Analytic Hierarchy Process aided Key Management Schemes Evaluation in Wireless Sensor Network

Article *in* Journal of Networks · January 2012

DOI: 10.4304/jnw.7.1.88-100 · Source: DBLP

Yoshiaki Hori
Saga University
109 PUBLICATIONS **453** CITATIONS

Kouichi Sakurai
Kyushu University
506 PUBLICATIONS **2,769** CITATIONS

Analytic Hierarchy Process aided Key Management Schemes Evaluation in Wireless Sensor Network

Ruan Na [†], Yizhi Ren [‡], Yoshiaki Hori [†], Kouichi Sakurai [†]
[†] Department of Informatics, Kyushu University, Fukuoka, Japan
[‡] School of Software Engineering, Hangzhou Dianzi University, China
Email: {ruannana, renyizhi}@gmail.com, {hori, sakurai}@inf.kyushu-u.ac.jp

***Abstract*— Wireless sensor networks (WSNs) have been widely used in various applications. Since their sensor nodes are resource-constrained and their security primitives need to store a set of security credentials to share a secure channel, key management is one of the most challenging issues in the design of WSN. Currently, various efficient lightweight key management schemes (KMs) have been proposed to enable encryption and authentication in WSN for different application scenarios. According to different requirements, it is important to select the trustworthy key management schemes in a WSN for setting up a fully trusted WSN mechanism. In this context, adaptive methods are required to evaluate those schemes.**

In this paper, we exploit Analytic Hierarchy Process (AHP) to help with the complex decision. Specifically, we consider the following performance criteria: *scalability, key connectivity, resilience, storage overhead, processing overhead and communication overhead*. Two case studies are added for verifying our proposal. Via the two case studies, it is verified that our method is able to help selecting a suitable scheme for given requirements.

***Index Terms*— Analytic Hierarchy Process, Key management scheme, Trustworthy decision, Wireless sensor network**

I. Introduction

A. Background

The advance in miniaturization techniques and wireless communications has made possible the creation and subsequent development of the wireless sensor network (WSN) paradigm [1]. The application area of WSN includes military sensing and tracking, environmental monitoring, patient monitoring and smart environment. When a sensor node is installed in a dangerous and untrusted area, its security becomes very important. Thus, WSN security is a prerequisite for wider use [2]. The communication channels between any pair of nodes inside WSN must be protected to avoid attacks from external parties. Such protection, in terms of confidentiality, integrity and authentication, is provided by some security primitives. A key management scheme is an important security primitive for WSN. The task of generating and distributing those keys has to be done by a global key management system [3]. For the above reasons, designing a trustworthy key management scheme is a necessary work. Meanwhile, to select a appropriate key management scheme is a necessary work.

In this paper, we design an evaluation method which supports the decision-making processes of selecting a trustworthy key management scheme in a WSN. We focus on the calculation of how much the existing key management schemes can be appropriate to perform a particular application. The trust of the trustworthy decision is based on the firm belief in the reliability under the assumed wireless sensor network scenario. The key management schemes must satisfy traditional needs of security, such as availability, integrity, confidentiality, authentication and non-reputation [6] in a typical wireless network. Compared with the typical wireless network, the key management has other special challenges such as resilience, expansibility and efficiency [7] in WSN because of its specificity.

B. Related Work

Recent research works focus on producing an efficient system to evaluate these key management schemes. In recent years, there has been a significant progress on key management schemes in WSN. Researchers have proposed a large number of key management schemes in WSN which focus on different security requirements. Each scheme has its own advantages and disadvantages. Even though quite a number of key management schemes in wireless sensor network exist now, they can be divided into six categories. The six categories are stated as follows: Dedicated pair-wise key management solution in distributed wireless sensor network (DWSN), reusable pair-wise key management solutions in DWSN, group-wise key management solutions in DWSN, pair-wise key management solutions in hierarchical wireless sensor network (HWSN), group-wise key management solutions in HWSN and network-wise key management solutions in HWSN [3]. If changing into another perspective, because WSN is energy limited network and pre-distributed key

This paper is based on “A Generic Evaluation Method for Key Management Schemes in Wireless Sensor Network,” by R. Na, Y. Ren, Y. Hori and K. Sakurai, which appeared in the Proceedings of the 5th International Conference on Ubiquitous Information Management and Communication (ICUIMC), Seoul, Korea, February 2011. © 2011 ACM.

This work was supported by the governmental scholarship from China Scholarship Council.

doi:10.4304/jnw.7.1.88-100

management scheme is energy-efficient scheme, most of the key management schemes in WSN are based on pre-distribution key management schemes. Commonly used key management schemes in WSN are listed as follows: random pre-distribution key management scheme based on key-pool [8]; pre-distribution key management scheme based on polynomial [9]; pre-distribution key management scheme based on block design [10]; pre-distribution key management scheme based on position [11]; pre-distribution key management scheme based on matrix [12] and so on [13].

Some researchers proposed certain evaluation indexes for qualitative evaluation of these key management schemes in WSN [3]. However, such proposals have limited utility unless they take node replication attacks and robustness into consideration. Their proposals fail to address all of the criteria that a key management scheme in WSN should satisfy to.

In this paper, we propose a generic method to evaluate key management schemes, which can help researchers to select the scheme quantitatively according to different network requirements. The most related work to our research on security evaluation is Hwang *et al.* [5]. It employs the Analytical Hierarchy Process (AHP) method in guiding information security policy decision making. It uses the application of AHP as a method to develop information security decision model for information security policy. Meanwhile, after comprehensively surveying all of the criteria for KMs evaluation in WSN, we propose an AHP-aided method to select the optimum key management scheme for an assumed WSN.

C. Challenging Issues

The following reasons motivate us to propose the AHP-aided method for evaluating key management schemes in wireless sensor network.

1) The security of a WSN depends on the existence of efficient key management solutions [3]. Many key establishment techniques have been designed to address the trade off between limited computational resources and security requirements, but it is not easy to determine which scheme is the best one in an assumed scenario.
2) All these key management schemes have their own advantages and disadvantages. All of them can be suitable for different needs. Comprehensive consideration of the parameters selection is not a simple problem.
3) To select the most proper key management scheme quantitatively from a large amount of existing schemes is not an easy issue [15].
4) Despite the utmost importance of a generic evaluation method for these key management schemes, it is surprising that we find almost nothing in literature on this subject.

D. Our Contribution

In this paper, we propose an evaluation method to evaluate the key management schemes, which can help us to select the scheme quantitatively according to different network requirements. The contributions of our paper can be summarized as follows:

1) We use an analytical hierarchy process (AHP) model to construct a framework to do the decision making. AHP can help with a quantitatively decision. Thus, we can overcome the difficulty in selecting a proper key management scheme for wireless sensor network having multiple criteria decision making.
2) Based on our proposal, we provide evaluation and analysis of the existing key management schemes. We show that our method can build an intuitive method to select a proper scheme and to present key management schemes in the order of suitability, based on the previously given network requirements. In a word, we provide a feasible quantitative evaluation system to select the best key management scheme from various schemes.
3) Finally, we classify several typical key management schemes and make a comparison among the trade off in those schemes. At the same time, we can obtain quantitative analysis results via two kinds of case study. In other words, our method can be helpful in a complicated network environment.

This work is organized as follows: Section II describes basic definitions and notions used in wireless sensor network for key management schemes evaluating. At the same time, corresponding case study is proposed. Section III provides our quantitative system which based on linear algebra and focused on matrix. Section IV discusses the system in details via two case studies. Finally, we draw conclusions in Section V.

