Received: 19 September 2019 | Revised: 26 March 2020 | Accepted: 1 April 2020

DOI: 10.1002/eng2.12176

RESEARCH ARTICLE

WILEY

Multi-user broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography

Philemon Kasyoka[1,2] | **Michael Kimwele**[1] | **Shem Mbandu Angolo**[3]

[1]School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya

[2]School of Information and Communication Technology, South Eastern Kenya University, Kitui, Kenya

[3]School of Computing and Mathematics, Co-operative University of Kenya, Karen, Kenya

Correspondence
Philemon Kasyoka, School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya.
Email: pkasyoka@gmail.com

Abstract

Wireless sensor networks (WSNs) have found use in many areas ranging from military to healthcare among other areas of interest. Multiuser broadcast authentication is an important security feature in WSNs that can enable users to securely broadcast their data in a WSN. By its very nature, a WSN is resource constrained in nature making security implementation on such a network a major challenge of concern. In this paper, we present an efficient pairing-free broadcast authentication (BA) scheme with message recovery based on a lightweight digital signature protocol for use on WSNs. Our proposed BA scheme is able to accelerate message authentication broadcasted over a WSN while providing user anonymity. Comparing our proposed BA scheme with previous existing and related BA schemes, we have demonstrated that a reduction in computation, communication, and energy cost is possible making our scheme efficient for use on WSNs.

KEYWORDS

broadcast authentication, elliptic curve cryptography, identity-based signature scheme, wireless sensor networks

1 | INTRODUCTION

Wireless sensor networks (WSNs) are increasingly becoming popular due to tremendous advancements in radio communication technologies and micro-electrical-mechanical systems. A WSN is a type of wireless ad hoc network that deploys a large number of low-cost tiny sensor nodes distributed over an area of interest and runs autonomously.[1] The sensor nodes sense and monitor a physical phenomenon in an environment and report back information to a sink node that serves the role of a base station. A sensor in a network has the capacity to exchange information with other sensors in a network. The base station controls and coordinates the activities of the sensor networks, takes decisions, assigns tasks, and has the capability to query the network for data or any information. The sensors are referred to as nodes and they are resource constrained in terms of low computation, low power consumption and storage capacity. There resource constrained nature poses a challenge in the implementation of traditional security schemes in the WSNs.

Ever more attention is currently being focused on security issues in WSNs as they have found use on many critical human and environmental applications. WSN's security is also becoming a major challenge because of the openness nature of its network architecture. Without an effective security mechanism an adversary is able to capture information from its nodes and use it for malicious purpose. Cryptography has become one of the most preferred techniques used to secure data in a WSN environment.

Authentication is a key service in WSNs because wireless sensor nodes are increasingly being deployed in an unattended environment, leaving them open to possible hostile network attack.[2] Authentication schemes used in WSNs can be differentiated according to the purpose they accomplish, that is, authenticating unicast, multicast or broadcast messages. Secondly, authentication schemes can be categorized according to the cryptographic method they use, which can either be a symmetric method or an asymmetric in nature.[3]

A relatively slow signature verification process in broadcast authentication (BA) schemes will lead to high energy consumption reducing the life span of a sensor node in a WSN. BA is an important feature in WSNs. Hence, development of more lightweight and efficient BA scheme has become more crucial. There is urgent need to ensure basic security goals such as confidentiality and integrity among others are achieved in a more efficient manner on resource constraint environments. A security protocol utilizes security mechanisms comprising of one or more primitives such as a cipher for encryption and a message digest for message authentication and integrity.[4]

Authentication schemes based on symmetric cryptography do exist that are efficient in authentication.[5,6] The sender and its receivers share the same secret key and hence any one of the receivers can impersonate the sender and forge messages to other receivers. This problem is prevalent in all symmetric cryptographic schemes and to overcome the problem we need to use public key encryption.[7]

Traditional public key cryptosystems (PKCs) form the core of security protocols. However, they have been found to consume a lot of energy due to their complex algorithms that require significant computational power.[8] This makes traditional PKCs not suitable for use on WSNs as sensor nodes have limited battery power.[9] Different PKCs approaches have been proposed for the sole purpose of securing data. In public-key infrastructure (PKI) users' public keys are bound with respective users' identities by means of public-key certificates issued by a Certificate Authority (CA).[10] To preserve the authenticity of the public key of a corresponding user, the signature of the CA's on the certificate is used. The CA records the identity of a user together with the user's public key so they can be used later for verification of the user's public key. The CA also performs certificate management activities such as certificate issuance, certificate renewal, and certificate revocation.[11] Certificate management has been shown to lead to extra storage, large computation and communication costs.[12]

To overcome the limitations of PKI, the notion of identity-based (ID) cryptography was first proposed in 1984.[13] ID-based cryptography is an approach to public-key cryptography that does not require a user to precompute his public key or obtain a certificate for the public key as is the case with conventional PKCs. A user's private key can be computed by a trusted third party referred to as public key generator while the public key can be an arbitrary identifier such as a telephone number or an e-mail address that can uniquely identify a user. ID-based cryptography is supposed to provide a more convenient alternative that solves the problem of the conventional public key infrastructure. Some ID-based signature schemes have been proposed.[10,14,15]

The use of elliptic curves[16] in cryptography presents a great advantage in a few unique areas. For instance, compared to rivest, shamir, and adelman, the inventors of the technique (RSA) cryptosystems elliptic curve-based systems require less memory and small key size.[17] A key size of 1024 bits for both RSA and DSA gives the same level of security as 160 bits in an elliptic curve cryptosystem,[18] and this presents us with an opportunity to use elliptic curves for development of efficient cryptographic schemes for use on resource-constrained devices.

A good example of a digital signature that makes use of elliptic curves is the Elliptic Curve Digital Signature Algorithm (ECDSA) which is the elliptic curve analogue of the DSA and is also a standardized variant of the original El-Gamal signature scheme. ECDSA was proposed in 1992 by Scott Vanstone and serves the same purposes of key generation, signature generation, and verification.[19] The mathematical basis for the security of elliptic curve cryptosystems is the computational intractability of the elliptic curve discrete logarithm problem.[20] Given elliptic curve E defined over Z_p and a point $P \in E(Z_p)$ of order p, a point $Q \in E(Z_p)$ generated as $Q = dP$ with integer $d \in_R [1, n-1]$ it is difficult to determine the value of integer d. The procedure of computing ECDSA is discussed in Reference 21.

The use of ECDSA is not appropriate for achieving mutual authentication between the entities like the base station, cluster heads, and nodes.[22] Speeding up ECDSA signature generation and verification is a problem of considerable importance. To this end, we propose a new BA scheme for WSN with message recovery that makes use of an efficient signature scheme based on elliptic curve. Second, we proof the efficiency of our proposed BA scheme against previous related BA schemes.

