Identity Authentication and Key Agreement
Integrated Key Management Protocol for Heterogeneous Sensor Networks

Chunguang Ma
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
China State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
College of National Secrecy, Harbin Engineering University, Harbin 150001, China
Email: machunguang@hrbeu.edu.cn

Jiuru Wang, Peng Wu
College of Computer Science and Technology, Harbin Engineering University, Harbin 150001, China
Email: {jiuruwang, wupeng}@hrbeu.edu.cn

Hua Zhang
China State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
Email: zhanghua_288@bupt.edu.cn

Abstract—In order to integrate identity authentication and key agreement, a novel academic thought is set out, a fasting one-way accumulator is constructed, and a fasting one-way accumulator-based key management protocol is put forward for Heterogeneous Sensor Networks (HSNs). The experiments and analysis show that the proposed protocol not only implements identity authentication function, but has high connectivity and security, low energy consumption as well.

Index Terms—heterogeneous sensor network, fasting one-way accumulator, identity authentication, key agreement

I. INTRODUCTION

Heterogeneous Sensor Networks (HSNs) has been an area of great interest to both academia and industry. It is usually deployed in unattended, non-controlled environment, so security is very important for HSN applications in military, homeland security and other hostile environments [1]. As the basis for a variety of security mechanisms, key management problem must be resolved first [2].

In HSN security mechanism, both authentication key and communication key belong to the range of key management. The former provides protection for authentication security, and the latter does the support to secure communication. Several literatures have studied security issues in sensor network. But most of them mainly focus on the distribution and management of communication key, including the Eschenauer and Gligor’s pioneering protocol [3], its extensions [4-5], as well as routing-driven protocols [6], and are designed from random graph theory point of view. Only few user authentication protocols are well suited for sensor networks [8]. The research combining them together is rare.

Through our studies, we find that the randomness assumption ignores the fact that all nodes belong to a set, limits the study of authentication protocol, makes the identity authentication and key agreement separation, and restricts the innovative of academic thoughts. So, in this paper, we introduce a novel academic thought, construct a fasting one-way accumulator, and propose a fasting one-way accumulator-based key management protocol for HSNs. The proposed protocol integrates identity authentication and key agreement together. The experiments and analysis show that the protocol not only implements identity authentication function, but has high security and connectivity, low energy consumption as well.

The rest of paper is organized as follows: Section 2 provides the related works. Section 3 introduces the academic though. Section 4 describes the fasting one-way
accumulator. Section 5 provides the protocol. Section 6 gives the experiment and analysis. Section 7 concludes this paper.

II. RELATED WORKS

Eschenauer and Gligor [3] first proposed a probabilistic pre-distribution scheme for key management in sensor networks. The main idea is that let each sensor node randomly pick up a set of keys from a key pool before deployment, so any pair of sensor nodes has a certain probability of sharing at least one common key. Liu [4], et al., proposed a group-based deployment model to improve key pre-distribution. In this model, sensor nodes are only required to be deployed in groups. Feng [5], et al., proposed a general key seeds management and assignment (KSMA) model to study the security of key pre-distribution schemes, which is used to study the security of key pre-distribution schemes with five attributes for requirement of confidentiality and authentication. In Ref. [6], Du, et al., proposed a routing-driven key management protocol for Heterogeneous Sensor Networks, which only establishes shared keys for neighbor sensors that communicate with each other. The routing-driven protocol utilizes Elliptic Curve Cryptography in the design of an efficient key management scheme for sensor nodes. Yao [7], et al., put forward a broadcast authentication algorithm based on the properties of fasting one-way accumulator. Vaidya [8], et al., proposed a user authentication protocol for Wireless Sensor Networks. Literatures [3-8] are all designed from the standpoint of random graph theory. All of them ignore the fact that all nodes belong to a set, so they have studied authentication key and communication key, separately. In this paper, we integrate them together.

Benaloh and Mare [11] presented one-way accumulator, which satisfies a quasi-commutative property that allows it to be used for membership testing. Nyberg [12] introduced a fasting accumulator, which can be efficiently realized in practice using existing cryptographic hash algorithms and pseudorandom sequence generators.

