A generic evaluation method for key management schemes in wireless sensor network

Conference Paper · January 2011

DOI: 10.1145/1968613.1968680 · Source: DBLP

4 authors, including:

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

SEE PROFILE

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

SEE PROFILE

A Generic Evaluation Method for Key Management Schemes in Wireless Sensor Network

Ruan Na
Department of Informatics
Kyushu University
Japan
ruannana@gmail.com

Yizhi Ren
Department of Informatics
Kyushu University
Japan
renyizhi@gmail.com

Yoshiaki Hori
Department of Informatics
Kyushu University
Japan
hori@inf.kyushu-u.ac.jp

Kouichi Sakurai
Department of Informatics
Kyushu University
Japan
sakurai@csce.kyushu-u.ac.jp

ABSTRACT

Wireless sensor networks (WSN) have been widely used in various applications. Since their sensor nodes are resource-constrained, key management is one of the most challenging issues in design of WSN. Currently, various efficient lightweight key management schemes 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.* Our method is able help choosing a suitable scheme for given requirements.

Categories and Subject Descriptors

C.2 [**Computer Systems Organization**]: Computer Communication Networks; H.4.3 [**Information Systems**]: Information Systems Applications—*Communications Applications*

General Terms

Design, Security

Keywords

Analytic Hierarchy Process, Key management scheme, Trustworthy decision, Wireless sensor network

1. INTRODUCTION

1.1 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. So, 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 this reason, to design a trustworthy key management scheme is necessary.

In this paper, we design a mechanism which supports the decision-making processes of choosing a trustworthy key management scheme in WSN. We focus on the calculation of how much the existing key management schemes can be trusted to perform a particular task. Here, the trust is based on firm belief in the reliability under a specific wireless sensor network scenario. Just as in a typical wireless network, the key management must satisfy the traditional needs of security, such as availability, integrity, confidentiality, authentication and non-reputation [6]. And as to the specificity of WSN, the key management has other special challenges such as resilience, expansibility and efficiency [7].

1.2 Related Work and Challenging Issues

Recent research works focus on producing an efficient system to evaluate these key management schemes. Also, in recent years, there has been significant progress in key management of WSN, and researchers have proposed a number of key management schemes in WSN which focus on

different security requirements, each scheme with advantages and disadvantages. Now, there are lots of key management schemes in wireless sensor network. They can be divided into 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]. Specific examples include, 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].

To select the most proper key management scheme from large amount of existing schemes is not an easy issue. Some researchers proposed the evaluation index for these schemes using the qualitative analysis [3]. However, such proposals have limited utility unless they take node replication attacks and robustness into consideration. Their proposals fail to address all the criteria that a key management scheme should satisfy. In this paper, we propose a general method to evaluate the key management schemes, which can help us to choose the scheme quantitatively according to different network requirements. The most related work to our research is Hwang et al. [5]. It employs 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 while our proposal uses AHP to select the best key management scheme.

Challenging Issues.

Security of a WSN depends on 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 best in an assumed scenario. All these key management schemes have their own advantages and disadvantages. All of them can suitable for different needs. 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. This reason has pushed us to performance analysis of some parameter of key management schemes [15].

1.3 Our Contribution

In this paper, we propose a generally method to evaluate the key management schemes, which can help us to choose 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, so that we can overcome the difficulty in choosing proper key management scheme for wireless sensor network when there is a multi-criteria decision.

2. Based on our proposal, we provide analysis and simulation of the existing key management schemes. We show that our method can build a visual way to choose a proper scheme and present key management schemes in order of suitability, based on the previously given network requirements. In a word, we provide a feasible quantitative evaluation system to choose the best key management scheme from so many schemes.

3. Finally, we classify several typical key management schemes and make comparison among the trade off in those schemes and show that our method can be helpful in a complicated network environment based on quantitative analysis results.

This work is organized as follows: In Section 2 describes basic definitions and notions used in wireless sensor network for evaluating key management schemes. At the same time, corresponding case study is also proposed. In Section 3 gives out our quantitative system which based on linear algebra and focused on matrix. In Section 4 discusses the system in details via an example. Finally, we draw conclusions in Section 5.