1.1 | Related work

Authentication among sensors in a WSN is key to ensuring secure communication. In a study conducted by Reference 23, they proposed a mutual authentication scheme for WSN. However, their scheme was based on pairing cryptography which has been proven in recent studies to be complex for use on resource constrained devices.[24] An authentication scheme based on RSA and Diffie-Hellman algorithms was proposed by authors in Reference 25. The scheme was found to be vulnerable to stolen-verifier, replay, and forgery attacks.[26] In Reference 27, a RSA-like public key cryptography was employed in the design of a multiuser BA scheme for WSNs. However, Elliptic Curve Cryptosystems (ECC) have been proved to be more efficient than RSA.[28]

The first user authentication protocol based on elliptic curve cryptography for WSNs was proposed by Reference 29, the scheme was found not to have mutual authentication between the user and the sensor node.[30]

A hybrid BA scheme based on ECC was proposed by Reference 31. It makes use of bloom filter and Merkel hash tree. Merkel hash tree limits the total number of users making the scheme not to be scalable. To add a new user, one will have to remove one user in the setup. In Reference 32 Kheradmand proposed an enhanced energy efficient WSN by improving the ECDSA, the researcher cited the need to decrease the verification process by exploiting cooperation among sensor nodes.

A study by Reference 33 proposed an improved elliptic curve digital signature scheme for use on WSNs by optimizing the signature generation module of ECDSA. However, they were unable to reduce the number of point additions and point multiplication in the verification algorithm. To overcome the challenges in efficient remote monitoring[34] proposed a privacy preservation secure cross-layer protocol design for WBAN using ECDSA. However, ECDSA has been found not to be suitable for design of authentication protocol. Reference 22 proposed a mutual authentication protocol with the help of a computationally low signature scheme.

Some of the significant protocols such as SNEP and TESLA[35] have been used in WSN as they are able to provide authentication and some level of security. Since these security protocols use source routing, they are highly vulnerable to traffic analysis during transmission.[36] BA scheme with private key protocols such as μTESLA[35] suffers from delay in message authentication that can lead to DoS attack.[37]

Since Boneh and Franklin[38] defined the first secure model for ID-based encryption, several BA schemes have been proposed. In Reference 39 an ID-based BA scheme was proposed using pairing cryptography. To minimize communication and computational costs in a BA scheme, Shim et al[40] proposed the use of a pairing-optimal ID-based signature scheme with message recovery, where the original message of the signature was not required to be transmitted together with the signature as the message would be recovered during the verification process. Their scheme was based on pairing cryptography. The notion of pairing cryptography requires expensive bilinear pairing operations making it inefficient for use on WSN. The cost of performing the pairing is at least eight times slower than that for a scalar multiplication in elliptic curves.[24]

In a study by Reference 41, they proposed a pairing-free ID-based multiuser BA scheme with partial message recovery for a base station. They also proposed a password-based user symmetric key mechanism to prevent compromise attacks. Their scheme was found by Reference 42 to be vulnerable to attacks due to the use of signature scheme with partial message recovery. To minimize communication and computation cost[10] proposed a pairing-free ID-based signature scheme. They used the scheme as a building block for a design of ID-based multi-user BA scheme. Other ID-based BA schemes that provide message recovery have been proposed.[40,43,44]

In Reference 7 the authors proposed a scheme to allow sensor nodes to authenticate broadcast messages from a base station using a one-time signature scheme. They mitigate the general drawbacks of one-time signature schemes by using an extremely large key size and limited authentication to only a few messages. Reference 45 proposed a symmetric BA scheme for WSNs. Symmetric-based authentication schemes have been proved not to be secure[3] and for that reason we will focus our work on asymmetric method of authentication.

1.2 | Motivation and contributions

In the previous section, we have discussed BA schemes having the following weaknesses: (a)They require the public key infrastructure necessitating the need for use of certificates. (b) They make use of pairing operations. (c) Make use of private key protocols such as μTESLA that suffer from delay in message authentication. We are motivated to propose a solution for the design of a BA scheme for WSNs that supports the following contributions:

1. First, we propose an efficient signature protocol based on elliptic curve cryptography with an efficient signature verification process.
2. Secondly, we use the proposed signature protocol to design BA scheme with message recovery that does not required pairing operations and thus, it requires less effort for realization.
3. We propose a BA scheme with an approach that will ensure sensor nodes do not have to execute the entire signature verification process hence improving on the efficiency of the overall computation and energy cost.
4. Lastly, the computational cost of our scheme is much lower than other existing related schemes and can be implemented on resource constrained environments such as a WSN.

1.3 | Organization

The rest of this paper is organized as follows. Section 2 presents the preliminaries which include digital signature and elliptic curve cryptography. Section 3 presents related work while the proposed signature protocol is presented in Sections 4. The proposed BA system is presented in Section 5. Performance comparison of the proposed BA scheme against other related schemes is presented in Section 6. Finally, Section 7 concludes the paper.

2 | PRELIMINARIES

2.1 | Digital signature

Digital signature schemes have become an important building block of many cryptographic applications and they are used to achieve integrity, non-repudiation and authentication of data. They are described in terms of a signing process, verifying process and associated key. The key generation procedures can best be explained as a tuple of polynomial-time algorithm $\Sigma = (Gen, Sig, Ver)$ where a key generation algorithm Gen, on input 1^k,where k is a security parameter and it gives an output a signing key and a verification key $(s_{\text{key}}, v_{\text{key}})$. The signing algorithm Sig takes as input a message M and a signing key s_{key} and outputs a signatureσ. The verification algorithm Ver, on input (σ, M, Ver) outputs 1 to accept the signature for the message given or $\perp$ to reject the signature.

When a signer wants to communicate a message M with another party who is a receiver, both the sender and receiver must have followed the signature scheme's setup procedures to generate necessary private and public keys. Every time sender wants to communicate with receiver, sender must follow the signing procedure to sign M thenconveysthe signed messageand its signature to the receiver. When the receiver gets $M$and signature of M, receiver must apply the set verification procedure of the digital signature scheme to verify the authenticity of the message M. A digital signature can be check for authenticity using a public key.

2.2 | Elliptic curve cryptography

Elliptic curves appear in many diverse areas of mathematics, ranging from number theory to cryptography. In cryptography, elliptic curves have found use in ECC which is increasingly gaining popularity in public key cryptography since it was invented by Reference 46. ECC is based on algebraic concepts related with elliptic curves over Galois Fields. These fields can be binary fields $GF(2^n)$ or prime fields $GF(P)$. In Elliptic Curve over $F_p$where $F_p$is a prime finite field so that $p > 3$ is an odd prime number, let a, $b \in F_p$ that satisfy $4a^3 + 27b^2 \not\equiv 0 \ mod \ p$ then the elliptic curve over F_p consists of the set of points $P = (x, y)$ for $x, y \in F_p$ defined by an equation of the form $y^2 \equiv x^3 + ax + b \ (\text{mod } p)$ and an additional point of infinity denoted as $\mathcal{O}$.