III. ACADEMIC THOUGHT

A typical HSN model consists of two physically different types of sensor nodes: powerful High-end sensors (H-sensors) and Low-end sensors (L-sensors) [9]. As shown in Fig. 1, both H-sensors and L-sensors are uniformly and randomly distributed in the field. After deployment, clusters are formed in an HSN [10]. It is natural to let powerful H-sensors serve as cluster-heads (CH) and form clusters around them. All H-sensors form a backbone in the network. Each L-sensor sends data to its cluster head (an H-sensor) through one or more hops. Furthermore, an H-sensor aggregates data and transmits compressed data to the sink via the H-sensor backbone. So, the many-to-one communication pattern plays a dominant role in HSN. An L-sensor only needs to communicate with a small part of its neighbors, which are in the routes from itself to the sink. That is to say, an L-sensor does not need shared-keys with all neighbors [5].

Let V represents nodes set (including H-sensors and L-sensors), E for edges (links) set, an HSN can be defined as follows: HSN=(V, R), where, V={S, H₁, ... , Hₚ, L₁, ..., Lₚ, m≥1, n≥m}, R={R₁, R₂}, R₁={<S, H₁> | 1≤i≤p}, R₂={<Hᵢ, Lⱼ> | m≥1, n≥m}. After deployment and before routing is established, the elements of V only belong to the same set, and have no other relationships. If x, y ∈ V exists a path, (x, y) constitutes an edge from x to y. So, the nodes set V and the edges set E constitute a network. The key management issues of HSN could be transformed into the problems of identity authentication and key agreement between the set elements. Fasting one-way accumulator (FOA) is an effective technology to solve the problems.

IV. FASTING ONE-WAY ACCUMULATOR

In this section, we will firstly introduce fasting one-way accumulator and its properties, and then construct a FOA.

A. FOA Properties

Fasting one-way accumulator [12] is a type of non-trapdoor one-way accumulator. It can accumulate all elements of the set to a value, and provides a witness for each element to demonstrate that the element is a part of the original hash [11]. It is commonly used to construct a membership testing system without the need for a trusted central authority.

A family of FOA is an infinite set of functions hᵢ : Xᵢ × Yᵢ → Xᵢ having the following properties [11]:

1. There exists a polynomial P such that for each integer k, hᵢ(x, y) is computable in time P(k, ||x||, ||y||) for all x ∈ Xᵢ and all y ∈ Yᵢ.

2. There is no polynomial P such that there exists a probabilistic polynomial time algorithm which, for all sufficiently large k, will when given k, a pair (x, y) ∈ Xᵢ × Yᵢ, and a y’ ∈ Yᵢ, find an x’ ∈ Xᵢ such that hᵢ(x, y) = hᵢ(x’, y’) with probability greater than 1/P(k) when (x, y) is chosen uniformly among all
elements of $X_i \times Y_i$ and $Y'$ is chosen uniformly from $Y_i$.

3. A function $h_k : X_i \times Y_i \rightarrow X_k$ is said to be quasi-commutative, if for all $\forall x \in X_i$ and for all $\forall y, y_j \in Y_i$, $h_k(h_k(x, y), y_j) = h_k(h_k(x, y_j), y_j)$. From the properties of the FOA, we can obtain the following theorems:

Theorem 1. A fasting one-way accumulator $h_k : X_i \times Y_i \rightarrow X_k$, given $\forall x, x_j \in X_i$, $\forall y, y_j \in Y_i$, then $z_i \neq z_j$.

Proof. Suppose a fasting one-way accumulator $h_k : X_i \times Y_i \rightarrow X_k$, for $\forall x, x_j \in X_i$, $\forall y, y_j \in Y_i$. Let $z_i = h_k(x_i, y)$, $z_j = h_k(x_j, y)$. By the properties of FOA, we assert that: $z_i \neq z_j$.