2. PRELIMINARIES

2.1 Brief reviews of AHP

The Analytical Hierarchy Process (AHP) is a decision approach designed to aid in the solution of complex multiple criteria problems in a number of application domains. 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 consider complex and unstructured decisions. The AHP has been used in a large number of applications to provide some 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 weighting of each decision alternative. There are three steps for considering decision problems by AHP: constructing hierarchies; comparative judgment; and synthesis of priorities.

1. **Construction hierarchies:** User of the AHP first decompose 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 its various elements by comparing them to one another two at a time. In making the comparisons, the decision makers can use concrete data about the elements, or they can 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 is presumably missing.

Table 1: 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

The three steps above show a brief reviews of AHP hierarchy at the end of the decision making process.

We also provide some details on synthesis of priorities and the measurement of consistency as follows (n : the order of matrix; RI: the average random index; CR: the consistency ratio; CI: the consistency index; λ: the maximum eigenvalue) [4]:

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 the number of elements at the lower level that it links to. After all criteria are developed and all pair-wise comparisons are obtained, eigenvectors or the relative weights (the degree of relative importance among the elements), global weights, and the maximum eigenvalue (λ_{max}) for each matrix are then calculated using Expert Choice software (Expert Choice, 2000). The software is easy to use and understand, as well as providing visual representations of overall ranking on a computer screen.

The λ_{max} value is an important validating parameter in AHP. It is used as a reference index to screen information by calculating the consistency ratio CR of the estimated vector in order to validate whether the pair-wise comparison matrix provides a completely consistent evaluation. The consistency ratio is calculated as per the following steps:

1) Calculate the eigenvector or the relative weights and λ_{max} for each matrix of order n.

2) Compute the consistency index CI for each matrix of order n by the formula: $CI = \frac{(\lambda_{max}-n)}{(n-1)}$

3) The consistency ratio CR is then calculated using the formula: $CR = \frac{CI}{RI}$

Where RI is a known random consistency index obtained from a large number of simulations runs and varies depending upon the order of matrix. Tables 1 shows the value of the random consistency index (RI) for matrix size of order 1 to 10 obtained by approximating random indices using a sample size of 500 [16].

Because in next section, our proposal based on AHP will use 5-order matrix. It means the order of matrix $n = 5$. Because $n = 5$, the average random index $RI = 1.11$ based on Table 1 search. If the matrix want to past the consistency check, the consistency ratio $CR = \frac{CI}{RI}$ need to be small than 0.1. So here need the consistency index CI satisfy $CI < 0.1 \times 0.11 = 0.111$. Furthermore, as $CI = \frac{\lambda-n}{n-1} = \frac{\lambda-5}{4}$ and $CI < 0.111$, we get the maximum eigenvalue $\lambda < 5.444$, the 5-order matrix will pass the consistency check.

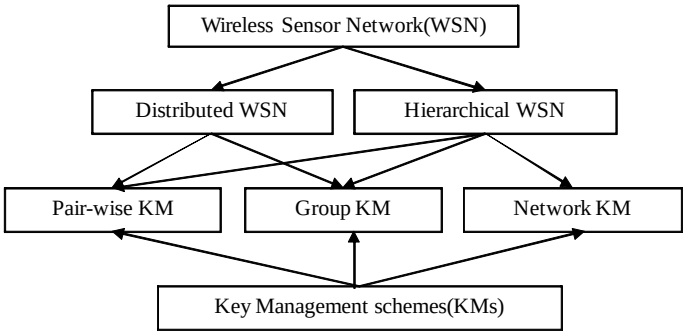

Figure 1: Classification of Key Management schemes

2.2 Classification of key management schemes in WSN

Key management schemes in wireless sensor network (WSN) can be decomposed into several kinds. As Figure 1, in general, WSN are organized in distributed or hierarchical structures. In hierarchical WSN, data flow may be divided 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; network-wise (broadcast) from base stations to sensor nodes. In distributed WSN, data flow is similar to data flow in hierarchical WSN with a difference that network-wise (broadcast) messages can be sent by every sensor nodes.

As given in Table 2 , J. Lopez classified papers on dedicated pair-wise, reusable pair-wise, group-wise and network-wise key management schemes in both Distributed WSN and Hierarchical WSN. Then, as shown in Figure 2 , based on the six criteria which used to evaluate and compare the key management in an assumed network scenario from quantitative calculation, we give out the framework of AHP based method for choosing the most suitable key management scheme among these schemes.