Cryptographic schemes based on ECC rely on difficulty of solving elliptic curve discrete logarithm. Given integer x and a point $P \in F_p$, scalar multiplication is the process of adding P to itself x time to get point $Q = xP \in F_p$. Find value x is the discrete logarithm of point Q to base P denoted as $k = \log_P Q$. In elliptic curve points scalar multiplication can be computed efficiently using the addition rule together with the double-and-add algorithm or one of its variants as explained in Reference 20.

The additive elliptic curve group can be defined as $G = \{(x, y) : x, y \in F_p\}$ and $x, y \in E_q(a, b) \cup \{o\}$ where o is the infinity point.[47] The order of the elliptic curve over F_p is given as $E(F_p)$ that must satisfy $1 - 2\sqrt{q} \leq E(F_p) \leq q + 1$.

2.2.1 | Addition formula for curve

Given $P = (x_1, y_1) \in E_p$ and $Q = (x_2, y_2) \in E_p$ then $P + Q = (x_3, y_3)$, where $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ and

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \; if \, P \neq Q \\ \frac{3x_1^2 + a}{2y_1} if \, P = Q. \end{cases}$$

In Reference 48 the authors have provided a summary of addition formula for zero j-invariant over F_p and nonzero j-invariant over F_p. The main strength that an elliptic curve system has compared to a system based on the intractability of integer factorization is that there is no subexponential-time algorithm that can easily be used to discover discrete logs in these groups.

2.2.2 | Point multiplying

Point multiplication over $E(F_p)$ is computed as follows given a constant t as t-fold addition of P, that is, $= P + P + P + P + \cdots + P(t - \text{times})$.[49] To recover value t from a given pair (tP, P) is called elliptic curve discrete logarithm program and it is assumed to be intractable.[41]

3 | PROPOSED SIGNATURE PROTOCOL

We propose an ID-based signature protocol consists of four phases: Setup, key generation, signature generation, and signature verification. The researchers' goal is to improve computational efficiency in the verification process making the scheme adaptable for use on resource constrained environments such as WSNs.

3.1 | Setup

Given security parameter γ, an elliptic curve $E(F_p)$ is selected which is defined over finite field F_p where p represents number of points on the elliptic curve. G is a cyclic group of $E(F_p)$ generated by point $P \in G$, with prime order q. Pick a random $msk \in Z_q^*$ and compute $P_{\text{pub}} = msp \cdot P$. Select a cryptographic hash functions $H_1 \; : \; \{0,1\}^2 \rightarrow Z_q^*$ and $H_1 \; : \; \{0,1\}^2 \times G \rightarrow Z_q^*$ that are collision resistant. System parameters are set as param $< F_q$, E, p, G, Q, P_{pub}, H_1, $H_2 >$ and the master secret key is msk.

3.2 | Key generation

The key generation process will proceed as follows:

Select a random integer $d \in_R Z_q^*$, given a user identity ID compute $v = \text{msk} + H_1(ID_i, d)$, Compute $Q = vP$ and $z = v^{-1} \; mod \; q$. Where Q is a signer's public key and full private key is set as SK $= (d, z)$.

3.3 | Signature generation

Select integer $k \in_R Z_q^*$;Compute $F = k \cdot P$; If $F_x = 0$ then go to start else, compute $e = m \oplus d \, || \, F_x$ where F_x denotes the x-coordinate of point $F = (x, y)$; $c = H_2(e, ID, P_{\text{pub}})$; $s = z \cdot (c \cdot k)$ mod q then sends signature as $\sigma = < F, s, e, c >$.

The message m is not send together with the signature as the proposed signature scheme has a property of message recovery.

3.4 | Signature verification

Upon receiving $\sigma = <F, s, e, c>$, the verification process proceeds as follows:

Check if equation $c = H_2(e, ID, P_{\text{pub}})$ holds, if it does not hold drop the message else compute $w = s \cdot e^{-1} \text{mod } q; X = w \cdot Q$. If $X = F$ then accept the signature and recover the message by computing $m' = e \oplus d \,||\, F_x$ else reject the signature.

Correctness The correctness of our scheme is as follows:

$$X = w.Q,$$

$$= s \cdot c^{-1}Q,$$

$$= z(c \cdot k)c^{-1}Q,$$

$$= z \cdot k \cdot Q$$

$$= d^{-1} \cdot k \cdot Q$$

$$= d^{-1} \cdot k \cdot d\boldsymbol{P}$$

$$= k \cdot P = F$$

3.5 | Security considerations

- *Parameter manipulation*: If it is possible to generate $H(m) \equiv H(m')$ mod q for a given pair of messages m and m' then it can also be assumed that any signature for m' is also a valid signature for m'. This can be checked by $q = H(m) - H(m')$. This parameter manipulation will not hold in our proposed scheme our value for c is computed as $c \leftarrow H(e, ID, P_{\text{pub}})$ where each signer uses a unique ID and a unique e computed as $e = m \oplus d_i \,||\, F_x$, making collision search in the hash function difficult.
- *Message forgery*: An attacker cannot forge a message for our scheme. If an attacker alters the value of m to m' this change will alter the value of (e', c', s'). The attacker cannot find the value of ε' such that $(\varepsilon + z(c \cdot k)c^{-1}) \cdot Q = k \cdot P$ such that the two sides of the equation are equal as the two values z and k are secret. Given the fact value k and z are not know to an attacker and the generator point P is never shared publicly as part of elliptic curve parameters it is not possible to forge a message.
- *Domain parameter shifting attack*: In Reference 50 the researcher shows how an adversary can perform a domain parameter shifting attack on ECDSA where the adversary intercepts the domain parameters ams = (q, representation, a, b, n, P, seed). Give that Q is a public key, the adversary picks a random d' and constructs new set of *params'* in which P is replaced by $P' = (d^{'-1}$ mod $q)Q$. The params' is send to the verifier and the adversary forges signatures using signature algorithm where d is replaced by d'. To thwart this attack P must be protected by some means. This attack will not be possible in our scheme as the parameters shared with the verifier do not include point P.

4 | PROPOSED BA SCHEME

Our proposed scheme is made up of four parts: (a) Initialization, where sensor nodes are initialized by the base station; (b) Sensor addition, in which the base station generates a public/private key pair for the new node joining the sensor network; (c) BA protocol, in which a sensor signs a message and broadcasts it to the neighboring sensors and eventually the message relied to the base station as depicted in Figure 1. (d) Sensor revocation, which maintains a list of all the compromised sensors. Table 1 describes the notations used in our proposed scheme.