II. Preliminaries

A. Brief reviews of AHP

In a set number of application domains, the Analytical Hierarchy Process (AHP) is a decision approach designed to aid in the solution of complex multiple criteria problems. It was developed by Thomas L.Saaty in the 1980s [4]. This method has been found to be an effective and practical approach that can make complex and unstructured decisions. The AHP has been used in a large number of applications to provide certain structures on a decision making process. When used in the systems engineering process, AHP can be a powerful tool for comparing alternative design concepts. The decision-maker judges the importance of each criterion in pair-wise comparisons. The outcome of AHP is a prioritized ranking or weighted of each decision alternative. There are three steps for considering decision problems by AHP: constructing hierarchies, comparative judgments, and synthesis of priorities.

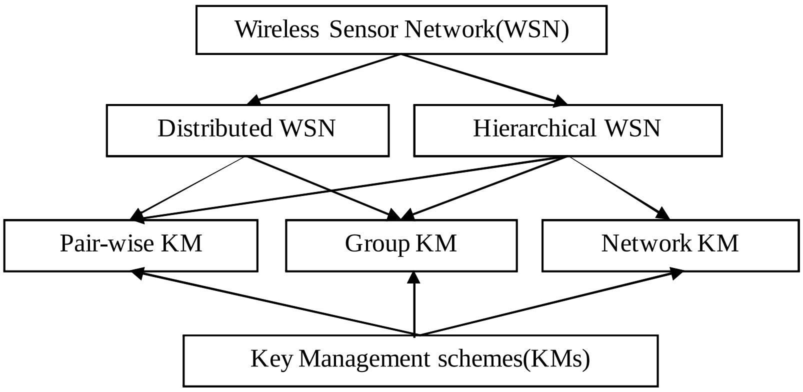


Figure 1. Classification of Key Management schemes

1) **Construction hierarchies:** User of the AHP first decomposes his decision problem into some hierarchy of more easily comprehended sub problems, each of them can be analyzed independently.
2) **Comparative judgments:** After the hierarchy is built, the decision makers systematically evaluate various elements of the hierarchy by comparing each one of them to another one of them at a time. In making the comparisons, the decision makers can either use concrete data about the elements or use their judgments about the elements' relative meaning and importance. The AHP converts these evaluations to numerical values that can be processed and compared over the entire range of the problem.
3) **Synthesis of Priorities:** Numerical priorities are calculated for each of the decision alternatives. These numbers represent the alternatives' relative ability to achieve the decision goal. Something are presumable missing in allowed range.

The above three steps show a brief review of AHP hierarchy for the decision making process.

Futhermore, details on both the synthesis of priorities and the measurement of consistency are claimed as follows [4]:

- n: the order of the matrix. The AHP authors use n for explaining the size of these matrixes in AHP method. In section III, the matrix of hierarchies and the matrix of judgements will be used in our AHP-aided method.
- λ: the eigenvalue of the matrix. Maximum value of λ is expressed by λ_{max}. If we want to calculate the consistency ratio, we should calculate the eigenvector of the relative weights λ_{max} for each matrix with order n.
- RI: the average Random Index for consistency checking. RI is a known random consistency index obtained from a large number of simulations which run and vary depending upon the order of matrix. Tables I shows the value of the RI for matrix with the size from order 1 to 10 [16].
- CI: the Consistency Index. CI for each matrix of order n can be calculated by using the formula: $CI = (\lambda_{max} - n)/(n-1)$.
- CR: the Consistency Ratio. CR is calculated by using the formula: $CR = CI/RI$.

TABLE I.
AVERAGE RANDOM INDEX (RI) BASED ON MATRIX SIZE

Size of matrix(n)	Random consistency Index(RI)
1	0
2	0
3	0.52
4	0.89
5	1.11
6	1.25
7	1.35
8	1.40
9	1.45
10	1.49

As constructing hierarchy is the first step of AHP, the pair-wise comparisons generate a matrix of relative rankings for each level of the hierarchy. The number of criteria depends on the number elements at each level. The order of the criteria at each level depends on its lower level number of elements. After all criteria are developed and all pair-wise comparisons are obtained, eigenvectors of the relative weights (the degree of relative importance among the elements), global weights and the maximum eigenvalue λ_{max} for each matrix are calculated by using Expert Choice software (Expert Choice, 2000). The software is easy to use and understand. It provides visual representations of overall ranking on a computer screen.

The value of λ_{max} is an important validating parameter in AHP. It is used as a reference index to screen information via calculating the consistency ratio CR of the estimated vector. This step is in order to validate whether the pair-wise comparison matrix provides a completely consistent evaluation or not.

n-order matrix means the order of matrix n equals n. In section III, our proposal which is based on AHP will use 5-order matrix and 6-order matrix. Thus, we present the consistency check of them in this section in advance.

When $n = 5$, we can calculate the eigenvalue of the matrix λ for consistency check. The processes are as follows:

1) Selecting $n = 5$ from Table I as an example, the average random index RI is 1.11.
2) Because the matrix should be validated to pass the consistency check, the consistency ratio CR need to be smaller than 0.1. Meanwhile, CR equals CI/RI.
3) Thus, the consistency index CI needs to satisfy: $CI < 0.1 \times 0.11 = 0.011$
4) Furthermore, as $CI = (\lambda - n)/(n-1) = (\lambda - 5)/4$ and $CI < 0.011$, the maximum eigenvalue λ is smaller than 5.444.
5) The 5-order matrix will pass the consistency check when $\lambda < 5.444$.

Similar to the process where $n = 5$, we do consistency check while $n = 6$. The result is as follows:

1) When there is $n = 6$, the average random index is $RI = 1.25$. Accordingly, the maximum eigenvalue λ is smaller than 6.625.
2) The 6-order matrix will pass the consistency check when $\lambda < 6.625$.

B. Classification of key management schemes in WSN

Key management schemes (KMs) in wireless sensor network (WSN) can be categorized into several types. Figure 1 explains the classification of KMs in WSN. WSN are organized in distributed or hierarchical structures in generally. WSN communication usually occurs in ad hoc manner, and shows similarities to wireless ad hoc network. When nodes in hierarchical WSN communicate, data flow may be classified into three parts: pair-wise (unicast) among pairs of sensor nodes and from sensor nodes to base station, group-wise (multicast) within a cluster of sensor nodes and network-wise (broadcast) from base stations to sensor nodes. Likewise, data flow in distributed WSN is similar to data flow in hierarchical WSN with a difference that network-wise (broadcast) messages can be sent by every sensor nodes.

As Table II shows, S. A. Camtepe *et al.* 2008 [3] classified the currently existing key management schemes based on the network structure. The network structure is classified into two types: Distributed WSN (DWSN) and Hierarchical WSN (HWSN). In DWSN, key management schemes (KMs) in DWSN are categorized into three types: dedicated pair-wise KMs, reusable pair-wise KMs and group-wise KMs. Meanwhile, KMs in HWSN are categorized into three types: pair-wise KMs, group-wise KMs and network-wise KMs. Our evaluation work follows this classification.

III. Our Proposal based on AHP

In order to determine which key management scheme is the best for an assumed WSN scenario, we propose a method based on AHP.

In different proposed key management schemes, there have different parameters assumption even distinct assumption. It is not possible to give strict quantitative comparison criteria due to distinct assumptions made by these key management solutions. However, the following criteria can be used to evaluate and compare these key management schemes in WSN [3]. Our target is to give quantitative comparisons among various KMs in WSN based on these five criteria.

- **Scalability**: Ability of a key management solution to handle an increase in the WSN size.
- **Key connectivity**: Probability that a pair or a group of sensor nodes can generate or find a common secret key to secure their communication.
- **Resilience**: Resistance of the WSN against node capture and node replicate. The adversary often captures or replicates a sensor node, such as in some well-known network attacks in the WSN (e.g., sybil attack and wormhole routing attack). Keys which are stored on a sensor node or exchanged over radio links should not reveal any information about the security of any other links.
- **Storage overhead**: Amount of memory units required to store security credentials.
- **Processing overhead**: Amount of processing cycles required by each sensor node to generate or find a common secret key.
- **Communication overhead**: Amount and size of messages exchanged between a pair or a group of sensor nodes to generate or find a common secret key.