3. OUR PROPOSAL BASED ON AHP

In this paper, we present the formulation of AHP-based model for selecting the best key management scheme in the assumed WSN scenario. Based on the properties and mechanism of AHP, we provide a solution to evaluate the KM schemes in a mathematics analytical way. Our solution can be applied to choose key management scheme within a particular network scenario. Basically, there are two steps for considering decision problems by AHP.

For giving quantitative comparisons and distinct assumptions made by these key management schemes, following criteria can be used to evaluate and compare these key management schemes in WSN.

- 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.

Table 2: Classification of KMs [J. Lopez. 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]

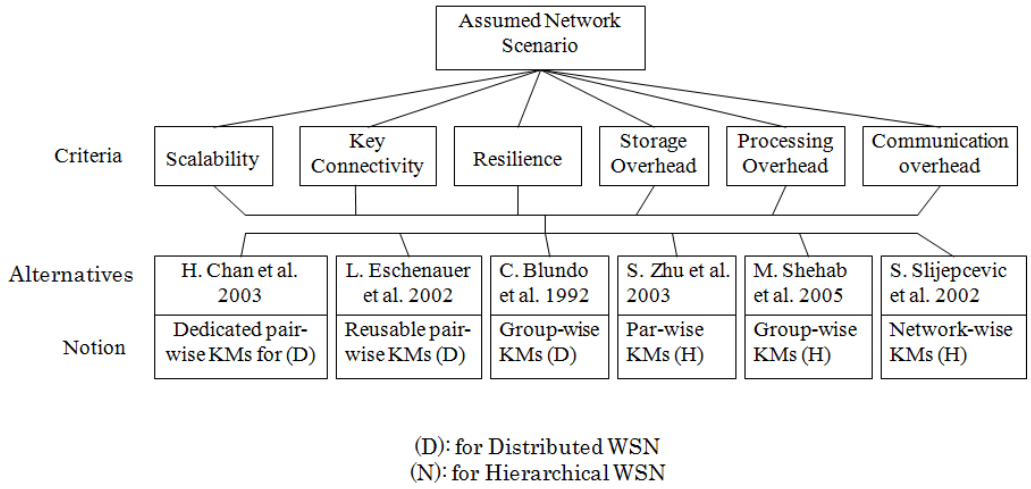

Figure 2: Framework of AHP based method for choosing a key management scheme

- 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.

Communication overhead is the amount and size of messages exchanged between a pair and a group of sensor nodes to generate or find a common secret key. Processing overhead is the amount of processing cycles required by each sensor node to generate or find a common secret key. Consider the power consumption [35], we can see that processing overhead based on the hardware choosing and it is not the main power consumption for WSN. Here we do not take it into evaluation.

In order to determine which key management scheme is the best for the assumed WSN scenario, we propose the method based on AHP. There are two steps in our proposal. First step is establishment of a structural hierarchy. Second step is establishment of comparative judgments. we described the two steps in both section 3.1 and section 3.2. In section 3.2, we present the assumed network scenario which is used for the second step:establishment of comparative judgments.

3.1 Establishment of a structural hierarchy

As in Figure 3, the procedure for using the AHP into evaluation on key management in WSN can be summarized as:

Here we present two inputs: one is importance evaluation of each criterion, the other one is importance evaluation of each scheme. Establish criteria (5 aspects: S-scalability, K-key connectivity, R-resilience, M- storage overhead and C-communication overhead) 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 choose key management scheme for army area, 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 type matrix series. One is pairwise comparison matrix A for network scenario which

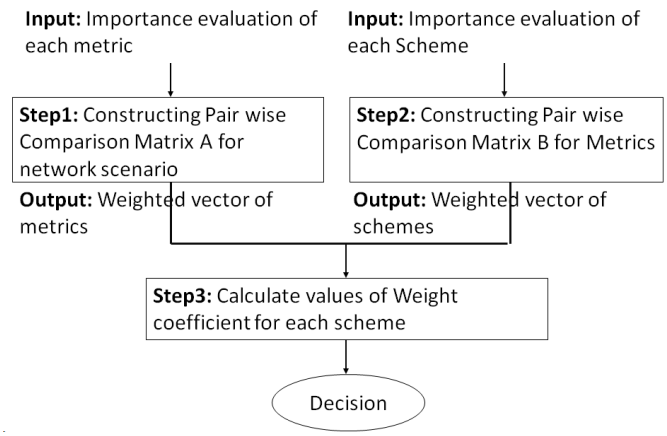

Figure 3: The inputs and outputs of our scheme

is constructed based on each criterion's importance evaluation. The other one is pair wise 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.