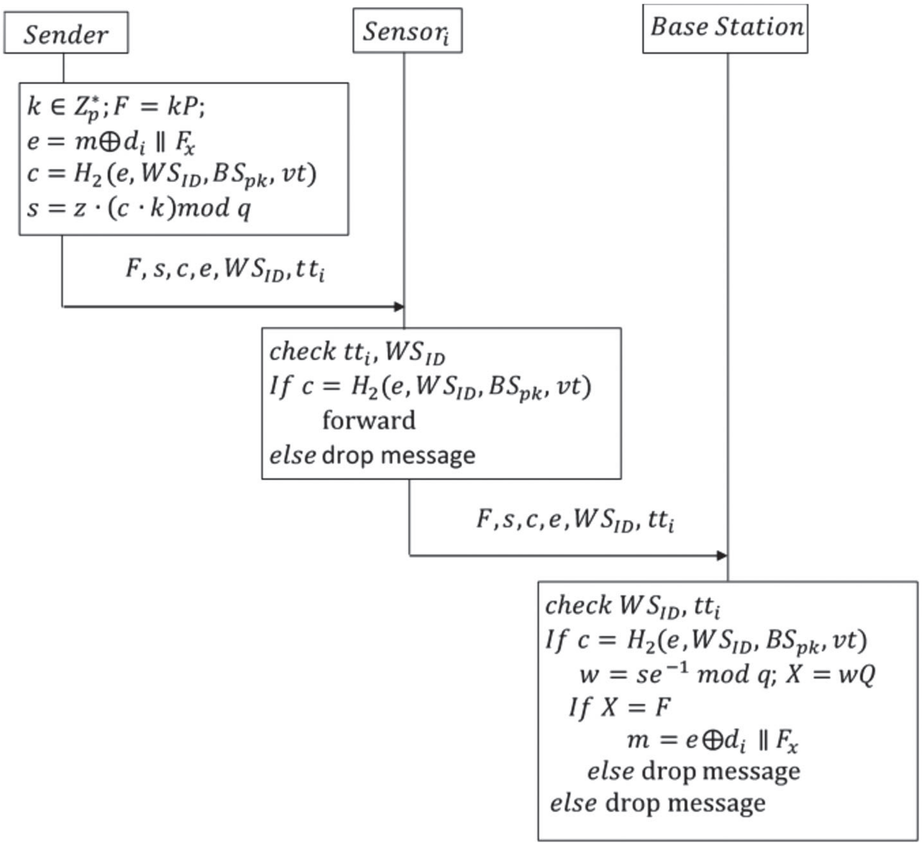
Sender
Sensor$_i$
Base Station
$k \in Z_p^*; F = kP;$
$e = m \oplus d_i \parallel F_x$
$c = H_2(e, WS_{ID}, BS_{pk}, vt)$
$s = z \cdot (c \cdot k) mod\ q$
$F, s, c, e, WS_{ID}, tt_i$
check tt_i, WS_{ID}
If $c = H_2(e, WS_{ID}, BS_{pk}, vt)$
forward
else drop message
$F, s, c, e, WS_{ID}, tt_i$
check WS_{ID}, tt_i
If $c = H_2(e, WS_{ID}, BS_{pk}, vt)$
$w = se^{-1}\ mod\ q;\ X = wQ$
If $X = F$
$m = e \oplus d_i \parallel F_x$
else drop message
else drop message

FIGURE 1 Broadcast authentication process

TABLE 1 List of notations

Notation	Description
WS, BS	Wireless sensor and base station/sink, respectively
$H(\cdot)$	One-way function
WS$_{\mathrm{ID}}$	Wireless sensor device identity Hash(ID)
Q_i	Wireless sensor public key
BS$_{pk}$, msk	Base station's public key and secret key, respectively
SK = (d_i, z_i)	Wireless sensor private key
vt	Verification token
m, c	message and ciphertext, respectively
$\oplus$	Exclusive XOR operation

4.1 | Initialization

The BS acting as a key generator center selects an elliptic curve E over finite field F_q and $P \in G$ of prime order q. BS defines a secure cryptographic hash functions $H_1 : \{0,1\}^* \times G \times G \to Z_q^*$, $H_2 : \{0,1\}^2 \to Z_q^*$, $H_3 : \{0,1\}^2 \times G \to Z_q^*$ and $H_4 : \{0,1\} \to Z_q^*$ then selects secret key msk$\in_R Z_q^*$ as its master secret key. The BS proceeds to compute its own master public key as $\mathrm{BS_{pk}} = \mathrm{msk} \cdot P$, and sets another secret value $z_b = \mathrm{msk}^{-1} \bmod q$.

4.2 | Key generation

In this phase, the base station will generate the private and public keys for each sensor node. Given identity $\mathrm{WS}_{\mathrm{ID}_i} = H_4(\mathrm{ID})$ for a sensor node, the BS begins by selecting a random value $d_i \in_R Z_q^*$ proceed to compute $v_i = \mathrm{msk} + H_1(\mathrm{WS}_{\mathrm{ID}_i}, d_i)$

then sets public key for a sensor as $Q_i = v_i P$. A random value $vt \in_R Z_q^*$ is selected and set as a common verification token for all sensor nodes in the network which can be changed regularly by the BS. The private key for a sensor node will be set as $\text{SK} = (d_i, z_i, vt)$ where $z_i = v^{-1} \bmod q$ and vt is a common verification token. To reduce on communication overhead, all the sensor nodes before deployment to the WSN are preconfigured with sensors' information such as S_{pk} z_i, d_i, a list of public keys and identities of sensor nodes already registered in the network and the elliptic curve parameters. To ensure each sensor node device is protected from physical device capture, a user is allowed to select a secret password PW then use his/her PW to computes $d' = H_4(\text{PW})^{-1}d, z' = H_4(\text{PW})^{-1}z$ and $vt' = H_4(\text{PW})^{-1}vt$. Following the approach proposed in Reference 41, if a user wants his/her private key, the user will first have to enter a valid password PW to recover (d, z, vt) from the stored (d', z', vt').

4.3 | Message BA

To send an authenticated message to sink in a WSN, a sensor with identity WS_{ID_i} will proceed as follows:

1. Choose a random value $k \in_R Z_q^*$ and compute $F = k \cdot P$;
2. If $F_x = 0$ goto step 1;
3. Compute $e = m_i \oplus d_i \parallel F_x$ where m_i is the message;
4. Compute $c = H_2(e, \text{WS}_{\text{ID}_i}, \text{BS}_{pk}, vt)$ and output $\sigma_i = \, <F, s, e, c>$ as the signature.