We can see that processing overhead is based on the hardware selecting. Considering the power consumption, especially comparing with communication overhead [35], processing overhead is not the main power consumption for WSN. Thus, it is appropriate if we omit the processing overhead of KMs in our AHP-aided evaluation proposal.

Numerical priorities, derived from the decision makers' input, are shown for each item in the hierarchy of AHP method. To make comparisons, the scale of numbers indicates that how much one element is more important than another element. The indication is based on the criterion or property with respect to which they are compared.

Then, based on the five criteria which are used to evaluate and the key management scheme comparison in an assumed network scenario by quantitative calculation, we present the framework of AHP based method for selecting the most suitable key management scheme among these schemes.

Figure 2 is the framework of our AHP-aided method. In the top of this figure, there is an assumed network scenario. Under the scenario, six criteria are listed. Under the criteria, six key management schemes which are called alternatives are listed. Each of the alternatives belongs to one category of key management schemes. In this figure, the criteria are used to select the optimum alternative for the assumed network scenario.

Our proposal consists of three steps. Figure 3 shows the procedure of our proposal. First step is establishment of a structural hierarchy. The center of this step is to construct pair-wise comparison matrix A for assumed network

TABLE II.
CLASSIFICATION OF KMS [S. A. CAMTEPE. 2008]

	Notions	Steps
DWSN	Dedicated pair-wise KMs	**H.Chan *et al.* 2003** [8],D.liu *et al.* 2003 [23], B. Dutertre *et al.* 2004 [24], D. Huang *et al.* 2004 [25].
	Reusable pair-wise KMs	**L.Eschenauer *et al.* 2002** [18], D. Hwang *et al.* 2004 [26], R. D. Pietro *et al.* 2003 [27], S. A. Camtepe *et al.* 2004 [28].
	Group-wise KMs	**C.Blundo *et al.* 1992** [9], M. Ramkumar *et al.* 2004 [29].
HWSN	Pair-wise KMs	**S. zhu *et al.* 2003** [19], G. Jolly *et al.* 2003 [30]
	Group-wise KMs	**M. Shehab *et al.* 2005** [20], A. Chadha *et al.* 2005 [31] .
	Network-wise KMs	**S. Slijepcevic *et al.* 2002** [21], A. Perrig *et al.* 2002 [32], D. Liu *et al.* 2003 [33], M.Bohge *et al.* 2003 [34]

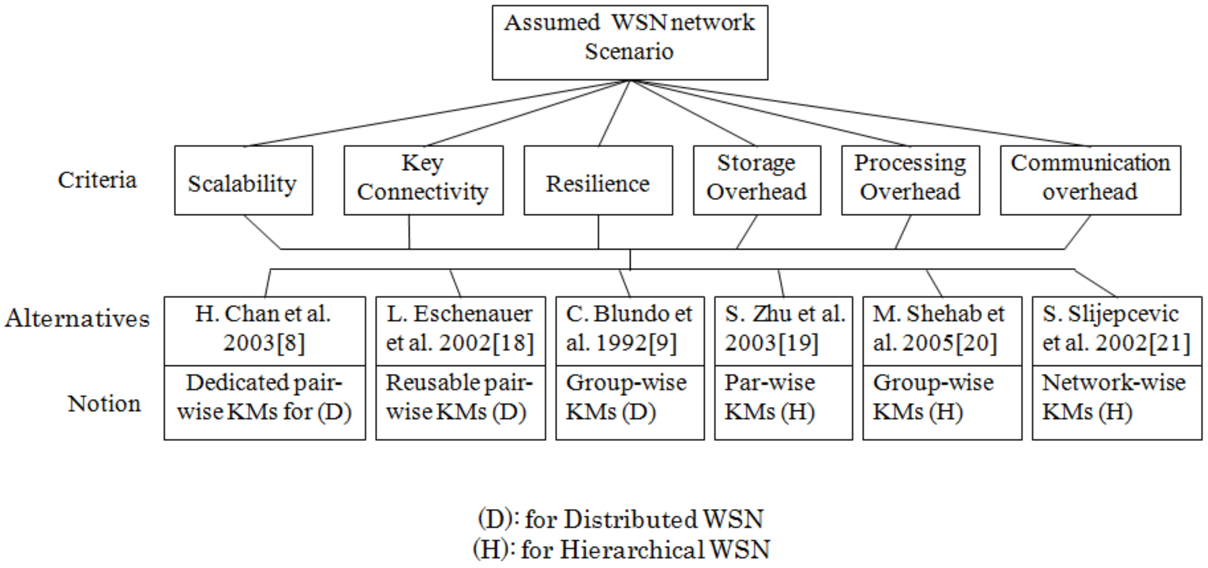


Figure 2. Framework of AHP based method for selecting a key management scheme

scenario. The importance preference of each criterion is the input. Output is the weighted vector of criteria. Second step is establishment of comparative judgments. Likewise, the center of this steps is to construct series of pair-wise comparison matrix B for each criterion. The importance value of each key management scheme is the input. Output is the weighted vectors of schemes. After finishing the first and second steps, the third step is to do consistency check, calculate values of weight coefficient for each scheme and do final decision.

We describe the first step in subsection: Establishment of a structural hierarchy. We describe the second step and the third step in subsection: Establishment of comparative judgments respectively. Specifically in subsection: Establishment of comparative judgments, we present the network scenario and its parameters.

A. Establishment of a structural hierarchy

Two inputs are presented firstly. One is the importance evaluation of each criterion. Five criteria are involved here: scalability (S), key connectivity (K), resilience (R), storage overhead (M) and communication overhead (C). The other is importance evaluation of each scheme.

The importance evaluation of each criterion points out criteria establishing among the elements of the hierarchy by making a series of judgments based on pair wise comparisons of the criteria. For example, when we want to select an optimum key management scheme for army areas, choosers might say they prefer higher security and less normal nodes can be captured. Numerical priorities are derived from the decision makers' input.

In the next step, we present two types of matrix series. One is pairwise comparison matrix A for network scenario which is constructed based on each criterion's importance evaluation. The other one is pairwise comparison matrix B for criteria which is constructed based on each scheme's importance evaluation.

After constructing the two type matrix series, we can obtain two outputs. One is the weighted vector of criteria and the other one is the weighted vector of schemes. In the next section, the consistency check, calculating values of the weight coefficient for each scheme and final decision will be illustrated. In this section, we focus on explaining the matrix construction proceeds.