Algorithm 1 Our proposal

1: Input: importance values of each metric $A = (a_{ij})_{6\times6}$, importance values of each scheme $B = (b_{mn})_{5\times5}$.
2: Output: the decision of the evaluation for the key management schemes $\overrightarrow{W} = (W_k)_{1\times6}$.
3: **while** Assumed network scenario: $\overrightarrow{A}\&\overrightarrow{B}$ **do**
4: **while** the importance value of each criterion:a_{ij} **do**
5: Construct the pairwise comparison matrix A ;
6: Calculate the weighted vectors of the matrices $\overrightarrow{W_A}$;
7: **end while**
8: **while** the importance values of each key management scheme:b_{mn} **do**
9: Construct the pairwise comparisons matrix B;
10: Calculate the weighted vectors of the key management scheme $\overrightarrow{W_B}$;
11: **end while**
12: **if** $\overrightarrow{W_A}\&\overrightarrow{W_B}$ **then**
13: Calculate the values of weight for each scheme $\overrightarrow{W_k} = \overrightarrow{W_A} \cdot \overrightarrow{W_B}$;
14: **end if**
15: Output the decision of which scheme is the best choice $\overrightarrow{W_{max}} = \max \overrightarrow{W_k}$;
16: **end while**

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

3.2 Establishment of comparative judgments

Here, 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, low costs, 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 metric need to be considered because the communication is the most energy-consuming.

Secondly, an attacker may capture a sensor node or introduce its own malicious nodes inside the network, so security must be taken into account in WSN design. Keys which are stored on a sensor node or exchanged over radio links should not reveal any information about the security of any links. Higher Resilience(R) means lower number of compromised links so the resilience (R)is also an important issue in such a hostile environment. (i.e., Node S_i $(1 \le i \le N)$stores the corresponding pair-wise keys for other N-1 sensor nodes in the WSN with each pair-wise key coming from one node. Thus, each sensor S_i stores a key-chain $KC_i = \{K_{i,j} | i \ne j, 1 \le j \le N\}$ 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 to have a connected key graph. So, R is less important to C [3].)

Thirdly, storage overhead 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 data measured over potentially 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, between key connectivity and scalability, key connectivity is more importance. Moreover, without key connectivity the scalability will be affected due to the low communication efficiency[3].

As above, we can know that, we can get Scalability (1) < Key connectivity (3) < Storage overhead (5) < Resilience (7) < Communication overhead (9). Taking this policy into AHP method, we can get the specific levels about the above metrics.

Level 1 Two metrics are of equal importance. Storage Overhead and Resilience are of equal importance.

Level 2 This level between Level 1 and Level 3 means that it has an intermediates value. Communication Overhead is a little more important than Storage Overhead. Resilience VS Key Connectivity: Because Storage Overhead has the same importance with resilience, storage overhead also is a little importance than Key Connectivity.

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

Table 3: Pairwise comparison judgment matrix for five-point metrics

	S	K	R	M	C
S	1	$\frac{1}{3}$	$\frac{1}{7}$	$\frac{1}{5}$	$\frac{1}{9}$
K	3	1	$\frac{1}{2}$	$\frac{1}{2}$	$\frac{1}{3}$
R	7	2	1	1	1
M	5	2	1	1	$\frac{1}{2}$
C	9	3	1	2	1

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 the five levels means that it has a intermediates value. It is used to represent compromise between the levels list above. Reciprocal is also suitable here for inverse comparison. The decision makers give their decision from quality aspect. They do not need the exactly input. The decision makers need to give the relative importance between each two performances. Based on these relative importance items, we get the compared matrix. The most important thing in AHP is how to choose items and how to give out the decision framework. First, we describe the relative importance of five metrics. Then based on these the relative importance, a five level hierarchy decision process displayed is described as in Table 3.