The sender will broadcast message $<\sigma_i$, WS_{ID}, $tt_i>$ to the next hop where s is generated using the signing algorithm of our proposed protocol and tt_i is the current timestamp of the sensor node signing the message. Our proposed scheme has the property of message recovery whereby message m_i signed does not need to be forwarded together with the signature. It can be recovery in the verification process of our proposed BA scheme. Message recovery approach will help minimize communication overhead by reducing on size of message transmitted.[10]

The signing of each message will occur only once when a sensor node is signing its own messages before transmitting to the BS. The neighboring sensor node will verify the transmitted message using the verification algorithm of our signing protocol and will forward to the next neighboring sensor. This implies that the verification process will occurs several times on the same message as the message is propagated along the WSN, until it reaches the BS. By reducing the cost of operations in the signature verification phase of our proposed signature protocol, the computational cost of each sensor node during the verification process will be reduced. As a result of the reduction of computational cost the, the overall energy consumption of the WSN is significantly reduced.

4.4 | Sensor message authentication

The authentication process for each sensor node before the message reaches the BS is conducted as follows: When the neighboring sensor node receives $<\sigma_i$, WS_{ID}, $tt_i>$ it checks if tt_i and WS_{ID} are valid else drops. It will check if equation $c = H_2(e, \text{WS}_{\text{ID}i}, \text{BS}_{pk}, vt)$ holds, if it does not hold it will drop the message else it will forward massage $<\sigma_i$, WS_{ID}, $tt_i>$ to the sensor node in the next hop. The same verification process will continue until the message reaches the BS. In resource constrained environments such as WSNs, speeding up the signature verification process is a problem of considerable practical importance.[51]The process of validating c is ciphertext authenticity. It helps reduce computational cost of intermediate sensor nodes by ensuring that they do not have to run the entire signature verification process as prescribed in our proposed signature protocol.

4.5 | Base station message authentication

When BS receives $<\sigma_i$, WS_{ID}, $tt_i>$ it checks for validity of the data as follows:

1. BS checks if tt_i is fresh as per set time delay threshold else it discards the data.
2. Checks if WS_{ID} is valid else drop data.

3. Run the signature verification algorithm on the message received. If the signature verification process is successful it recovers the message m_i as $m_i{}' = e \oplus d_i \,||\, F_x$.

4.6 | Revocation

All the communicating sensor nodes whose message fails verification process are reported to the BS by the verifying sensor where further investigations can be conducted. If the sensor node is found to have been compromised by an adversary it will be added to the revocation list. The BS will generate a signature on message $m = (\text{WS}_{\text{ID}_x}||\text{Rev})$, where *Rev* is a revocation message and WS_{ID_i} is the identity of the compromised sensor node. It will selecting a random value $k \in_R Z_q^*$ and compute $F = k \cdot P$ then encrypts message m as $e = m \oplus vt||F_x$, $c = H_3(e, vt, \text{BS}_{pk})$ and set the signature as $\sigma_i = <F$, s, e, $c>$. The base station will broadcast message $M_{\text{Rev}} = <\sigma_i$, $tt_i>$ to all sensor nodes in the network, where s is a signature generated using the signing algorithm of our signature protocol and tt_i is the current timestamp of the BS. When a sensor receives the message M_{Rev} it runs the process outlined in the proposed verification algorithm to validate the message. If the verification process is successful, the sensor node recovers $m' = (\text{WS}_{\text{ID}_x}||\text{Rev})$ and adds WS_{ID_x} to its local revocation list. If the sensor receives a message from a node whose identity is in revocation list it will immediately drop the message.

5 | SECURITY ANALYSIS

Our proposed authentication protocol is secure against, the authenticity threats, message integrity threats and replay attacks.

- *Our authentication scheme provides data confidentiality*. The messages sent from the WS_i to the the BS are encrypted into ciphertext c and signed any adversary trying to intercept the message will not be able to read its content. Our scheme provides message recovery and no plaintext message is transmitted to the BS. Only the BS can decrypt the message after proofing its authenticity.
- *Our scheme provides security against authenticity threats*. The messages sent from the sensor nodes to the BS are signed using the private key of the sensor nodes. Any change in the message will change value s, e and c. Since, the approach used for signing is $s = z \cdot (c \cdot k)$ the adversary will need to provide a value c' such that $c' = (s.\ z)/k$. The values z and k are private and k is a nonce that changes with every new message.
- *Message integrity*. If an active adversary makes changes to the massage m_i, the message will be rejected at the ciphertext authentication stage since $c = c\prime = H_2(e\prime, \text{WS}_{\text{ID}_i}, \text{BS}_{pk}, vt)$ will not hold.
- *Compromise attack*. To resist the compromise attack proactively, a user protects its private key pair with a secret password PW. If an adversary could capture a sensor node, it can only get encrypted user private keys (d', z', vt'). The adversary cannot recover (d, z, vt) since he/she has no access to user's password *PW*.
- *Secure against replay attack*. Assuming that our protocol has a time synchronization mechanism agreed between sensor nodes WS_i and BS to enable checking for data freshness. If an adversary was to intercept message and replay it at time $tt_{i'}$, assuming that the valid time delay is given as ΔT.The WS_i and BS will receive this message and check if $tt_{i'} - tt_i \geq \Delta T$ is within the allowed propagation delay time, if it is not the message is assumed to be a replay attack and dropped.
- *Denial-of-service attack*. A sensor node will only receive messages from preauthorized sensor node based on their S_{ID}. Any sensor node that fails the verification process, its broadcast message will immediately be dropped and reported to the BS. Each sensor is only allowed to authenticate a broadcast message from one node at a time. If a sensor node fails to validate the received broadcast message to a predetermined threshold in a row, it will report the occurrence to the Base station. The BS will take the initiative of limiting its access to the WSN as it investigates the incident.
- *User anonymity*. An adversary will not be able to know the identity of the user since the sensor sends $\text{WS}_{\text{ID}} = H_4(\text{ID})$, which is not the actual identity of the user/sensor. The message is encrypted as $e = m_i \oplus d_i \,||\, F_x$ reducing the chances

TABLE 2 Unit conversion of various operations based on modular multiplication

Notations	Description
T_M	Modular multiplication
T_{PA}	Elliptic curve point addition $T_{\text{PA}} = 0.12T_M$
T_{SM}	Scalar multiplication $T_{\text{SM}} = 29T_M$
T_{INV}	Modular inverse operation $T_{\text{INV}} = 11.6T_M$
T_H	One-way hash function, Negligible
T_{Add}	Modular add operation, Negligible