The formulation of AHP-based model for selecting the best key management scheme in the assumed WSN scenario is presented as shown in Algorithm 1. Based on the properties and mechanism of AHP, we provide a solution to evaluate the key management schemes in a mathematical analysis method. Our solution can be applied to select an optimum key management scheme

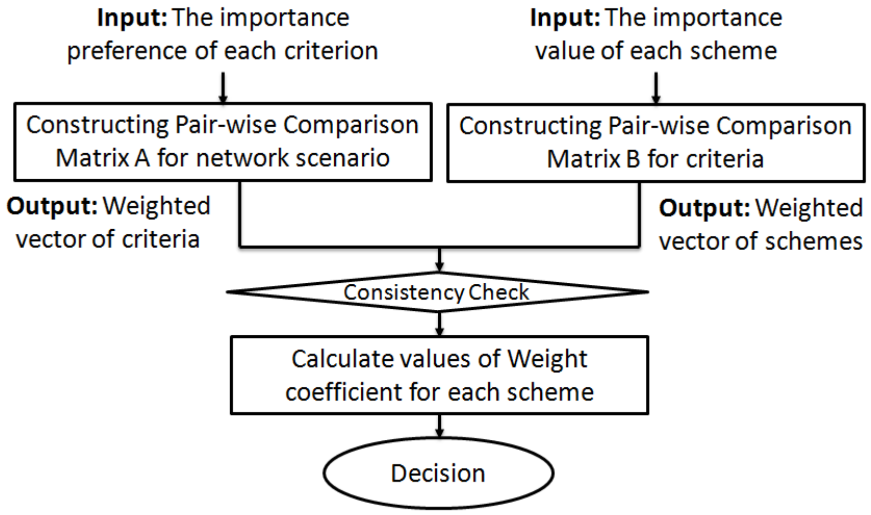

Input: The importance preference of each criterion
Input: The importance value of each scheme
Constructing Pair-wise Comparison Matrix A for network scenario
Constructing Pair-wise Comparison Matrix B for criteria
Output: Weighted vector of criteria
Output: Weighted vector of schemes
Consistency Check
Calculate values of Weight coefficient for each scheme
Decision

Figure 3. The inputs and outputs of our former proposal

within a particular network scenario. Basically, there are two steps for considering decision problems by AHP. Firstly, the two types of matrix series have been constructed based on the inputs.

1) One is pairwise comparison matrix $A = (a_{ij})_{6\times 6}$ for network scenario which is constructed based on each criterion's importance evaluation.
   In judgment matrix, we set $a_{ii} = 1$. Furthermore, if we set $a_{ij} = \eta$, then we set $a_{ji} = 1/\eta$.
   Here, $A = (a_{ij})_{6\times 6}$, $a_{ij} = w_i/w_j$, w_i is the relative importance, $a_{ij} > 0$, $a_{ij} = 1/a_{ji}$, $a_{ii} = 1$, $i, j = 1, 2, \ldots, n$.
   The other one is pair-wise comparison matrix $B = (b_{ij})_{5\times 5}$ for the five criteria which are constructed based on each scheme's importance evaluation.
2) After constructing the two types of matrix series, we can obtain two outputs.
   One is the weighted vector of criteria $\overrightarrow{A}$ and the other is the weighted vector of schemes $\overrightarrow{B}$.
3) Then we can calculate the values of weight for each scheme $\overrightarrow{W_\kappa} = \overrightarrow{W_A} \cdot \overrightarrow{W_B}$, $\kappa = 1, \ldots, 6$.
   Finally, We can obtain the output of the decision of which scheme is the best choice $\overrightarrow{W}_{max} = \max(\overrightarrow{W}_\kappa)$.

Algorithm 1 Our proposal

```
Input: importance values of each criterion $A = (a_{ij})_{6\times 6}$, importance values of each scheme $B = (b_{ij})_{5\times 5}$.
Output: the decision of the evaluation for the key management schemes $\overrightarrow{W} = (W_\kappa)_{1\times 6}$, $\kappa = 1, \ldots, 6$.
while Assumed network scenario: $\overrightarrow{A} \& \overrightarrow{B}$ do
    while the importance value of each criterion:$a_{ij}$ do
        Construct the pairwise comparison matrix $A$ ;
        Calculate the weighted vectors of the matrices $\overrightarrow{W_A}$;
    end while
    while the importance values of each key management scheme:$b_{ij}$ do
        Construct the pairwise comparisons matrix $B$;
        Calculate the weighted vectors of the key management scheme $\overrightarrow{W_B}$ ;
    end while
    if $\overrightarrow{W_A} \& \overrightarrow{W_B}$ then
        Calculate the values of weight for each scheme $\overrightarrow{W_\kappa} = \overrightarrow{W_A} \cdot \overrightarrow{W_B}$ ;
    end if
    Output the decision of which scheme is the best choice $\overrightarrow{W}_{max} = \max(\overrightarrow{W}_\kappa)$ ;
end while
```

B. Establishment of comparative judgments

In this subsection, we first describe the network scenario and provide the matrix A, which is pairwise importance comparison of each criterion. Then both the parameters of the assumed network scenario and the series of matrix B are presented. The series of matrix B is pairwise importance comparison of each scheme.

We assume there is a scenario of judgment as follows: In [22], the government wants to enforce its homeland security using the WSN to aggregate the information on the borderline. In such a scenario, the perimeter surveillance is one of the most promising WSN applications. WSNs can be easily deployed permanently (e.g., public places) or on-demand (e.g., high risk events) in a very short time, with low costs and with little or no supporting communications infrastructure.

First of all, the sensor nodes must work at a low energy consumption to survive in a long time without energy supply and keep collecting and transmitting the information without breaking down. Under such a circumstance, Communication Overhead (C) becomes the most important criterion which should be considered because communication is the most energy-consuming. For instance, Mica2Dot has a 7.3MHz Atmel ATMEGA128L low-power micro-controller which runs TinyOS, 128KB of read-only program memory, 4KB of RAM, a 433MHz Chipcon CC1000 radio which provides a 19.2 Kbps data rate with an approximate indoor range of 100 meters [3].

Secondly, an attacker may capture part of sensor nodes or introduce its own malicious nodes inside the network, hence security must be taken into account in WSN design. Keys stored on a sensor node or exchanged over radio links should not reveal any information about the security of any links. Considering the Resilience (R), higher resilience means lower number of compromised links. Therefore, the resilience is an important issue in such a hostile environment.

For instance, as well as each pair-wise key coming from one node, node S_i ($1 \leq i \leq N$) stores the corresponding pair-wise keys for other N-1 sensor nodes in the WSN. Thus, each sensor S_i stores a key-chain $KC_i = \{K_{i,j} | i \neq j, 1 \leq j \leq N\}$ of size $|KC_i| = N - 1$ out of $N(N-1)/2$ keys. However, not all $N - 1$ keys are required to be stored in nodes' key-chain and not all $N - 1$ keys are required to have a connected key graph. Thus, R is less important to C [3].)

Thirdly, Storage Overhead (M) is important because storage is necessary in order to support the store-and-forward operating principle. The data should be stored when several nodes run out of battery. And as a result, the network becomes partitioned. In this case, it is important not to lose the potentially measured data over a long period of time.

Finally, the size of the WSN is pre-determined in most of homeland security application so that the key connectivity (K) and scalability (S) is not an important issue for the government's judgments. And the location of nodes is usually fixed, which means each network scenario is assigned a scalability rank. Hence, key connectivity is more importance than scalability. Moreover, without key connectivity, the scalability will be affected due to the low communication efficiency [3].

As above, we conclude our importance is set in the increasing order of: (low) Scalability < Key connectivity < Storage overhead < Resilience < Communication overhead (high). From another aspect, we know that there are five levels in AHP. Their scale are claimed as: equal importance, weakly more important, strongly more important, very strongly more important and absolutely more important. They are described as follows:

- **Level 1** Two criteria are of **equal importance**. Storage Overhead and Resilience are of equal importance.
- **Level 2** This level which is between Level 1 and Level 3 means an intermediates value. Communication Overhead is a little more important than Storage Overhead. Resilience VS Key Connectivity: Because Storage Overhead has the same importance as resilience, storage overhead is a little more important than Key Connectivity.

TABLE III.
PAIRWISE COMPARISON JUDGMENT MATRIX OF THE FIVE CRITERIA

	S	K	R	M	C
S	1	1/3	1/7	1/5	1/9
K	3	1	1/2	1/2	1/3
R	7	2	1	1	1
M	5	2	1	1	1/2
C	9	3	1	2	1

- **Level 3** Metric i is **weakly more important** than metric j. Key Connectivity is weakly more important than Scalability. Communication Overhead is weakly more important than Key Connectivity.
- **Level 5** Metric i is **strongly more important** than metric j. Storage Overhead is strongly more important than Scalability.
- **Level 7** Metric i is **very strongly more important** than metric j. Resilience is very strongly more important than Scalability.
- **Level 9** Metric i is **absolutely more important** than metric j. Communication Overhead is absolutely more important than Scalability.