B. FOA Design

Different from traditional one-way accumulator, fasting one-way accumulator is constructed based on a common hash function. All operations are simple bit operations and can achieve rapidly accumulation. The constructor is as follows.

Let $N = 2^t$ be an upper bound to the number of items to be accumulated and let $r$ be an integer. We assume that there is a one-way hash function $H$ which maps bit strings of arbitrary length to bit strings of fixed length $s = rt$. Let $x_i, \ldots, x_m, m \leq N$, be the items to be accumulated and let $y_i = H(x_i)$, $i = 1, \ldots m$ be their corresponding hash codes. These strings are divided into $r$ blocks of length $t$ and denoted by $y_i = (y_{i1}, \ldots, y_{it})$. Moreover, we map each item $y_i$ to a binary string $b_i$ of length $r$ by replacing $y_{ij}$ by 1, if $y_{ij} \neq 0$, and by replacing $y_{ij}$ by 0, if $y_{ij}$ is a string of zero bits [12]. In this way, we have mapped each item $x_i$ to a bit string $b_i = \alpha_i(\beta_i) = \alpha_i(H(x_i)) = (b_{i1}, \ldots, b_{ir})$ of length $r$, which in the case of an ideal hash function $H$ can be considered as values of $r$ independent binary random variables, for which the probability of taking the value 1 is equal to $2^{-t}$.

The accumulated hash value $z = (a_1, \ldots, a_r)$ is gotten by $z = H_{F OA}(k_z, y)$, which is computed as “or” operation of $k_z$ and $y$. Then, that is to say:

$z = H_{F OA}(k_z, y) = k_z \mid \alpha(H(x))$. It is constructed based on one-way hash function, so it has one-way property. With the exchange property of logical “or” operator, it is quasi-commutative. Namely, for all $\forall y, y_j \in Y_i$,

$H_{F OA}(H_{F OA}(k_z, y), y) = H_{F OA}(H_{F OA}(k_z, y), y) = H_{F OA}(H_{F OA}(k_z, y), y)$. So, $z = H_{F OA}(k_z, y) = k_z \mid \alpha(H(x))$ is a one-way accumulator.

Furthermore, with the absorbent property of logical "or" operation $X \mid X = X$, $H_{F OA}(k_z, y)$ can be used to verify the membership of an item $x$. Namely:

$H_{F OA}(H_{F OA}(k_z, y), y) = H_{F OA}(k_z, y)$

V. KEY MANAGEMENT PROTOCOL FOR HSN

In this Section, we present an efficient key management protocol for HSN, which utilizes FOA and the many-to-one communication pattern in sensor networks. We adopt a realistic model of HSN which is used in most sensor network applications. The network consists of one sink, $m$ H-sensors and $n$ L-sensors ($m < n$). The sink is well protected and trusted. H-sensors are equipped with tamper-resistant hardware. Due to cost constraints, L-sensors are not equipped with tamper-resistant hardware. Each L-sensor (and H-sensor) is static and aware of its own location. Both L-sensor and H-sensor are powered by batteries and have limited energy supply. Each L-sensor (and H-sensor) has a unique node ID. L-sensors use multi-hop communications to reach H-sensors, and H-sensors use multi-hop communications to reach the sink. Since H-sensors are powerful nodes, key establishment for H-sensors are relatively easy. In this paper, we focus on key establishment for L-sensors. The key management protocol is performed basically in five phases: key pre-distribution, identity authentication, key agreement, adding new nodes and removing nodes.

A. Key Pre-distribution

Each L-sensor (say $i$) is pre-loaded with a random Data, a shared-key with sink (say $k_{ui}$), and a HMAC($k_{ui}$), which is the message authentication code (MAC) of message $m$ using the symmetric key $k$. An H-sensor has large storage space. It is pre-loaded with the HAMC and all of the shared-keys. Each L-sensor also performs the following process:

1. The MAC set for the node is generated by each pre-loaded shared key. Namely, $[MAC = HMAC(k_{ui}, Data, m + n \geq i \geq 1)]$. Randomly select a $k_{ui}$, and compute the accumulated value, $z_i = k_{ui} \mid \alpha(H(MAC)) \mid \cdots \mid \alpha(H(MAC_{num}))$. $z_i$ is also stored to the node.

