IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received March 21, 2020, accepted April 5, 2020, date of publication April 14, 2020, date of current version April 29, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2987978

Fast Multivariate-Polynomial-Based Membership Authentication and Key Establishment for Secure Group Communications in WSN

QI CHENG[1], CHINGFANG HSU[2], ZHE XIA[3], AND LEIN HARN[4]

[1]Product Engineering Department, Wuhan Digital Engineering Institute, Wuhan 430074, China
[2]Computer School, Central China Normal University, Wuhan 430079, China
[3]Department of Computer Science, Wuhan University of Technology, Wuhan 430071, China
[4]Department of Computer Science Electrical Engineering, University of Missouri-Kansas City, Kansas City, MO 64110, USA

Corresponding author: Chingfang Hsu (cherryjingfang@gmail.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61772224 and Grant 61872152, in part by the Fundamental Research Funds for the Central Universities under Grant CCNU19TS019, and in part by the Research Planning Project of National Language Committee under Grant YB135-40.

ABSTRACT The primary task of secure group communications in wireless sensor networks (WSNs) is to securely transmit various types of data, for example weather data, traffic data, etc. Collected data in WSNs is different from most data transmitted in digital communication applications. Most collected data in WSNs contains only few bits of information. Conventional protocols are not suitable for WSNs since WSNs need more fast and lightweight protocols for secure group communications. User authentication and key establishment are two fundamental security services in secure communications for WSNs. The user authentication allows communication entities to authenticate their communication partners and the key establishment allows a secret session key to be shared among all communication entities. The session key can be used to protect exchange information in the communication. Communication has been moved from traditional one-to-one communications to many-to-many communications, also called group communications. Traditional user authentication which authenticates one user at one time is no longer suitable for a group communication which involves multiple users. In this paper, we propose a protocol which provides both membership authentication and key establishment simultaneously for WSNs. However, all existing solutions can only provide either user authentication or key establishment separately. Furthermore, our proposed membership authentication has complexity $O(n)$, where n is the number of users in a group communication, which is different from all existing user authentication schemes which are one-to-one authentications with complexity $O(n^2)$.

INDEX TERMS Group communications, group keys, membership authentication, secret sharing, multivariate polynomials, wireless sensor networks.

I. INTRODUCTION

Wireless Sensor Networks (WSNs) have been developed to collect data remotely for various applications [27], [28]. For example, data has been collected for traffic analysis, for weather prediction, and medical analysis, etc. For security reason, collected data needs to be protected from eavesdropping. Data encryption requires that both the source node and the receiver node share a pairwise shared key. The source node encrypts collected data under the shared key and the receiver node decrypts the ciphertext under the shared key to recover the data.

In general, security researches in WSNs are focused on the development of key establishment and key management solutions. Random key pre-distribution schemes [29]–[31] have been developed to allow two sensors to establish a shared key. The random key distribution is a probabilistic scheme and does not guarantee connectivity in WSNs. Each sensor is preloaded with k keys randomly selected from a large pool of keys. Blom [32] proposed the first pairwise key establishment scheme based on threshold cryptography. This approach is a deterministic scheme which can guarantee

The associate editor coordinating the review of this manuscript and approving it for publication was Mohamad Afendee Mohamed.

connectivity in WSNs. Blundo *et al.* [33] have discussed the key establishment using polynomials. Khan *et al.* [34] proposed a pre-distribution scheme using a symmetric matrix and a generator matrix of maximum rank distance to establish pairwise keys for sensor nodes. Group key distribution based on Bivariate polynomials [24], [35]–[37] have also been developed to allow a group of sensors to establish a shared key deterministically. The design of WSNs have been classified into two types: *flat* and *hierarchical*. In flat WSNs, all sensors have the same capabilities to collect data and forward data to other sensors in the network. In hierarchical WSNs, devices are organized into a hierarchy based on their capabilities. The key management protocols in WSNs have also been proposed according to two different types: *flat* and *hierarchical*.

Collected data in WSNs is different from most data in digital communication applications. Most collected data, for example weather/traffic data, in WSNs contains only few bits of information. Conventional protocols are not suitable for WSNs since WSNs need more fast and lightweight protocols for secure group communications.

User authentication and key establishment are two fundamental security services in secure communications for WSNs. The user authentication enables communication entities to authenticate the identities of their communication partners. After users being successfully authenticated, a key establishment enables a secret session key to be shared among communication entities such that all exchange information can be protected using this shared secret key.