As the same as original pair-wise comparison values in AHP, the value between each two of the five levels means that it has an intermediates value. It is used to represent compromise between the levels list above. Reciprocal is suitable here for inverse comparison. The decision makers give their decision from quality aspect. They do not need the exact input. The decision makers need to give the relative importance of each two performances. Based on these relative importance items, we get the compared matrix.

Taking previous expert judgement of the five criteria into AHP-based method, we can obtain the specific levels of the above five criteria. Scalability (1) < Key connectivity (3) < Storage overhead (5) < Resilience (7) < Communication overhead (9). The most important thing in AHP is how to select items and how to give the framework of decision. First, we describe the relative importance of each of the five criteria. Then based on these the relative importance, a five level hierarchy decision process is described in Table III. As shown in Table III, we present the numerical based on the AHP pair-wise comparison table [4]. The criteria listed on the left are compared with each criterion listed on top one by one. Due to the priority of the existing alternative key management schemes, it relates to the assumed network scenario with definite comparison judgment matrix.

In judgment matrix, a_{ii} is set to equal 1. Furthermore, we set a_{ij} to equal η, then a_{ji} equals $1/\eta$, where $A = (a_{ij})_{6\times6}$, $a_{ij} = w_i/w_j$, $a_{ij} > 0$, $a_{ij} = 1/a_{ji}$, $a_{ii} = 1$, $i, j = 1, 2, \ldots n$. Next, we calculate the consistency ratio $CR = 0.0088 < 0.1$, which means that the pair-wise comparison judgment matrix of five criteria keeps consistency well [17].

From Table III, we normalize to obtain the relative weight or eigenvector of each rating scale. Using expert

TABLE IV.
MATRIX B_S: PAIR-WISE COMPARISON MATRIX OF THESE KEY MANAGEMENT SCHEMES' SCALABILITY METRIC

	H.Chan *et al.* [8]	L.Eschenauer *et al.* [18]	C.Blundo *et al.* [9]	S. zhu *et al.* [19]	M. Shehab *et al.* [20]	Slijepcevic *et al.* [21]
[8]	1	1	2	2	2	2
[18]	1	1	2	2	2	2
[9]	1/2	1/2	1	1	1	1
[19]	1/2	1/2	1	1	1	1
[20]	1/2	1/2	1	1	1	1
[21]	1/2	1/2	1	1	1	1

TABLE V.
RELATIVE WEIGHTS OF EACH METRIC FOR PAIR-WISE COMPARISON MATRIX OF THESE SCHEMES

	$B_S Avg.$	$B_K Avg.$	$B_R Avg.$	$B_M Avg.$	$B_C Avg.$
H.Chan *et al.* [8]	0.25	0.25	0.049	0.273	0.180
L.Eschenauer *et al.* [18]	0.25	0.25	0.049	0.273	0.450
C.Blundo *et al.* [9]	0.125	0.125	0.095	0.265	0.192
S. zhu *et al.* [19]	0.125	0.125	0.269	0.041	0.069
M. Shehab *et al.* [20]	0.125	0.125	0.269	0.038	0.069
Slijepcevic *et al.* [21]	0.125	0.125	0.269	0.110	0.039
	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$

Choice software, the relative weights of Scalability (S), Key connectivity (K), Resilience (R), Storage Overhead (M) and Communication Overhead (C) are calculated, which are equal to 0.03, 0.119, 0.269, 0.218 and 0.352 respectively.

IV. CASE STUDY

In this section, six key management schemes based on five criteria are compared. Because the importance scale of the five criteria can be various values, two case studies for further comparison are presented in this section.

We select six typical schemes: H.Chan *et al.* 2003 [8], L.Eschenauer *et al.* 2002 [18], C.Blundo *et al.* 1992 [9], S. zhu *et al.* 2003 [19], M. Shehab *et al.* 2005 [20] and S. Slijepcevic *et al.* 2002 [21] for the schemes comparison in next step. The six key management schemes are selected because each of them belongs to one kind of classification of KMs for WSN. Each of the six key management schemes has its own advantages and disadvantages. Both of their advantages and disadvantages are classified from the five criteria.

In our case study, we prove our method from three steps. The first step we assume one criteria preference and one network parameters, then we show our method step by step in details. This proceeding is presented in both subsection: Case Study 1 and subsection: Result of Case Study 1. The second step, we alter to another criteria preference as the alternation requirement from network scenario and calculate the result for analysis of the final values. We can see what is the alternation as the change of criteria preference. For the third step, we change the network size for further more explanation. This proceeding is presented in both subsection Case Study 2 and subsection: Result of Case Study 2. Finally, we compare the result of both case study 1 and case study 2 in subsection: Comparison between Case Study 1 and Case Study 2.

A. Case Study 1

We assume the network and key's parameters as follows: In each 1 km^2 square unit area, for providing available WSN model, the relationship between communication distance l and limiter power overhead E of each sensor node is $E \propto l^n$ $(2 < n < 4)$, n is effected by external influence and n is usually set to 3 for calculation. Accordingly the communication radius of each node is set to 100 m [36]. Thus, the available nodes number is set to $N = 100$ for each 1 km^2 square unit area. Let p denote the probability of sharing a key in pair-wise keys between any two nodes. Let $d = p \times (N - 1)$ be the expected degree of a node.

L.Eschenauer *et al.* 2002 [18] has shown that: A key pool which has 10,000 keys means the key pool size KP equals 10,000. When $KP = 10,000$, only need store 75 keys in a node's memory to ensure that the probability p can satisfy $p = 0.5$. p means the probability that the nodes share a key in their key rings. If the pool size becomes ten times larger, for example, $KP = 100,000$, while the number of keys required for keeping the same probability $p = 0.5$ is only 250. The basic scheme is a key management technique which has the characters: scalable, flexible and be suitable for large networks. Thus, the key pool size $KP = 10,000$ keys, the keys number 75 keys and the probability $p = 0.5$ can be taken as an example in our case study 1.

In the key set up phase, each node ID is matched with N_p. N_p is randomly selected node identities with probability $p = 0.5$. $p = 0.5$ is always used for a qualified value for evaluation [6]. Thus we can get $N_p = 50$. At the beginning of the AHP evaluation, the matrix key distribution scheme generates a $m \times m$ key matrix for a WSN with size $N = m^2$. During key pre-distribution phase, each node is assigned a position (i, j), receives both the keys in i-th column and the keys in j-th row of the key matrix as the key-chain, which totally has $2m$ keys. Here m denotes the number of keys in master key list of a node and $m = \sqrt{N} = 10$. t is the size of group in

TABLE VI.
QUOTED SYMBOLS IN CASE STUDY 1

Quoted Symbols	Symbol's Name
E	Power overhead
l	Communication distance
n	l's exponent
N	Nodes number
p	Probability of two nodes share a key
d	Expected degree of a node
S	Key pool size
m	Side of Key matrix
t	Size of sub-group network
λ	Size of adversary coalitions
N_p	The number of each nodes stores a random set which dedicated pair-wise keys to achieve probability p that two nodes share a key

the assumed network scenario. If we assumes one group here, t is set to 100. λ is the size of adversary coalitions and equals 50.

All the quoted symbols in this section are concluded in Table VI. At the same time, the six key management schemes we have marked with black front in Table II.

For instance, the six key management schemes informed in our paper are listed in Table II. If we take their scalability into consideration, the basic numerical value of each key management scheme's scalability can be obtained from their original paper: $Value(S)$ [8] = 2, $Value(S)$ [18] = 2, $Value(S)$ [9] = 1, $Value(S)$ [19] = 1, $Value(S)$ [20] = 1, $Value(S)$ [21] = 1. Thus, we can obtain the pair-wise comparison matrix of these key management schemes' scalability value and we show the matrix (B_S) as in the form of Table IV.