B. Identity Authentication

After sensor deployment, clusters are formed in an HSN. The H-sensors serves as cluster-heads and the L-sensors play a part of cluster members. The details of clustering scheme can be found in Ref. [10]. If two sensors are in communication range, they attempt to establish session key. All legitimate nodes belong to the same set, but have no other relationship. To prevent malicious nodes, before the key agreement is established, nodes have to authenticate each other. Fig. 2 shows the specific process.
In this section, we evaluate the performance of the proposed key management protocol. The E-G protocol [3] is used for comparison. We compare the connectivity and energy consumption in subsection 6.1 and 6.2, respectively. The security analysis is presented in subsection 6.3.

A. Connectivity Analysis

Assume that the number of H-sensors and L-sensors in an HSN is $M$ and $N$, respectively. Typically we have $M < N$. FOA-based key management protocol establishes shared key through the key agreement. It is known from the section 4.3 that any two legitimate nodes in communication range can establish unique shared key through the exchange $ID \| Data \| z$. Thus, the connectivity
The probability of the proposed protocol is constant. However, in the E-G protocol, for H-sensors and L-sensors the different storage capability, the number of keys they store is not equal. Assume that when the key pool is \( S \), the number of keys in H-sensor and L-sensor is \( H \) and \( L \) (\( H \geq L \)), respectively. The probability (\( p_{HL} \)) of between L-sensor at least one key is shared as follows:

\[
p_{HL} = 1 - \left( \frac{1}{S} \right)^{2(S-H-L+1)} - \left( \frac{2}{S} \right)^{2(S-2-H-L+1)}
\]

The probability (\( p_{HL} \)) of sharing at least one key between H-sensor and L-sensor is as following:

\[
p_{HL} = 1 - \left( \frac{1}{S} \right)^{(S-H-L+1)} - \left( \frac{1}{S} \right)^{(S-L-L+1)}
\]

It is shown in Fig. 4 that the connectivity probability of the proposed protocol is always 1. In E-G protocol, the relationship between \( p_{HL} \) (\( p_{HL} \)) and the combinations of \( S \) and \( L \) (\( H \)). While \( S \) is equal to 10, 20, 30, 40, 50, 60, 70, 80, 90, 100 respectively, \( L \) is equal to 3, 7, 9, and \( H \) is equal to 3, 8, 12, we get the probability of at least sharing one key. It can be seen that while \( H \) and \( L \) are unchanged, \( S \) becomes larger, and the probability is smaller. However, while \( S \) stays the same, and \( L \) (\( H \)) becomes bigger, the probability increases.

### B. Energy Consumption Analysis

We run simulations to compare the energy consumption of our protocol and the E-G protocol. The simulations are conducted by using the Omnet4.1 simulator. The simulation testbed has 1 sink, 4, 5, 6, 7, 8 H-sensors, and corresponding 16, 35, 54, 73, 92 L-sensors randomly distributed in a 200*200m² area. The system parameters are set according to the MICA2 Mote datasheet [13]. We compare the total energy consumption under the proposed protocol and the E-G protocol in the same deployment. The energy consumption reported here only includes the energy used to set up security keys, but does not include energy for data communications.

As shown in Fig. 5, the energy consumption of the proposed protocol is lower than the E-G protocol. The reason is that utilizing the many-to-one communication pattern can effectively lower the energy consumption in sensor networks.

### C. Security Analysis

The security of the fastest one-way accumulator depends in a proven way only on the randomness properties of the hash function \( H \). We also derive estimates to what is the required size of the length of the accumulator to achieve a certain security level.