It is well known that symmetric key encryption a way that each pair of users shares a symmetric key, but this way cannot provide authentication. Hence, pubic key encryption appeared, which can provide authentication but with high computation cost due to very large modulus and modular exponentiation operations. (RSA modulus is at least 1024 bits). How to realize efficient membership authentication and key distribution is an important problem for secure group communications.

Traditional communications are one-to-one type of communications which involves only two communication entities. Most existing user authentication schemes [1]–[7] involve only two entities, one is the prover and the other one is the verifier. The verifier interacts with the prover to validate the identity of the prover. However, communication has been moved to many-to-many communications recently, also called *group communications*. Traditional user authentication which authenticates one user at one time is no longer suitable for a group communication which involves multiple users. Recently, a new type of authentication, called *group authentication* [8], is proposed which can be used to determine whether all users belong to the same group or not. The group authentication is very efficient since it can authenticate all members at one time. However, the group authentication can only be used as a pre-processing of user authentication since if there are non-members, group authentication cannot determine who are non-members. Additional one-to-one user authentications are needed to identify non-members.

The use of centralized group key establishment protocols is the most commonly used protocol due to its efficiency. For example, the IEEE 802.11i standard [9] uses an online server to select a group key and transport it to each group member. More specifically, the server in the IEEE 802.11i encrypts the group temporal key (GTK) using the key encryption key (KEK) obtained from the authentication server (AS) and then the server transmits the encrypted message to each mobile client (group member) separately. Using a (t, n) secret sharing scheme to distribute a group key to all members can be found in [10]–[13]. Harn and Lin [14] have proposed an authenticated group key transfer protocol based on the secret sharing. Their protocol uses an RSA modulus to resist inside attack. The most commonly used public-key agreement protocol is Diffie-Hellman (DH) key exchange protocol [15]. However, DH key exchange can only provide session key for two entities; not for a group more than two members. Most public-key based group key distribution protocols [16]–[23] took natural generalization of the DH key agreement. One major concern of this type of protocols is due to its computational cost. Since the group key is contributed by all group members, the number of public-keys computations by each group member is proportional to the number of members involved in a secret group communication.

In this paper, we propose a membership authentication and key establishment protocol based on polynomials for WSNs. There are two unique features of our proposed protocol, (a) our proposed membership authentication has complexity $O(n)$, where n is the number of users in a group communication, which is different from most existing user authentication schemes which are one-to-one type of authentications with complexity $O(n^2)$; and (b) our protocol provides both membership authentication and key establishment simultaneously; but all most solutions provides either user authentication or key establishment separately. Here, we summarize the contributions of our paper.

· Our protocol provides both membership authentication and key establishment simultaneously.

· Our membership authentication has complexity $O(n)$.

· Our protocol is polynomial-based protocol so the computation is very efficient.

The rest of this paper is organized as follows: In the next section, we review a pre-distribution scheme of group keys which was published recently. Our proposed protocol is built upon this scheme. In Section 3, we describe the model of our protocol and the security feature of our protocol. In Section 4, we propose our membership and key establishment protocol. We analyze the security and performance in Section 5. We conclude in Section 6.

II. REVIEW OF PRE-DISTRIBUTION SCHEME FOR ESTABLISHING GROUP KEYS [24]

Our proposed protocol is built upon a recent paper by Harn and Hsu [24] which is a pre-distribution scheme of group keys in sensor networks using a multivariate polynomial. In this section, we review their scheme.

There has a mutually trusted key generation center (KDC) and there are n sensors, $\{P_1, P_2, \ldots, P_{\mathrm{n}}\}$. Each sensor loads shares by the KDC initially. The KDC selects an RSA modulus N, where N is the product of two large safe primes, p and q, i.e., p=2p'+1 and q=2q'+1, where p' and q' are also primes. p and q are KDC's secrets, N is made publicly known. The KDC selects a random polynomial having degree k as $f(x) = a_k x^k + \ldots + a_1 x + a_0 \, mod \, N$, and uses it to generate an m-variate polynomial, $F(x_1, x_2, \ldots, x_m) = \prod_{i=1}^{m} f(x_i)$. KDC computes shares, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$, where $s_{i,j}(x) = f_{i,l}(i) f(x) \, mod \, N$, for $l = 1, 2, \ldots, m-1$, and $f_{i,1}(i) \cdot f_{i,2}(i) \cdot \ldots \cdot f_{i,m-1}(i) = f(i) \bmod N$, for each sensor. Shares are stored in sensor P_i secretly for $i = 1, 2, \ldots$, n.