Accordingly, this matrix-Table IV is normalized to obtain the relative weight of eigenvector via the rating scale. As a consequence, the relative weights of key management scheme in H.Chan *et al.* 2003 [8], L.Eschenauer *et al.* 2002 [18], C.Blundo *et al.* 1992 [9], S. zhu *et al.* 2003 [19], M. Shehab *et al.* 2005 [20] and S. Slijepcevic *et al.* 2002 [21] are calculated and equal to 0.25, 0.25, 0.125, 0.125, 0.125 and 0.125, respectively. On the other hand, the consistency index CI is calculated and is equal to 0, which means that the matrix-Table IV passes consistency check. Namely, the matrix-Table IV keeps consistency well and the expert preferences are reasonable.

As the similar processing of scalability matrix B_S calculation, we can go through a similar process on the other four criteria: key connectivity, resilience, storage overhead and communication overhead. Finally, the relative values of all the five criteria are calculated and summarized in Table V.

Then, as we obtain both the judgment matrix (Matrix A) and the matrixes for key management schemes with respect to each criteria's comparison (Matrix B_S, B_K, B_R, B_M and B_C), we can calculate the final vectors of each key management scheme for the assumed WSN scenario. Recalling our overall weights, we can get a final value for each key management scheme now. The value for H.Chan *et al.* [8] is 0.175555. The solution of equations is as follows:

$$\overrightarrow{A}\cdot\overrightarrow{W_A}=\lambda\overrightarrow{W_A}$$
$$\overrightarrow{B}\cdot\overrightarrow{W_B}=\lambda\overrightarrow{W_B}$$
$$\overrightarrow{W}_{[8]}=\overrightarrow{W_A}\cdot\overrightarrow{W_B}$$

Thus, the value of H.Chan *et al.* [8] ($\overrightarrow{W}_{[8]}$)is calculated out.

- With H.Chan *et al.* [8], $\overrightarrow{W}_{[8]} = 0.039 \times 0.25 + 0.119 \times 0.25 + 0.269 \times 0.049 + 0.218 \times 0.273 + 0.352 \times 0.180 = 0.175555$

Similarly, the value of the other five key management schemes are calculated in turns and concluded as follows:

- With L. Eschenauer *et al.* [18], $\overrightarrow{W}_{[18]} = 0.039 \times 0.25+0.119\times0.25+0.269\times0.049+0.218\times0.273+ 0.352 \times 0.450 = 0.270595$
- With C. Blundo *et al.* [9], $\overrightarrow{W}_{[9]} = 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.095 + 0.218 \times 0.265 + 0.352 \times 0.192 = 0.170659$
- With S. Zhu *et al.* [19], $\overrightarrow{W}_{[19]} = 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.269 + 0.218 \times 0.041 + 0.352 \times 0.069 = 0.125337$
- With M. Shehab *et al.* [20], $\overrightarrow{W}_{[20]} = 0.039\times0.125+ 0.119 \times 0.125 + 0.269 \times 0.269 + 0.218 \times 0.038 + 0.352 \times 0.069 = 0.124683$
- With S. Slijepcevic *et al.* [21], $\overrightarrow{W}_{[21]} = 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.269 + 0.218 \times 0.110 + 0.352 \times 0.039 = 0.129819$

B. Result of Case Study 1

Comparing the final value of the six schemes, we obtain the order of the six schemes' values. Their values decrease in the following order: L. Eschenauer *et al.* [18], H.Chan *et al.* [8], C. Blundo *et al.* [9], S. Slijepcevic *et al.* [21], S. Zhu *et al.* [19] and M. Shehab *et al.* [20]. Among the value of the six schemes, L. Eschenauer *et al.* scheme [18] has the biggest value and M. Shehab *et al.* scheme [20] has the least one.

The scheme with the biggest value means that it is the optimum scheme. The optimum scheme L. Eschenauer *et al.* [18] is superior to the traditional key pre-distribution schemes. Because it presents a new key management scheme for a large scale distribution sensor network. All such schemes must be extremely simple given the sensor-node computation and communication limitations. Their approach is scalable and flexible: trade-offs may occur between sensor-memory cost and connectivity, and design parameters can be adapted to fit the operational requirements of a particular environment.

The scheme with the least value means that it is not a suitable scheme for the assumed WSN scenario. We know that scheme M. Shehab *et al.* [20] is suitable for limited computation and energy capability sensor network. This proposed key generation algorithm is based on low cost hashing functions that enable the efficient key generation. Its key distribution protocol is also energy efficient. Thus, this scheme satisfies with the energy limitation problem

TABLE VIII.
ANOTHER RELATIVE WEIGHTS OF EACH CRITERION FOR PAIR-WISE COMPARISON MATRIX OF THE SIX SCHEMES

	$B_S Avg.$	$B_K Avg.$	$B_R Avg.$	$B_M Avg.$	$B_C Avg.$
H.Chan *et al.* [8]	0.25	0.125	0.049	0.041	0.069
L.Eschenauer *et al.* [18]	0.25	0.25	0.269	0.273	0.450
C.Blundo *et al.* [9]	0.125	0.125	0.095	0.265	0.192
S. zhu *et al.* [19]	0.125	0.25	0.269	0.273	0.180
M. Shehab *et al.* [20]	0.125	0.125	0.269	0.038	0.069
Slijepcevic *et al.* [21]	0.125	0.125	0.049	0.110	0.039
	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$

TABLE VII.
FURTHER ONE MORE CASE ABOUT PAIRWISE COMPARISON JUDGMENT MATRIX OF THE FIVE CRITERIA

	S	K	R	M	C
S	1	1/3	1/7	1/5	1
K	3	1	1/2	1/2	3
R	7	2	1	1	7
M	5	2	1	1	5
C	1	1/3	1/7	1/5	1

of wireless sensor network. The trade-off between energy and security is the biggest problem in wireless sensor network, so it cannot satisfy the requirement in our assumed network scenario.

C. Case Study 2

Both subsection A and subsection B in section 4 are the results of our case study 1. Case study 1 considers the preference setting for the evaluation criteria and the assumed WSN network scenario. For more clear explanation, further work with more discussion can be done well from two aspects: the first one is to change the criteria preferences even to do all the permutation of the criteria. Under other criteria preferences, we can see what is changed from the final optimum scheme result. Under the all permutation of criteria, we can obtain the different result of optimum scheme according to different preference.

The other one is to change the parameters of WSN network scenario, such as the network size and the key pool size. Accordingly, we can do analysis on the final scores of these key management schemes in wireless sensor network which can help us come to be familiar with these schemes and make the decision for selecting optimum scheme easily.

First, we analyze one more case on the pairwise comparison judgement matrix of the criteria. If the WSN is for civil use which can provide enough energy and can keep the advantage of WSN, we can obtain the preference of criteria as follows: (low) Scalability (1) = Communication overhead (1) < Key connectivity (3) < Storage overhead (5) < Resilience (7) (high). The judgement matrix of criteria preference is shown in Table VII accordingly.

Keeping the same network parameters of WSN network scenario, we can calculate the final value under the one more case study which is according to one more criteria preference. The final values of the six typical schemes are sorted in decreasing order: L. Eschenauer *et al.* [18] $= 0.1935$, H.Chan *et al.* [8] $= 0.17757$, S. Slijepcevic *et al.* [21] $= 0.1679$, C. Blundo *et al.* [9] $= 0.1636$, S. Zhu *et al.* [19] $= 0.1468$ and M. Shehab *et al.* [20] $= 0.1459$.