**Theorem 2.** Let \( b_0 \) and \( c_i \) be independent binary random variables such that \( Pr(b_0 = 0) = Pr(c_i) = 2^{-r} \), for \( i = 1, \ldots, m \) and \( j = 1, \ldots, r \). Let \( a = (a_1, \ldots, a_o) \) be the coordinatewise product of the \( r \)-tuples \( b = (b_1, \ldots, b_m) \), \( i = 1, \ldots, m \). Then the probability that, for all \( j = 1, \ldots, r \), we have \( c_j = 1 \), only if \( a_j = 1 \), is equal to \((1 - 2^{-r}(1 - 2^{-r})^m)\)' [7,12].

Proof. For each \( j = 1, \ldots, r \) the probability that \( c_j = 1 \) and \( a_j = 0 \) equals \( 2^{-r}(1 - 2^{-r})^m \). Assuming that \( H \) produces truly random hash codes, and recalling that \( N = 2^r \) is the upper bound to the number of items to be accumulated, we get by the theorem that the probability of finding a forged item to a list described by an accumulated hash value \( a = (a_1, \ldots, a_o) \) can be estimated as follows:

![Figure 4 Probabilities about shared-key discovering](image-url)
(1 - 2^{-\frac{1}{2}}(1 - 2^{-\frac{1}{2}})^n) \leq (1 - \frac{1}{2^n})(1 - \frac{1}{2^n}) \approx (1 - \frac{1}{2^n})^2 \approx e^{-\frac{1}{2^n}}
\nonumber

Theorem 3 In the process of nodes joining, it can resist Man-in-the-Middle Attack.

Proof. In the process of nodes joining, the adversary can intercept broadcast messages (\text{ID} || \text{Data} || z) between the nodes. The adversary can tamper with \text{ID} \rightarrow \text{ID}', Data \rightarrow \text{Data}' or z \rightarrow z'. If the \text{ID} was tampered with, although it goes through authentication, malicious node can be found in section 4.3, and can't complete the key agreement. If the Data or z was tampered with, for z'= H_{\text{FOA}}(z, \text{HMAC}(k_a, \text{Data})) \neq z or z''= H_{\text{FOA}}(z', \text{HMAC}(k_a, \text{Data})) \neq z', nodes cannot go through authentication. So, the process resists Man-in-the-Middle Attack.

VII. CONCLUSIONS

We first introduce a novel academic thought, then construct a fasting one-way accumulator, finally propose an efficient key management protocol is for Heterogeneous Sensor Networks. The proposed protocol utilizes fasting one-way accumulator and the many-to-one communication pattern in sensor networks. It integrates identity authentication and key agreement together. The experiment and analysis show that the proposed protocol not only has identity authentication function, but has high connectivity and security, low energy consumption. In future work, we'll delve into how to better integrate authentication key and communication key in HSN, and design more comprehensive key management protocol.

ACKNOWLEDGMENT

The authors like to express their sincere thanks to the anonymous reviewers and the editor P. Mahanti of Journal of Computers for their constructive comments and suggestions.

REFERENCES


Chunguang Ma was born in Shuangyashan on the 3th January, 1974. He received his Ph. D. degree of cryptography in July 2005 at Beijing University of Posts and Telecommunications. He is a professor at college of computer science and technology, Harbin Engineering University. His research interests include cryptography, information security, network coding, Ad hoc & WSN.

Jiuru Wang was born in Nliny on the 28th September, 1983. He got master degree in the field of computer application technology from Anhui Science & Technology University, Huanain city, China in 2009. He is now a Ph. D. candidate in computer science and technology college of Harbin Engineering University, China. His research interests include information security and Ad hoc & WSN.

Peng Wu was born in Qiqihar on the 31th December, 1974. He got master degree in the field of computer application technology from Harbin Engineering University, Harbin city, China in 2009. His research interests include information security.

Hua Zhang was born in Siping on the 16th April, 1978. She received master degrees in the field of cryptography from Xiian University, Xi’an city China in 2005, and received her Ph. D. degree of cryptography in 2008 at Beijing University of Posts and Telecommunications.

She works as a Lecturer in the same college after her Ph. D. graduation. Her research interests include cryptographic protocol and information security.