If m sensors, $\{P_{i_1}, P_{i_2}, \ldots, P_{i_m}\}$ want to establish a secret group key among them, each sensor P_i, where $i \in \{1, 2, \ldots, m\}$, uses its shares, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$, to compute $K = s_{i,1}(i_1) \cdot s_{i,2}(i_2) \cdot \ldots \cdot s_{i,m-1}(i_{m-1}) \, mod \, N$, where $i_1, i_2, \ldots i_{r-1} \in \{1, 2, \ldots, m\} - \{i\}$ and $i_r \neq i_s, \forall r, s$. In fact, $K = f(i_1) \cdot f(i_2) \cdot \cdots \cdot f(i_m) \, mod \, N$. We illustrate the scheme in Figure 1.

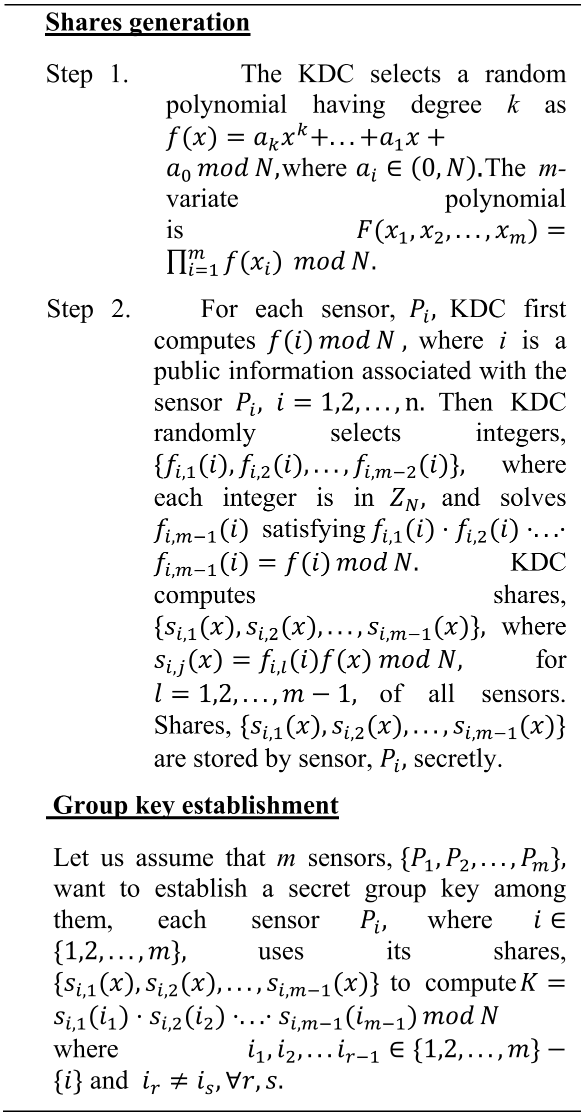
In [24], it has discussed that the proposed scheme satisfies following features.

(a) Correctness: The group key can be computed by each sensor in a group communication involving m (i.e., $2 \leq m \leq n$) sensors.

(b) k-secure: If k sensors are captured, there will have no information to be compromised.

(c) Key confidentiality: It is computationally infeasible for any attacker to discover any group key.

(d) Key independence: Knowing a subset of group keys, $K \subset K$, where k is the complete set of group keys, the attacker cannot discover any other group keys, $K'' = K - K'$.



Shares generation

Step 1. The KDC selects a random polynomial having degree k as $f(x) = a_k x^k + \ldots + a_1 x + a_0 \, mod \, N$, where $a_i \in (0, N)$. The m-variate polynomial is $F(x_1, x_2, \ldots, x_m) = \prod_{i=1}^{m} f(x_i) \; mod \, N$.

Step 2. For each sensor, P_i, KDC first computes $f(i) \, mod \, N$, where i is a public information associated with the sensor P_i, $i = 1, 2, \ldots$, n. Then KDC randomly selects integers, $\{f_{i,1}(i), f_{i,2}(i), \ldots, f_{i,m-2}(i)\}$, where each integer is in Z_N, and solves $f_{i,m-1}(i)$ satisfying $f_{i,1}(i) \cdot f_{i,2}(i) \cdot \ldots \cdot f_{i,m-1}(i) = f(i) \, mod \, N$. KDC computes shares, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$, where $s_{i,j}(x) = f_{i,l}(i) f(x) \, mod \, N$, for $l = 1, 2, \ldots, m-1$, of all sensors. Shares, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$ are stored by sensor, P_i, secretly.