Both the best scheme and the worst scheme in this result is the same as case study 1. However the order of the six values has been changed. Scheme C. Blundo et al. [9] and scheme S. Zhu et al. [19] change their order to each other. Thus, we can see the affect from the changing of the criteria preference .

Then, we analyze the affection from WSN network parameters setting. Previous network size $N = 100$. If more nodes have been added in and we also want to keep the same probability $p = 0.5$ for the probability of that two nodes share a key, it is an interesting problem on the optimum scheme alteration for the current network scenario. As shown in L. Eschenauer *et al.* [18], it is worth mentioning that only $k = 75$ keys are needed for probability $p = 0.5$ that any two nodes can share a key in their key ring as $KP = 10,000$. Thus, we assume the new network scenario as follows: Network size $N = 1000$. As we know, there is the expected degree of a node $d = p \times (N-1) = 500$. Accordingly we get the successfully connected nodes number $Np = 500$, the size of adversary coalitions $\lambda = 50$, $t = 200$ which means five grids here. In matrix key distribution scheme, $m = 10$ as $m = \sqrt{N}$. We let all the schemes keep the same key pool $KP = 10,000$ as given in scheme L. Eschenauer *et al.* [18]. Then, the alternation has been showed in Table VIII.

D. Result of Case Study 2

Under the criteria preference setting in Table III and the WSN network parameters setting in Table VIII, we apply our AHP-aid method to calculate the combining of both Table III and Table VIII. We can calculate the final value and come to the conclusion that scheme S. Zhu *et al.* [19] takes advantage of the other schemes. Here the optimum scheme is S. zhu *et al.* [19] which is different from previous optimum scheme L. Eschenauer *et al.* [18]. This is the effect of network nodes number alternation from $N = 100$ to $N = 1000$. Scheme S. zhu *et al.* [19] is an efficient security key management scheme for larger scale sensor network. It can reduce the communication overhead between each communication unit. Thus, the more larger network size the more obvious the advantages are. This can be shown to be the same as the original

TABLE IX.
PARAMETERS COMPARISON BETWEEN CASE STUDY 1 AND CASE STUDY 2

	n	N	p	d	KP	k	m	t	λ	Np	Optimum scheme
Case Study 1	3	100	0.5	50	10,000	75	10	100	50	50	L. Eschenauer *et al.* [18]
Case Study 2	3	1000	0.5	500	100,000	250	100	200	50	500	S. Zhu *et al.* [19]

paper assumption [19]. It consistent to our new network requirement.

E. Comparison between Case Study 1 and Case Study 2

In the above four subsections, we describe two groups network scenario. We called them Network scenario $Net1$ and Network scenario $Net2$, respectively. Firstly, we conclude both of the network scenario. Then Table IX is used to show clearly the parameters' value of the two network scenario. Lastly, we explain the different parameters' value between the two network scenarios.

Network Scenario $Net1$**:** Recall from Section IV.A, the parameters of network scenario and key management scheme have been presented. The parameters can be concluded in the following:

$p = 0.5$, $N = 100$, $Np = 50$, $d = 50$, $KP = 10,000$, $k = 75$, $m = 10$, $\lambda = 50$, $t = 100$.

Network Scenario $Net2$**:** L. Eschenauer *et al.* [18] scheme infers that if the pool size is ten times larger, for example, $KP = 100,000$, then the number of keys required is still only 250 for keeping the value $p = 0.5$ which is the same as in the first group network scenario. The basic scheme is a key management technique that is scalable, flexible and can be used for large networks. Then we can present another WSN scenario: we enlarge the key pool size and the network nodes number.

We refer to the key pool size from scheme L. Eschenauer *et al.* [18]: $KP = 100,000$ keys, only $k = 250$ keys is needed for probability $p = 0.5$ such that any two nodes can share a key in their key ring. The available nodes number is enlarged to $N = 1,000$. Because of the same probability $p = 0.5$ and assumed $N = 1,000$, we can obtain that $Np = 500$, $d = 500$, $t = 200$ (five grids for the hierarchical structure), $m = 100$.

Table IX concludes the parameters used in both case study 1 and case study 2. The value of n, p and λ are the same in both case studies as shown in Table IX. Keeping the value of p as the same as precondition, the other parameters in case study 2 change to different values [18]. In both case studies, the basic changed values are the network size N and the key pool size KP. The key pool size KP is changed from 10,000 to 100,000 and the nodes number N change from 100 to 1000. k is changed as KP changed. Np, d and t are changed. Because the changing of the size of network grids t causes the number of network grids to change, m is changed as the network grids is changed.

All the changed values above cause the two case studies to perform different final decision. Case study 1 selects L. Eschenauer *et al.* [18] scheme as the optimum scheme. Meanwhile, case study 2 selects S. Zhu *et al.* [19] scheme as the optimum scheme. From the two case studies, the relationship between our method decision and the changing of the parameters are drawn. Obviously, the quantitative decision from our method brings into correspondence with the original case situations.

V. CONCLUSION

From the analysis, we can see all the key management schemes have their own shortcomings. For this reason, it is a very critical issue to select trustworthy and suitable key management scheme according to assumed scenario requests. Such evaluation analysis can help to provide some valuable information for designing the key management in WSN.

In this paper, we present a quantitative evaluation system for key management scheme which is based on the six aspects: scalability, key connectivity, resilience, storage overhead, processing overhead and communication overhead. We analyze it and show that this system can be used to select suitable key management scheme under assumed wireless sensor network scenario requirements. Furthermore, we show six typical key management schemes from the six classified aspects. Under assumed network scenarios, we can obtain the value order of the six schemes. Importantly, we obtain the best scheme and the worst one via their final calculated values.

Formalized decision should be made where there are a limited number of schemes choices. However each scheme has a number of attributes and it is difficult to formalize some of those attributes. Obviously, AHP-aided method can prevent subjective judgment errors and increase the likelihood that the results are reliable. AHP-aided method provides useful insight into the trade-offs embedded in a decision making problem.

ACKNOWLEDGMENT

The authors would like to thank lab colleagues for carefully reading the paper and providing detailed suggestions on paper structure and comments on the English writing. Also many thanks to the anonymous reviewers in the JNW editorial committee for their insightful comments on this work.

REFERENCES

[1] J. Lopez, J. Y. Zhou, Overview of wireless sensor network security, *Wireless Sensor Network Security, (J. Lopez and J. Y. Zhou Eds)*, IOS Press, 2008.

[2] Y. Jeong, S. Lee, Hybrid Key Establishment Protocol Based on ECC for Wireless Sensor Network, In proceeding of *the 4th international conference on Ubiquitous Intelligence and Computing*, Volume 4611, pages 1233-1242, Hong Kong, China, July, 2007.

[3] S. A. Camtepe, B. Yener, Key management in wireless sensor network, *Wireless Sensor Network Security, (J. Lopez and J. Y. Zhou Eds)*, IOS Press, 2008.

[4] T. L. Saaty, *The Analytic Hierarchy Process*, McGraw-Hill, New York, 1980.

[5] J. Hwang, I. Syamsuddin, Information Security Policy Decision Making: An Analytic Hierarchy Process Approach, In proceeding of *2009 Third Asia International Conference on Modelling and Simulation*, pages 158-163, May, 2009

[6] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, M. Galloway, A survey of key management schemes in wireless sensor networks, *Computer Communications, special issue on security on wireless ad hoc and sensor network*, Volumn 30, pages 2314-2341, September, 2007.

[7] C. J. Jia, Research on security of wireless sensor network, *PhD thesis, ZheJiang University*, July, 2008.

[8] H.Chan, A. Perrig, D. Song, Random key pre-distribution schemes for sensor networks, In proceeding of *IEEE Symposium on Security and Privacy*, pages 197-213, May, 2003.

[9] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, Perfectly-secure key distribution for dynamic conferences, In proceeding of *Advances in cryptology (CRYPTO 92)*, pages 471-486, August, 1992.

