOS) based broadcast authentication scheme is an attractive solution to this problem. An ID-based Signature (IBS) based distributed user authentication scheme is proposed to authenticate outside users. Session keys secure the further communication between the users and the sensor nodes. The main advantage of this framework is its re-usability, that is, it can also be reused with new IBS and IBOOS schemes for security and performance improvements. In the future, we intend to focus on user access control to provide a complete ID-based authentication framework which would enable the sensor nodes, on one hand, to broadcast a message to quickly respond to some critical situations and, on the other hand, to control user access according to his access privileges. We are on the way to implement the proposed framework on real sensor nodes to get actual results.

Acknowledgment

This work has been partially supported by the EPSRC project Verifying Interoperability Requirements in Pervasive Systems (EP/F033540/1).

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *Computer Networks*, vol. 38, pp. 393–422, 2002.

[2] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," in *Proc. EUROCRYPT '04*. Springer-Verlag, 2004, pp. 268–286.

[3] Z. Benenson, "Realizing robust user authentication in sensor networks," in *Proc. REALWSN '05*, 2005.

[4] Z. Benenson, F. Gartner, and D. Kesdogan, "User authentication in sensor networks (Extended Abstract)," in *Proc. Informatik 2004, Workshop on Sensor Networks*, 2004.

[5] J. Bohli, A. Hessler, O. Ugus, and D. Westhoff, "A secure and resilient WSN roadside architecture for intelligent transport systems," in *Proc. WiSec '08*. NY, USA: ACM, 2008, pp. 161–171.

[6] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: Identity-based multi-user broadcast authentication in wireless sensor networks," *Computer Communications*, vol. 31, no. 4, pp. 659 – 667, 2008.

[7] W. Chen and Y. Chen, "A bootstrapping scheme for inter-sensor authentication within sensor networks," *Communications Letters, IEEE*, vol. 9, no. 10, pp. 945–947, Oct. 2005.

[8] C. Chong and S. Kumar, "Sensor networks: evolution, opportunities, and challenges," *Proceedings of the IEEE*, vol. 91, no. 8, pp. 1247–1256, Aug. 2003.

[9] Crossbow, "MICA2." [Online]. Available: www.xbow.com

[10] M. Das, "Two-factor user authentication in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 8, no. 3, pp. 1086–1090, March 2009.

[11] J. Drissi and Q. Gu, "Localized broadcast authentication in large sensor networks," in *Proc. ICNS '06*. IEEE, p. 25.

[12] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line digital signatures," in *Proc. Advances in Cryptology CRYPTO '89*, ser. LNCS, vol. 435. Springer Berlin, 1990, pp. 263–275.

[13] M. C. Gorantla, C. Boyd, and J. M. González Nieto, "ID-based one-pass authenticated key establishment," in *Proc. sixth Australasian conference on Information Security, AISC '08*, pp. 39–46.

[14] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," in *CHES '04*, 2004, pp. 119–132.

[15] J. W. Kim, Y. H. Kim, H. Lee, and D. H. Lee, "A practical inter-sensor broadcast authentication scheme," in *HCI (5)*, ser. LNCS, vol. 4554. Springer Berlin / Heidelberg, 2007, pp. 399–405.

[16] T. Lee, "Simple dynamic user authentication protocols for wireless sensor networks," in *Proc. SENSORCOMM '08*, pp. 657–660.

[17] D. Liu and P. Ning, "Multilevel μTESLA: Broadcast authentication for distributed sensor networks," *ACM Trans. Embed. Comput. Syst.*, vol. 3, no. 4, pp. 800–836, 2004.

[18] D. Liu, P. Ning, S. Zhu, and S. Jajodia, "Practical broadcast authentication in sensor networks," in *Proc. MobiQuitous '05: Networking and Services*. IEEE Computer Society, pp. 118–132.

[19] M. Luk, A. Perrig, and B. Whillock, "Seven cardinal properties of sensor network broadcast authentication," in *Proc. SASN '06*. ACM, pp. 147–156.

[20] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.

[21] 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.

[22] K. Piotrowski, P. Langendoerfer, and S. Peter, "How public key cryptography influences wireless sensor node lifetime," in *Proc. SASN '06*. NY, USA: ACM, 2006, pp. 169–176.

[23] K. Ren, W. Lou, K. Zeng, and P. Moran, "On broadcast authentication in wireless sensor networks," *Wireless Communications, IEEE Transactions on*, vol. 6, no. 11, pp. 4136–4144, Nov. 2007.

[24] K. Ren, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," in *IEEE SECON '07*, pp. 223–232.

[25] Q. Ren, Y. Mu, and W. Susilo, "Mitigating phishing with ID-based online/offline authentication," in *Proc. Australasian conference on Information Security, AISC '08*, pp. 59–64.

[26] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO '84 on Advances in cryptology*, ser. LNCS. NY, USA: Springer-Verlag, 1985, pp. 47–53.

[27] I. Stojmenovi, Ed., *Handbook of Sensor Networks - Algorithms and Architectures*. WileyBlackwell, November 2005. [Online]. Available: http://books.google.co.uk

[28] P. Szczechowiak, A. Kargl, M. Scott, and M. Collier, "On the application of pairing based cryptography to wireless sensor networks," in *Proc. WiSec '09*. NY, USA: ACM, 2009, pp. 1–12.

[29] H. Tseng, R. Jan, and W. Yang, "An improved dynamic user authentication scheme for wireless sensor networks," in *Proc. GLOBECOM '07*. IEEE, 2007, pp. 986–990.

[30] K. H. M. Wong, Y. Zheng, J. Cao, and S. Wang, "A dynamic user authentication scheme for wireless sensor networks," in *Proc. SUTC '06*. IEEE Computer Society, 2006, pp. 244–251.

[31] S. Xu, Y. Mu, and W. Susilo, "Efficient authentication scheme for routing in mobile ad hoc networks," in *Proc. EUC '05 Workshops*, ser. LNCS, vol. 3823. Springer, 2005, pp. 854–863.

[32] R. Zhang, Y. Zhang, and K. Ren, "*DP*^{2}*AC*: Distributed privacy-preserving access control in sensor networks," in *Proc. IEEE INFOCOM '09*. IEEE, 2009, pp. 1251–1259.

[33] W. Zhang, N. Subramanian, and G. Wang, "Lightweight and compromise-resilient message authentication in sensor networks," in *Proc. IEEE INFOCOM '08*. IEEE, 2008, pp. 1418–1426.

[34] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "Interleaved hop-by-hop authentication against false data injection attacks in sensor networks," *ACM Trans. Sensor Networks*, vol. 3, no. 3, p. 14, 2007.