Group key establishment

Let us assume that m sensors, $\{P_1, P_2, \ldots, P_m\}$, want to establish a secret group key among them, each sensor P_i, where $i \in \{1, 2, \ldots, m\}$, uses its shares, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$ to compute $K = s_{i,1}(i_1) \cdot s_{i,2}(i_2) \cdot \ldots \cdot s_{i,m-1}(i_{m-1}) \, mod \, N$ where $i_1, i_2, \ldots i_{r-1} \in \{1, 2, \ldots, m\} - \{i\}$ and $i_r \neq i_s, \forall r, s$.

FIGURE 1. Pre-distribution scheme for establishing group keys [24].

III. MODEL OF MEMBERSHIP AUTHENTICATION AND KEY ESTABLISHMENT PROTOCOL

In this section, we describe the model of our proposed membership authentication and key establishment protocol including the protocol description, the adversary and security properties of our proposed protocol.

A. PROTOCOL DESCRIPTION

Figure 2 illustrates a sensor network consisting multiple secure group communications. In our proposed protocol, there has a membership registration center (MRC) and there are n members, $\{U_1, U_2, \ldots, U_{\mathrm{n}}\}$. Each member needs to register at the MRC initially and obtain secret tokens. The MRC selects a special type of m-variate polynomial and generates tokens. Tokens of each member is $m - 1$ univariate polynomials.

In order to establish a secure group communication involving m (i.e., $2 \leq m \leq n$) members, it requires to execute a membership authentication first in which all participated users interact with each other to prove that they belong to the same group. In the membership authentication, each member needs to broadcast his identity and a random integer. After receiving all identities and random integers, each member needs to use his secret tokens to compute a key-hash output as his authentication response. Members can use this authentication response to authenticate his membership. Since each member is required to generate an authentication response and to be verified by other members, the complexity of this membership authentication is $O(m)$. This membership authentication can also identify non-members. At the end of membership authentication, each member knows exactly the memberships of users participated in the secure communication. Then, a secret session key is computed by each member individually. There is no interaction with other members to compute the session key. Thus, our proposed protocol is very efficient in both membership authentication and key establishment since there is only broadcast transmission. Furthermore, the computation of each member needs only polynomial evaluation and key-hash function which are much

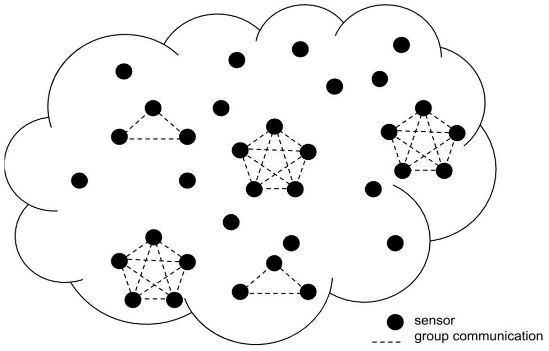


FIGURE 2. Sensor network.

faster than most public-key computations. We will give detail discussion for its performance evaluation in Section 5.

B. TYPE OF ADVERSARIES

We consider two types of attacks: inside and outside attacks. The inside attackers are legitimate members who have obtained valid tokens from MRC initially. From inside attack, colluded members try to recover MRC's secret polynomial used to generate tokens for members and then use these uncovered tokens to obtain group keys which they are not authorized to access. On the other hand, the outside attackers are illegitimate members who try to generate valid tokens of members and use them to impersonate members in a secure group communication or to recover secret group keys which they are not authorized to access. In the security analysis, we will show that none of these attacks can work properly against our protocol.

C. SECURITY FEATURES OF PROPOSED SCHE-ME

Since our protocol is based on the group key establishment scheme proposed in [24] with properties, k-secure, key confidentiality and key independence, as we have discussed in Section 2, it is obvious that our protocol shares the same properties in [24]. In addition, our protocol has the following features.

(a) ***Correctness:*** The protocol can successfully authenticate memberships of all participated users and then establish a secret group key among all members.

(b) ***Freshness of authentication response:*** The authentication responses generated by members in the membership authentication can only be used for one time. This feature can prevent replay attack in which attackers replay recorded authentication response to fail the membership authentication.