[10] D. Chakrabarti, S. Maitra, B. Roy, A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design, In *ISC 2005 Proceedings, Lecture notes in computer science*, ISSN 0302-9743, Volumn 3650. Springer, pages 89-103, 2005.

[11] T. Ito, H. Ohta, N. Matsuda, T. Yoneda, A key predistribution scheme for secure sensor network using probability density function of node deployment, In proceedings of *the 3rd ACM workshop on Security of ad hoc and sensor networks*, pages 69-75, November, 2005.

[12] L. Gong, D. J. Wheeler, A matrix key distribution schemes, In *Journal of Cryptology*, Volumn 2-1. pages 51-59, 1990.

[13] B. Dutertre, S. Cheung, J. Levy, Lightweight key management in wireless sensor networks by leveraging initial trust, *Technical Report SRI-SDL-04-02, System Design laboratory, SRI International*, April, 2004.

[14] C. Fei. Pair-wise Key Management in Wireless Sensor Network, In *Journal of Computer Simulation*, Volumn 22-5, 2005.

[15] H. Soussi, M. Hussain, H. Afifi, D. Seret. IKEv1 and IKEv2: A Quantitative Analyses, In proceeding of *International Conference on Information Security(ICIS WEC'05)*, Istanbul, Turquie, 24-26 June, 2005

[16] E. H. Forman. Decision by Objective, *http://mdm.gwu.edu/Forman/DBO.pdf.*

[17] AHP (Analytic Hierarchy Process) Calculation software by CGI, *http://www.isc.senshu-u.ac.jp/ thc0456/EAHP/AHPweb.html.*

[18] L. Eschenauer, V. D. Gligor, A key-management scheme for distributed sensor networks, In proceeding of *ACM Conference of Computer and Communication Security*, pages 41-47, November, 2002.

[19] S. Zhu, S. Setia, S. Jajodia, Leap:Efficient security mechanisms for large-scale distirbuted sensor networks, In proceeding of *ACM Conference of Computer and Communication Security*, pages 62-72, October, 2003.

[20] M.Shehab, E.Bertino, A.Ghafoor, Efficient hierarchical key generation and key diffusion for distribution for distributed sensor networks, In proceeding of *IEEE International Conference of Sensor and Ad Hoc Communication and Network*, pages 76-84, September, 2005.

[21] S.Slijepcevic, M.Potkonjak, V.Tsiatsis, S.Zimbeck, M.B.Srivastava, On communication security in wireless ad-hoc sensor network, In proceeding of *IEEE WETICE*, pages 139-144, November, 2002.

[22] A. Casaca, D. Westhoff, Scenario Definition and Initial Threat Analysis, In *report of UbiSec and Sens*, Deliverable D0.1, June, 2006

[23] D.Liu, P.Ning, Location-based pairwise key establishments for static sensor networks, In proceeding of *2003 ACM Workshop on Security in Ad Hoc and Sensor Networks (SASN'03)*, pages 72-82, October, 2003

[24] B.Dutertre, S.Cheung, J.Levy, Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust, In *Technical Report SRI-SDL-04-02, System Design Laboratory, SRI International*, April, 2004.

[25] D. Huang, M. Mehta, D. Medhi, L. Harn, Location-aware key management scheme for wireless sensor networks, In proceeding of *ACM Workshop on Security of Ad Hoc and Sensor Network*, pages 29-42, October, 2004

[26] D. Hwang, B. Lai, I. Verbauwhede, Energy-memory-security tradoffs in distributed sensor networks, In proceeding of *ADHOC-NOW*, LNCS, pages 70-81, July, 2004

[27] R. D. Pietro, L. V. Mancini, A. Mei, Random key assignment for secure wireless sensor networks, In proceeding of *ACM workshop on Security of ad hoc and sensor networks*, October, 2003.

[28] S. A. Camtepe, B. Yener, Combinatorial design of key distribution mechanisms for wireless sensor networks, In *9th European Symposium on Research Computer Security*, pages 293-308, September, 2004

[29] M. Ramkumar, N. Memon, An efficient random key predistribution scheme, In proceeding of *Global Telecommunications Conference (GLOBECOM '04)*, 29 Nov.-3 Dec. 2004, 2004.

[30] G. Jolly, M. C. Kuscu, P. Kokate, M. Younis, A low-energy key management protocol for wireless sensor networks, In proceeding of *Eighth IEEE International Symposium on Computers and Communication*, pages 335-340, June 30-July 3, 2003

[31] A. Chadha, Y. Liu, S. K. Das, Group key distribution via local collaboration in wireless sensor networks, In proceeding of *IEEE International Conference of Sensor and Ad Hoc Communication Network*, pages 46-54, February, 2006

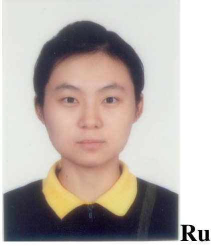
[32] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, Spins: Security protocols for sensor networks, In *Wireless Networks Journal*, Volumn 8-5, 2002

[33] D. Liu, P. Ning, Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks, In *Network and Distributed System Security Symposium*, February, 2003

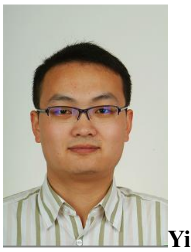
[34] M. Bohge, W. Trappe, An authentication framework for hierarchical ad hoc sensor networks, In *ACM WiSe*, pages 79-87, September, 2003

[35] M. Gabriela, C. Torres, Enegry Consumption in wireless sensor network using GSP, *Thesis for master degree, University of Pittsburgh*, 2006

[36] G. B. Zhou, Z. C. Zhu, G. Z. Chen and N. N. Hu, Energy-Efficient Chain-Type Wireless Sensor Network for Gas Monitoring, In proceeding of *The Second International Conference on Information and Computing Science*, pages 125-128, May, 2009



Ruan Na was born in AnQing, AnHui, China on 1986. She is currently a Ph.D. candidate at Kyushu University, Japan. She received her MS and BS degrees in communication from China University of Mining and Technology, China, in 2010 and 2007, respectively. Her research interests include security, wireless sensor network and communication systems.



Yizhi Ren received the B.S. degree in computer science from Anhui Normal University in 2004, and the M.S. degree and doctorate in computer software and theory from School of Software, Dalian University of Technology in 2006 and 2010, respectively. From 2008 to 2010, he was as a Joint Training PhD student in Kyushu University in Japan, supported by China Government Scholarship. Now, he worked for Software Engineering School of Hangzhou Dianzi University as an assistant professor. His main research interests include network security, social computing.

Yoshiaki Hori received B.E., M.E, and D.E. degrees on Computer Engineering from Kyushu Institute of Technology, Iizuka, Japan in 1992, 1994, and 2002 respectively. From 1994 to 2003, he was Research Associate at the Common Technical Courses, Kyushu Institute of Design. From 2003 to 2004, he was Research Associate at the Department of Art and Information Design, Kyushu University. From 2004, he was Associate Professor at the Department of Computer Science and Communication Engineering, Kyushu University. Since 2009, he has been Associate Professor of Department of Informatics, Kyushu University. His research interests include network security, network architecture, and performance evaluation of network protocols on various networks. He is a member of IEEE, ACM, and IPSJ.

Kouichi Sakurai received the B.S. degree in mathematics from the Faculty of Science, Kyushu University and the M.S. degree in applied science from the Faculty of Engineering, Kyushu University in 1986 and 1988 respectively. He had been engaged in the research and development on cryptography and information security at the Computer and Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received D.E. degree from the Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for the Department of Computer Science of Kyushu University as Associate Professor, and now he is Full Professor from 2002. His current research interests are in cryptography and information security. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM and the International Association for Cryptology Research.