TABLE 3 Time complexity of schemes measure in unit of T_M

Schemes	Signature gen	Time complexity	Signature verification	Time complexity
Cao[41]	$T_{SM} + T_M + T_{Add} + T_H$	$30T_M + T_{\text{Add}} + T_H$	$3T_{\text{SM}} + 2T_{\text{PA}} + 2T_H$	$87.24T_M + 2T_H$
Bashirpour[52]	$2T_{SM} + 2T_M + T_{Add} + T_H$	$60T_M + T_{\text{Add}} + T_H$	$2T_{\text{SM}} + T_{\text{PA}} + 2T_H$	$58.12T_M + T_H$
Our scheme	$T_{\text{SM}} + 2T_M + T_H$	$31T_M + T_H$	$T_{\text{SM}} + T_M + T_H + T_{\text{Inv}}$	$30.73T_M + T_H$

TABLE 4 Broadcast authentication time complexity

Schemes	Time complexity
Cao[41]	$T_x = 30T_M + (1000 * 87.24T_M) = 87270T_M$
Bashirpour,[52]	$T_x = 60T_M + (1000 * 58.12T_M) = 58180T_M$
Our scheme	$T_x = 31T_M + (1000 * 30.73T_M) = 30761T_M$

of knowing any information that may lead to the identity of the person associated with the sensor hence preserving user's privacy.

- *Mutual authenticity*. All entities are mutually authenticated with each other. When a sensor B receives message $\{F, s, e, c, \text{WS}_{\text{ID}_i}, tt_i\}$ from sensor A it has to validate that the message actually generated by sensor A and vise versa. Hence mutual authentication is achieved.
- *Man-in-the-middle attack*. If an adversary intercepts a message transmitted between nodes the adversary will not be able to masquerade as BS or WS_i. From the above discussion we know that our protocol can provide mutual authentication and is secure against reply attack hence, man-in-the-middle attack can be thwarted.

6 | PERFORMANCE COMPARISON

6.1 | Computational analysis

We evaluate the computational analysis of our scheme against other related schemes by References 41, 52. For convenience we evaluate the computational cost based on time complexity of ECC operations with regard to modular multiplication as summarized by Reference 52 in Table 2.

If T_s denotes the number of executions for signing and T_v denotes the number of signature verification in a WSN and T_x denotes the time complexity of BA. Now given a WSN has 1000 sensor nodes then $T_v = 1000$ and $T_s = 1$. The time complexity T_x is computed as shown in Table 4 where our scheme is more efficient compared to the other two schemes by References 41, 52. As observed in Table 3, the scheme by Reference 41 is more efficient in the signature generation than our proposed scheme and scheme proposed in Reference 52. However, our scheme is more efficient in the signature verification than the schemes by References 41, 52 as shown in Table 3. We place more emphasis on computation cost in the verification process during the BA process since the nodes are resource constrained. The overall complexity as shown in Table 4 computed using unit conversions in Table 2. Our authentication scheme is more efficient in computation than all the other two schemes shown in the Table 3.

6.2 | Communication efficiency analysis

In our communication analysis, we compare our scheme with the schemes by References 41, 52 which are pairing-free scheme based on ECC and we adopt the approach used in Reference 10. We consider a MICAz mote[53] which has a clock speed of 8 MHz with a 8-bit processor ATmega128L and a data rate is 12.4 kbps. The operating system used is TinyOS and the power level of the MICAz sensor is 3.0 V where the current draw in active mode is 8.0 mA, receiving current draw is 10 mA and the transmitting current draw is 27 mA.[41,54]

To achieve 80 bits security level on ECC we consider G as additive cyclic group generated by point $P = (x, y)$ on a nonsingular elliptic curve $E : y^2 = x^3 + ax + b \bmod p$ with order q. The size of elements in Z_q^* is 160 bits and a, b, p are prime numbers of 160 *bits*. Therefore, the elements in G is $160x2 = 320$ bits.The timestamp $|tt|$ and identity |ID| are set each at 32 bits. Additionally, the length of message is $|M| = 160$ bits.

The message transmitted by the scheme by Reference 41 is $<M$, tt, ID, $sig\{M, tt, \mathrm{ID}\}>$, where $sig\{M, tt, \mathrm{ID}\}$ is user generated signature on M, tt, ID giving an output of $\sigma = <R_i, y_i, z_i>$. The total length of transmitted message is $|M| + |tt| + |\mathrm{ID}| + |R| + |y| + |z| = 160 + 32 + 32 + 320 + 160 + 160 = 864$ bits. While the BA scheme proposed by Reference 52 will send message $<M$, tt, $sig\{M, tt, \mathrm{ID}\}$, $Q>$, where $sig\{M, tt, \mathrm{ID}\}$ is generated in the signature generation phase on M, tt, ID giving an output of $\sigma = <s, F, X>$. The total length of transmitted message is $|M| + |tt| + |s| + |F| + |X| = 160 + 32 + 160 + 320 + 320 + 320 = 1312$ bits. The message broadcasted by our proposed scheme is $<sig\{F, s, e, c\}ID, tt>$ where the complete message transmitted is $|F| + |s| + |e| + |c| + |ID| + |tt| = 320 + 160 + 160 + 160 + 32 + 32 = 864$ bits. It is clear that our scheme is 66% more efficient in terms of communication compared to the scheme by Reference 52 while compared to the scheme by Reference 41 our scheme has the same communication cost.

6.3 | Energy consumption analysis

In the evaluation of the energy consumption of our scheme against other related schemes by References 41, 52 we will only consider scalar multiplication of the elliptic curve cryptography. We will ignore other ECC operations as they are negligible.[10] The impact of communication cost on energy consumption for received and transmitted a message of n bytes are $W_r = V \times I_r \times n \times 8/r$ and $W_t = V \times I_t \times n \times 8/r$, respectively. The voltage is denoted as V while I_r denotes the current draw for receiving, I_t is the current draw for transmitting and r denotes the data rate. When a simple flooding method is used, a sensor node wishing to broadcast a message in the WSN will only transmit once and will receive message N times, where N represents neighboring sensor nodes. Following the approach adopted by Reference 10, we use assume a message will be 80 bits. The energy consumption for sensor transmitting a message M using scheme by[41,52] is $W_t = 3.0 \times 27 \times 864/12\,400 = 5.64$ mJ and $W_t = 3.0 \times 27 \times 1312/12\,400 = 8.57$ mJ respectively, while our proposed scheme will consume $W_t = 3.0 \times 27 \times 864/12\,400 = 5.64$ mJ. The energy consumption for receiving a message M using scheme by References 41, 52 is $W_r = 3.0 \times 10 \times 864/12\,400 = 2.09$ mJ and $W_r = 3.0 \times 10 \times 1312/12\,400 = 3.17$ mJ, respectively, while our proposed scheme will consume $W_r = 3.0 \times 10 \times 864/12\,400 = 2.09$ mJ. When broadcasting a message to the entire WSN, a sensor node will transmit once and can receive N number of times. This will lead to a communication energy cost of $(5.64 + 2.09N)$mJ for the scheme by Reference 41 while the overall consumption for the scheme by[52] is $(8.57 + 3.17N)$mJ and our proposed scheme will have an overall energy consumption of $(5.64 + 2.09N)$mJ similar to that of Reference 41. The energy consumption for running a scalar multiplication operation over a sect163k1 Koblitz curve on a MICAz mote is 7.9 mJ.[10] The computation energy cost of our scheme against the schemes by References 41, 52 is shown in Table 5. The scheme by Reference 41 and our proposed scheme are more 50% efficient compared to the scheme by Reference 52. Our proposed scheme requires sensor to perform ciphertext authentication without the need to run the entire verification process and this makes our scheme more efficient than the schemes by References 41, 52. The sensor verification process of the scheme by Reference 52 is 66% more efficient in computation energy compared to the scheme by Reference 41. The verification process of our scheme is 53% more efficient in computational energy cost at the Base Station compare to the scheme by Bashirpour[52] and 33% more efficient compared to the scheme by Reference 41.