(c) ***Freshness of group keys:*** The secret group key generated by members in the key establishment can only be used for one time communication. This feature can prevent attackers to reuse previously compromised group keys to gain access to other secure communications.

Token generation

Step 1. The MRC selects a random polynomial having degree k as $f(x) = a_k x^k + \ldots + a_1 x + a_0 \, mod \, N$, where $a_i \in (0, N)$. The m-variate polynomial is $F(x_1, x_2, \ldots, x_m) = \prod_{i=1}^{m} f(x_i) \ mod \ N$.

Step 2. For each member, U_i, MRC first computes $f(i) \ mod \ N$, where i is a public information associated with the member, U_i. Then MRC randomly selects integers, $\{f_{i,1}(i), f_{i,2}(i), \ldots, f_{i,m-2}(i)\}$, where each integer is in Z_N, and solves $f_{i,m-1}(i)$ satisfying $f_{i,1}(i) \cdot f_{i,2}(i) \cdot \ldots \cdot f_{i,m-1}(i) = f(i) \, mod \, N$. MRC computes tokens, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$ where $s_{i,j}(x) = f_{i,l}(i) f(x) \, mod \, N$, for $l = 1,2,\ldots,m-1$, of all members. Tokens$\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$, are sent and stored by member, U_i, secretly.

Membership authentication

We assume that m members, $\{U_1, U_2, \ldots, U_m\}$, want to establish a secret group communication. The membership authentication allows each member to authenticate memberships of all other members.

Step 1. Each member, U_i, where $i \in \{1,2,\ldots,m\}$, needs to broadcast his identity, i, and a random integer, r_i, to all other members.

Step 2. After receiving all identities and random integers, $\{(i, r_i), i = 1,2,\ldots,m\}$, of members, each member, U_i, uses his secret tokens, $\{s_{i,1}(x), s_{i,2}(x), \ldots, s_{i,m-1}(x)\}$, to compute a group key, $K = s_{i,1}(i_1) \cdot s_{i,2}(i_2) \cdot \ldots \cdot s_{i,m-1}(i_{m-1}) \, mod \, N$, where $i_1, i_2, \ldots i_{m-1} \in \{1,2,\ldots,m\} - \{i\}$ and $i_r \neq i_s, \forall r, s$.

Step 3. Each member, U_i, computes an authentication response, $AS_i = h(K, (i, r_i, (1, r_1), (2, r_2), \ldots, (m, r_m))$, where $AS_i = h(K, (i, r_i, (1, r_1), (2, r_2), \ldots, (m, r_m))$, is a key-hash function with $i, r_i, (1, r_1), (2, r_2), \ldots, (m, r_m)$ as its input. The authentication response, AS_i, is broadcast to all other members.

FIGURE 3. Membership authentication and key establishment.

Step 4. After receiving each authentication response, AS_j, from member, U_j, each member, U_i, uses the group key, K, computed in Step 2 to verify the authentication response by checking $AS_j \underline{?}\, h(K, (j, r_j, (1, r_1), (2, r_2), \ldots, (m, r_m))$. If the checking is passed successfully, the member, U_j, has been successfully authenticated; otherwise, the member, U_j, has been failed in authentication.

Repeat Step 4 for $m-1$ times to authenticate the memberships of all other members in the communication.

Key establishment

Let us assume that at the end of membership authentication, all m members, $\{U_1, U_2, \ldots, U_m\}$, have been successfully authenticated. Then, each member can compute the key-hash output, $K_c = h(K, (1, r_1), (2, r_2), \ldots, (m, r_m))$, where K_c is

FIGURE 3. ***(Continued.)*** **Membership authentication and key establishment.**

(d) ***Forward secrecy of group keys:*** The forward secrecy is ensured if a departing member cannot access the content of communications of any future group session.

(e) ***Backward secrecy of group keys:*** The backward secrecy is ensured if a new member cannot access the content of communications of any past session.

IV. PROPOSED PROTOCOL

In this paper, we propose a membership authentication and key establishment protocol using a multivariate polynomial in Z_N, where N is an RSA modulus [25]. Our protocol is built upon the pre-distribution scheme of group key establishment [24]. The storage space of each member is $m(k+1)$ coefficients which is linearly proportional to the size of group communication.

The MRC selects an RSA modulus N, where N is the product of two large safe primes, p and q, i.e., p=2p'+1 and q=2q'+1, where p' and q' are also primes. p and q are MRC's secrets, N is made publicly known. The protocol is illustrated in Figure 3.

Remark 1: As stated in [24], if there are less than m members, for example r (i.e., $2 \le r \le m \le n$) members, $\{U_1, U_2, \ldots, U_r\}$, want to establish a secure group communication. Then, the same steps in Figure 2 are executed except each member, U_j, where $j \in \{1, 2, \ldots, r\}$, uses his tokens, $\{s_{j,1}(x), s_{j,2}(x), \ldots, s_{i,m-1}(x)\}$, to compute a shared group key $K = s_{j,1}(i_l) \cdot s_{j,2}(i_2) \cdot \ldots \cdot s_{j,r-1}(i_r) \cdot s_{j,r}(0) \cdot s_{j,r+1}(0) \cdot \ldots \cdot s_{j,m-1}(0) \bmod N$, where $i_1, i_2, \ldots i_{r-1} \in 1, 2, \ldots, r - \{j\}$ and $i_r \neq i_s, \forall r, s$, by all these members.

V. ANALYSIS

A. SECURITY ANALYSIS

In this sub-section, we discuss security features of our protocol as described in Section 3.3.

(a) ***Correctness:*** *Membership authentication*- If all participated users are members as they claimed in Step 1, each member, U_i, in step 2 should be able to compute the group key, $K = s_{i,1}(i_1) \cdot s_{i,2}(i_2) \cdot \ldots \cdot s_{i,m-1}(i_{m-1}) \bmod N = f(1) \cdot f(2) \cdot \ldots \cdot f(m) \bmod N$. Thus, in Step 3 the authentication response, $AS_i = h(K, (i, r_i, (1, r_1), (2, r_2), \ldots, (m, r_m))$, can be used to verify his membership by other members in Step 4. Non-members cannot forge this authentication response since non-members do not know the secret tokens of member, U_i.

Key establishment - The correctness of this property comes from the scheme [24].

(b) ***Freshness of authentication response:*** In Step 3 the authentication response, $AS_i = h(K, (i, r_i, (1, r_1), (2, r_2), \ldots, (m, r_m))$, is a key-hash output of all random integers selected by participated members initially. By recording a previously used authentication response cannot impersonate a member since the verifier's random integer is different in every session.

(c) ***Freshness of group keys:*** In the key establishment, the group key, $K_c = h(K, (1, r_1), (2, r_2), \ldots, (m, r_m))$, is a key-hash output of random integers selected by participated members initially. This group key is different in every session.

(d) ***Forward secrecy of group keys:*** If a member has departed from the group, the departed member cannot access the content of future communications since the any group key, K, can only be computed by members involved in the secure communication.

(e) ***Backward secrecy of group keys:*** If a member joins the group, the new member cannot access the content of any past communications since the any group key, K, can only be computed by members involved in the secure communication.

B. PERFORMANCE EVALUATION

All existing schemes can either provides user authentication or group key establishment separately. But our protocol can provide both membership authentication and key establishment simultaneously. Furthermore, our membership authentication has complexity $O(n)$, where n is the number of members in a group communication, which is different from most existing user authentication schemes which are one-to-one authentication with complexity $O(n^2)$.

Each member needs to store tokens, $\{s_{j,1}(x), s_{j,2}(x), \ldots, s_{j,m-1}(x)\}$, which are $m-1$ univariate polynomials. Thus, the memory storage of each member is $(m-1)(k+1)$ coefficients from Z_N.

In Step 2 membership authentication, to compute the group key, $K = s_{i,1}(i_1) \cdot s_{i,2}(i_2) \cdot \ldots \cdot s_{i,m-1}(i_{m-1}) \bmod N$, needs to evaluate $m-1$ polynomials. Horner's rule [26] can be used to evaluate polynomials. From Horner's rule, evaluating a polynomial of degree k needs k multiplications and $k+1$ additions. The computational cost to establish a group key with size m consists of the cost of evaluating $m-1$ polynomials. Overall, the computational cost to compute the group key, K, each member needs to evaluate $(m-1)k$ multiplications and $(m-1)(k+1)$ additions. In addition, each member needs to generate one authentication response and to verify $(m-1)$ authentication responses. Since each authentication response is a key-hash output, each member needs to compute m key-hash outputs. Finally, there is one more key-hash output to compute the group session key by each member. This computation of our proposed protocol is much simpler than most public-key based schemes. For example, the RSA public-key operation requires approximately $1.5log_2N$ modulo multiplications (i.e., in RSA, N is at least 1024 bits).