7 | CONCLUSION

In this paper the researchers have proposed an efficient BA scheme that makes use of a lightweight signature protocol based on ECDLP that can be applied on sensor networks. Our proposed scheme has message recovery and ciphertext

TABLE 5 Computational energy cost

Schemes	User	Sensor	Base station (Sink)
Cao[41]	$T_{SM} + T_H$ $1 \times 7.9 = 7.9$ mJ	$3T_{SM} + 2T_H$ $3 \times 7.9 = 23.7$ mJ	$3T_{SM} + 2T_H$ $3 \times 7.9 = 23.7$ mJ
Bashirpour[52]	$2T_{SM} + T_H$ $2 \times 7.9 = 15.8$ mJ	$2T_{SM} + 2T_H$ $2 \times 7.9 = 15.8$ mJ	$2T_{SM} + 2T_H$ $2 \times 7.9 = 15.8$ mJ
Our scheme	$T_{SM} + T_H$ $1 \times 7.9 = 7.9$ mJ	T_H -	$T_{SM} + T_H$ $1 \times 7.9 = 7.9$ mJ

authenticity that negates the need for sensor nodes to run the entire signature verification process. We have evaluated our proposed authentication scheme against other related BA schemes and we have shown that our proposed BA scheme more efficient in computational overhead than the rest of other related schemes. Our proposed BA scheme is more suitable for use on WSNs than the other related schemes in the literature. The future work will focus on advancing the scheme to certificateless public key cryptography.

CONFLICT OF INTERESTS

The authors declare that they have no conflict of interest.

PEER REVIEW INFORMATION

Engineering Reports thanks the anonymous reviewers for their contribution to the peer review of this work.

AUTHOR CONTRIBUTIONS

Philemon Kasyoka: Conceptualization; data curation; formal analysis; investigation; methodology; validation; writing-original draft; writing-review and editing. **Michael Kimwele:** Formal analysis; project administration; supervision; writing-original draft. **Shem Mbandu:** Formal analysis; project administration; supervision.

ORCID

Philemon Kasyoka https://orcid.org/0000-0002-8232-0299

REFERENCES

1. C. Wang, C. Jiang, Y. Liu, Y. X. Li and S. Tang, "*Aggregation Capacity of Wireless Sensor Networks: Extended Network Case*," IEEE Transactions on Computers; 2014.
2. Farahmandian M, Masdari M, Farahmandian V. Comprehensive analysis of broadcast authentication protocols in wireless sensor networks. *J Comput Sci Inf Tech*. 2014;2(3):107-125.
3. Grover K, Lim A. A survey of broadcast authentication schemes for wireless networks. *Ad Hoc Netw*. 2015;24:288-316.
4. Prasithsangaree P, Krishnamurthy P. On a framework for energy-efficient security protocols in wireless networks. *Comput Commun*. 2004;27(17):1716-1729.
5. Mansoor K, Ghani A, Chaudhry SA, Shamshirband S, Ghayyur SA, Mosavi A. Securing IoT-based RFID systems: a robust authentication protocol using symmetric cryptography. *Sensors*. 2019;19(21):4752.
6. Ghani A, Mansoor K, Mehmood S, Chaudhry SA, Rahman AU, Najmus SM. Security and key management in IoT-based wireless sensor networks: an authentication protocol using symmetric key. *Int J Commun Syst*. 2019;32(16):e4139.
7. Chang SM, Shieh S, Lin WW, Hsieh CM. An efficient broadcast authentication scheme in wireless sensor networks. Paper presented at: Proceedings of the 2006 ACM Symposium on Information, computer and communications security; 2006.
8. Venkataraman K, Sadasivam T. FPGA implementation of modified elliptic curve digital signature algorithm. *Facta Univ Ser Electr Energ*. 2019;32(1):129-145.
9. Shamshirband S, Joloudari JH, GhasemiGol M, Saadatfar H, Mosavi AN. FCS-MBFLEACH: designing and energy-aware fault detection system for mobile wireless sensor networks. *Mathematics*. 2020;8(1):28.
10. Shim K-A. BASIS: a practical multi-user broadcast authentication scheme in wireless sensor networks. *Inf Forens Sec*. 2017;6(1):1545-1554.
11. Subhas CS, Manik LD, Bubu B. A provable secure key-escrow-free identity-based signature scheme without using secure channel at the phase of private key issuance. *Indian Acad Sci*. 2019;44(12):1-9.
12. Gayathri NB, Vasudeva R. Efficient and secure pairing-free certificateless directed signature scheme. *J King Saud Univ Comput Inf Sci*. 2018.
13. Shamir A. Identity-based cryptosystems and signature schemes. *Workshop on the Theory and Application of Cryptographic Techniques*; Berlin, Heidelberg: Springer; 1984.
14. Chung FY, Huang KH, Lai F, Chen TS. ID-based digital signature scheme on elliptic curve cryptosystem. *Comput Stand Interfaces*. 2007;29:601-604.
15. J. Salome, G. N.B and R. Vasudeva, "Pairing-free identity based blind signature scheme with message recovery," *Cryptography-MDPI*, vol. 2, no. 29, 2018;29.
16. Miller V. Uses of elliptic curves in cryptography-lecture notes in computer science. *Adv Cryptol-Crypto '85*. 1985;218:417-426.

17. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and publickey cryptosystems. *Commun ACM*. 1978;21(2):120-126.
18. Hankerson D, Menezes A, Vanstone S. *Guide to Elliptic Curve Cryptography*. *Springer Professional Computing Series*. New York, NY: Springer; 2005.
19. Vanstone S. Responses to NISTs Proposal. *Commun ACM*. 1992;35(7):50-52.
20. D. Johnson, A. Menezes and S. Vanstone, "*The Elliptic Curve Digital Signature Algorithm*," International Journal of Information Security; 2001;1(1):36-63.
21. Brown D. *The Exact Security of ECDSA*. In Advances in Elliptic Curve Cryptography; 2000.
22. Moon AH, Iqbal U, Bhat GM. Mutual entity authentication protocol based on ECDSA for WSN. Paper presented at: Proceedings of the 12th International Multi-Conference on Information Processing-2016 (IMCIP-2016); 2016.
23. Jebri S, Abid M, Bouallegue A. LTAMA-algorithm: light and trust anonymous mutual authentication algorithm for IoT. Paper presented at: Proceedings of the IEEE 87th Vehicular Technology Conference (VTC Spring); 2018.
24. Cao X, Kou W, Du X. A pairing-free identity-based authenticated key agreement protocol with minimal. *Inf Sci*. 2010;180:2895-2903.
25. Watro R, Kong D, Cuti SF, Gardiner C, Lynn C, Kruus P. TinyPK: securing sensor networks with public key technology. Paper presented at: Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '04); 2004; Washington, DC.
26. Tseng HR, Jan RH, Yang W. An improved dynamic user authentication scheme for wireless sensor networks. Paper presented at: Proceedings of the 50th Annual IEEE Global Telecommunications Conference (GLOBECOM '07); 2007; Washington, DC.
27. Chen-Yang C, Iuon-Chang L, Shu-Yan H. An RSA-like scheme for multiuser broadcast authentication in wireless sensor networks. *Int J Distrib Sens Netw*. 2015;11(9):743623.
28. Dindayal M, Dilip KY. RSA and ECC: a comparative analysis. *Int J Appl Eng Res*. 2017;12(19):053-9061.
29. Yeh HL, Chen TH, Liu PC, Kim TH, Wei HW. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *Sensors*. 2011;11(5):4767-4779.
30. Han W. Weakness of a secured authentication protocol for wireless sensor networks using elliptic curves cryptography. *IACR*. 2011;2011:293.
31. Ren K, Lou W, Zhang Y. Multi-user broadcast authentication in wireless sensor networks. *IEEE Trans Veh Technol*. 2009;58:4554-4564.
32. Kheradmand B. Enhancing energy efficiency in wireless sensor networks via improving elliptic curve digital signature algorithm. *World Appl Sci J*. 2013;21(11):1616-1620.
33. Zhong H, Zhao R, Cui J, Jiang X, Gao J. An improved ECDSA scheme for wireless sensor networks. *Int J Future Generat Commun Netw*. 2016;9(2):73-82.
34. Sharavan PT, Sridharan D, Kumar R. A privacy preservation secure cross layer protocol design for IoT based Wireless Body Area Networks Using ECDSA Framework. *J Med Syst*. 2018;42(10):196.
35. Perrig A, Szewczyk R, Tygar JD, Wen V, Culler DE. SPINS: security protocols for sensor networks. *Wirel Netw*. 2002;8(5):521-534.
36. Maidhili SR, Karthik GM. Energy efficient and secure multi-user broadcast authentication scheme in wireless sensor networks. Paper presented at: Proceedings of the International Conference on Computer Communication and Informatics (ICCCI-2018); 2018.
37. Benzaid C, Lounis K, Al-Nemrat A, Badache N, Alazad M. Fast authentication in wireless sensor networks. *Futur Gener Comput Syst*. 2016;55:362-375.
38. Boneh D, Franklin M. Identity-based encryption from the Weil pairing. *SIAM J Comput*. 2003;32:586-615.
39. Ren K, Lou W, Zeng K, Moran PJ. On broadcast authentication in wireless sensor networks. *IEEE Trans Wirel Commun*. 2007;6(11):4136-4144.
40. Shim K-A, Lee Y-R, Park C-M. EIBAS: an efficient identity-based broadcast authentication scheme in wireless sensor networks. *Ad-Hoc Netw*. 2013;11:182-189.
41. Cao X, Kou W, Dang L, Zhao B. IMBAS: identity-based multiuser broadcast authentication in wireless sensor networks. *Comput Commun*. 2008;31(4):659-667.
42. Chien HY, Lee CI, Wu C. Comments on IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks. *Security Commun Netw*. 2013;6:993-998.
43. Tso R, Gu C, Okamoto T, Okamoto E. Efficient ID-based digital signatures with message recovery. *CANs 07*; Berlin, Heidelberg: Springer; 2007.
44. F. Zhang, W. Susilo and Y. Mu, "Identity-based partial message recovery signatures (or how to shorten ID-based signatures)," in *Financial Cryptography 2005*, Berlin, Heidelberg: Springer; 2005.
45. Mbarek B, Meddeb A, Jaballah WB, Mosbah M. An efficient broadcast authentication scheme in wireless sensor networks. *Ant/SEIT*. 2017;553-559.
46. Kobiltz N. Elliptic curve cryptosystems. *Math Comput*. 1987;48:203-209.
47. Islam SH, Farash MS, Biswas GP, Khan MK, Obaidat MS. Provably secure and pairing-free certificateless digital multisignature scheme using elliptic curve cryptography. *Int J Comput Math*. 2013;90(11):2244-2258.
48. Koblitz N, Menezes A, Vanstone S. The state of elliptic curve cryptography. *Des Code Cryptogr*. 2000;19:173-193.
49. Koblitz N. *A Course in Number Theory and Cryptography*. Vol 114. New York, NY: Springer Science & Business Media; 1994.
50. Vaudenay S. Digital signature schemes with domain parameters. Paper presented at: Proceedings of the Australasian Conference on Information Security and Privacy; 2004; Berlin, Germany.
51. Benzaid C, Medjadba S, Badache N. Fast verification of an ID-based signature scheme for broadcast authentication in wireless sensor networks. Paper presented at: Proceedings of the 2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012); 2012.

52. Bashirpour H, Bashirpour S, Shamshirband S, Chronopoulos A. An improved digital signature protocol to multi-user broadcast authentication based on elliptic curve cryptography in wireless sensor networks (WSNs). *MDPI*. 2018;23(17):1-15.

53. N. A. Ali, M. Drieberg and P. Sebastian. Deployment of MICAz mote for wireless sensor network applications. Paper presented at: Proceedings of the 2011 IEEE International Conference on Computer Applications and Industrial Electronics (ICCAIE); 2011.

54. Wander A, Gura N, Eberle H, Gupta V, Shantz S. Energy analysis of public-key cryptography for wireless sensor networks. Paper presented at: 3rd IEEE international conference on pervasive computing and communications. (pp. 324-328). IEEE; 2005.

How to cite this article: Kasyoka P, Kimwele M, Angolo SM. Multi-user broadcast authentication scheme for wireless sensor network based on elliptic curve cryptography. *Engineering Reports*. 2020;e12176. https://doi.org/10.1002/eng2.12176