The communication of membership authentication is performed completely in the broadcast channel. Total communication time is to transmit m identities and random integers, $\{(1, r_1), i = 1, 2, \ldots, m\}$, and m authentication responses, $\{AS_i, i = 1, 2, \ldots, m\}$, of all participated members. There is no additional communication in order to establish the group key.

VI. CONCLUSION

We have proposed a novel design of a membership authentication and key establishment protocol for WSNs. Our protocol provides both membership authentication and key establishment simultaneously. However, all existing schemes can provide either user authentication or key establishment separately. We have included the security analysis and performance evaluation in the paper. Our protocol is very efficient in terms of computation and communication, so it is absolutely attractive for secure group communications in WSNs.

ACKNOWLEDGMENT

(Qi Cheng and Chingfang Hsu contributed equally to this work.)

REFERENCES

[1] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.

[2] I. Downnard, "Public-key cryptography extensions into kerberos," *IEEE Potentials*, vol. 21, no. 5, pp. 30–34, Dec. 2002.

[3] L. Harn and J. Ren, "Generalized digital certificate for user authentication and key establishment for secure communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 7, pp. 2372–2379, Jul. 2011.

[4] W.-C. Ku, "Weaknesses and drawbacks of a password authentication scheme using neural networks for multiserver architecture," *IEEE Trans. Neural Netw.*, vol. 16, no. 4, pp. 1002–1005, Jul. 2005.

[5] H.-A. Park, J. Wook Hong, J. Hyun Park, J. Zhan, and D. Hoon Lee, "Combined authentication-based multilevel access control in mobile application for DailyLifeService," *IEEE Trans. Mobile Comput.*, vol. 9, no. 6, pp. 824–837, Jun. 2010.

[6] K. Ren, S. Yu, W. Lou, and Y. Zhang, "Multi-user broadcast authentication in wireless sensor networks," *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4554–4564, Oct. 2009.

[7] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," *IEEE Secur. Privacy Mag.*, vol. 2, no. 5, pp. 25–31, Sep. 2004.

[8] L. Harn, "Group authentication," *IEEE Trans. Comput.*, vol. 62, no. 9, pp. 1893–1898, Sep. 2013.

[9] *IEEE Part 16: Air Interface for Fixed Broadband Wireless Access Systems*, Standard 802.16-2004, 2004.

[10] C. S. Laih, J. Y. Lee, and L. Harn, "A new threshold scheme and its application in designing the conference key distribution cryptosystem," *Inf. Process. Lett.*, vol. 32, no. 3, pp. 95–99, Aug. 1989.

[11] S. Berkovits, "How to broadcast a secret," in *Proc. Int. Cryptol. Conf. Adv. Cryptol.*, 1991, pp. 536–541.

[12] C. H. Li and J. Pieprzyk, "Conference key agreement from secret sharing," *Proc. 4th Australas. Conf. Inf. Secur. Privacy (ACISP)*, 1999, pp. 64–76.

[13] G. Sáez, "Generation of key predistribution schemes using secret sharing schemes," *Discrete Appl. Math.*, vol. 128, no. 1, pp. 239–249, May 2003.

[14] L. Harn and C. Lin, "Authenticated group key transfer protocol based on secret sharing," *IEEE Trans. Comput.*, vol. 59, no. 6, pp. 842–846, Jun. 2010.

[15] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[16] I. Ingemarsson, D. Tang, and C. Wong, "A conference key distribution system," *IEEE Trans. Inf. Theory*, vol. IT-28, no. 5, pp. 714–720, Sep. 1982.

[17] D. G. Steer, L. Strawczynski, W. Diffie, and M. J. Wiener, "A secure audio teleconference system," in *Proc. 8th Ann. Int. Cryptol. Conf. Adv. Cryptol. (Crypto)*, 1988, pp. 520–528.

[18] M. Burmester and Y. G. Desmedt, "A secure and efficient conference key distribution system," *Proc. Int. Cryptol. Conf. Adv. Cryptol.*, 1994, pp. 275–286.

[19] M. Steiner, G. Tsudik, and M. Waidner, "Diffie-hellman key distribution extended to group communication," in *Proc. 3rd ACM Conf. Comput. Commun. Secur. (CCS)*, 1996, pp. 31–37.

[20] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, "Provably authenticated group diffie-hellman key exchange," in *Proc. 8th ACM Conf. Comput. Commun. Secur. (CCS)*, 2001, pp. 255–264.

[21] J. M. Bohli, "A framework for robust group key agreement," in *Proc. Int. Conf. Comput. Sci. Appl. (ICCSA)*, 2006, pp. 355–364.

[22] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably-Secure Authenticated Group Diffie-Hellman Key Exchange," *ACM Trans. Inf. Syst. Secur.*, vol. 10, no. 3, pp. 255–264, Aug. 2007.

[23] J. Katz and M. Yung, "Scalable protocols for authenticated group key exchange," *J. Cryptol.*, vol. 20, no. 1, pp. 85–113, Jan. 2007.

[24] L. Harn and C.-F. Hsu, "Predistribution scheme for establishing group keys in wireless sensor networks," *IEEE Sensors J.*, vol. 15, no. 9, pp. 5103–5108, Sep. 2015.

[25] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.

[26] D. E. Knuth, *The Art of Computer Programming, Semi-numerical Algorithms*. Reading, MA, USA: Addison-Wesley, 1981.

[27] A.-N. Shen, S. Guo, and H.-Y. Chien, "An efficient and scalable key distribution mechanism for hierarchical wireless sensor networks," in *Proc. IEEE Sarnoff Symp.*, Mar. 2009, pp. 1–5.

[28] O. Cheikhrouhou, "Secure group communication in wireless sensor networks: A survey," *J. Netw. Comput. Appl.*, vol. 61, pp. 115–132, Feb. 2016.

[29] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 41–47, doi: 10.1145/586110.586117.

[30] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. Symp. Secur. Privacy*, May 2003, pp. 197–213.

[31] W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE INFOCOM*, 1997, p. 597.

[32] R. Blom, "Non-public key distribution," in *Advances in Cryptology-Proceedings of Crypto*, D. Chaum, R. L. Rivest, A. T. Sherman, Eds. New York, NY, USA: Plenum, 1982, pp. 231–236.

[33] C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Advances in Cryptology*, E. F. Brickell, Ed. Berlin, Germany: SpringerVerlag, 1992, pp. 471–486.

[34] E. Khan, E. Gabidulin, B. Honary, and H. Ahmed, "Matrix-based memory efficient symmetric key generation and pre-distribution scheme for wireless sensor networks," *IET Wireless Sensor Syst.*, vol. 2, no. 2, pp. 108–114, 2012.

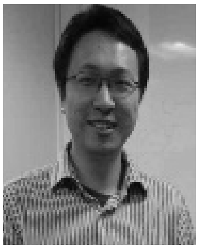
[35] A. Albakri and L. Harn, "Non-interactive group key pre-distribution scheme (GKPS) for end-to-end routing in wireless sensor networks," *IEEE Access*, vol. 7, pp. 31615–31623, 2019.

[36] A. Albakri, L. Harn, and S. Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)," *Secur. Commun. Netw.*, vol. 2019, pp. 1–11, Jul. 2019.

[37] L. Harn, C.-F. Hsu, O. Ruan, and M.-Y. Zhang, "Novel design of secure End-to-End routing protocol in wireless sensor networks," *IEEE Sensors J.*, vol. 16, no. 6, pp. 1779–1785, Mar. 2016.

QI CHENG received the M.Eng. degree in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2008. He is currently a Senior Engineer with the Engineering Department, Wuhan Digital Engineering Institute, Wuhan. His research interests include network security and especially in secret sharing and its applications.

CHINGFANG HSU received the M.Eng. and Ph.D. degrees in information security from the Huazhong University of Science and Technology, Wuhan, China, in 2006 and 2010, respectively. From September 2010 to March 2013, she was a Research Fellow with the Huazhong University of Science and Technology. She is currently an Assistant Professor with Central China Normal University, Wuhan. Her research interests include cryptography, network security, and especially in secret sharing and its applications.



ZHE XIA received the M.Eng. and Ph.D. degrees in information security from the University of Surrey, U.K., in 2005 and 2009, respectively. From 2009 to 2013, he was a Research Fellow with the University of Surrey. He is currently an Assistant Professor with the Department of Computer Science, Wuhan University of Technology, Wuhan, China. His research interests include cryptography, network security, and especially in secret sharing and its applications.

LEIN HARN received the B.S. degree in electrical engineering from National Taiwan University, in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook, in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota, in 1984. He is currently a Professor with the Department of Electrical and Computer Engineering, University of Missouri-Kansas City (UMKC). His current research interest includes investigating new ways of using secret sharing in various applications.