As shown in Table 3, we present the numerical based on the AHP pair-wise comparison table [4]. The criteria listed on the left are one by one compared with each criterion listed on top. Due to which key management scheme is better than others, it relates to the assumed network scenario with definite comparison judgment matrix. In judgment matrix, we set $a_{ii} = 1$. Furthermore, if we set $a_{ij} = k$, then we set $a_{ji} = \frac{1}{k}$. Here, $A = (a_{ij})_{6\times 6}$, $a_{ij} = \frac{w_i}{w_j}$, $a_{ij} > 0$, $a_{ij} = 1/a_{ij}$, $a_{ii} = 1$, $i, j = 1, 2, \ldots n$

Then, we calculate the consistency ratio $CR = 0.0088 < 0.1$, which means that the pair-wise comparison judgment matrix for five-point metrics keeps consistency well [17].

From matrix of Table 3, we normalize to obtain the relative weight or eigenvector of each rating scale. Using expert 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.

In next step, we compare all the key management schemes based on each criteria.

We choose [8, 18, 9, 19, 20, 21] for the comparison in next step. We choose them because each classification of KMs for WSN has its own advantages which are based on different metrics. We assume the network and key's parameters as follows. The nodes number is $N = 100$ and let p denote the probability of that two nodes share a key in pairwise keys. At key set up phase, each node ID is matched with N_p other randomly selected nodes ID with probability p and where

Table 4: Matrix B_S: Pair-wise comparison matrix of these key management schemes' scalability metric

	[8]	[18]	[9]	[19]	[20]	[21]
[8]	1	1	2	2	2	2
[18]	1	1	2	2	2	2
[9]	$\frac{1}{2}$	$\frac{1}{2}$	1	1	1	1
[19]	$\frac{1}{2}$	$\frac{1}{2}$	1	1	1	1
[20]	$\frac{1}{2}$	$\frac{1}{2}$	1	1	1	1
[21]	$\frac{1}{2}$	$\frac{1}{2}$	1	1	1	1

$N_p = 50$. We let the Key-pool size $KP = 1000$ and key ring $k = 50$. At the beginning of the AHP evaluation, the matrix key distribution scheme generates an $m \times m$ key matrix for a WSN of 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 total has $2m$ keys. Here m denotes the number of keys in master key list of a node and $m = \sqrt{N} = 10$.

For instance, if we take scalability into consideration and because we have already obtained each key management scheme's scalability numerical value from Table 2: $(B_S)_{[8]} = 2$, $(B_S)_{[18]} = 2$, $(B_S)_{[9]} = 1$, $(B_S)_{[19]} = 1$, $(B_S)_{[20]} = 1$, $(B_S)_{[21]} = 1$. We can obtain pair-wise comparison matrix of these key management schemes' scalability metric as following:

Accordingly, this matrix-Table 4 is then normalized to obtain the relative weight or eigenvector of each rating scale, the relative weights of key management scheme in [8], [18], [9], [19], [20], [21] are equal to 0.25, 0.25, 0.125, 0.125,0.125 and 0.125 respectively. The same time, obtain the CI=0, which also means the matrix keeps consistency well.

As the scalability matrix B_S, we can go through a similar process with key connectivity, resilience, storage overhead and communication overhead. Suppose the relative values for the objectives can be calculated as following Table 5:

4. CASE STUDY

As we obtain both the judgment matrix (Matrix A) and the matrixes for key management schemes with respect to each metric's comparison (Matrix B_S, B_K, B_R, B_M and B_C), we can calculate the final vectors for each key management scheme in the assumed WSN scenario.

Recalling our overall weights, we can get a final value for each key management scheme now. The value for [8] is 0.499. The solution of equations is as follows:

$\overrightarrow{A} \cdot \overrightarrow{W_A} = \lambda \overrightarrow{W_A}$, $\overrightarrow{B} \cdot \overrightarrow{W_B} = \lambda \overrightarrow{W_B}$

$\overrightarrow{W_{[8]}} = \overrightarrow{W_A} \cdot \overrightarrow{W_B}$

$0.039 \times 0.25 + 0.119 \times 0.25 + 0.269 \times 0.049 + 0.218 \times 0.273 + 0.352 \times 0.180 = 0.175555$

Similarly, the value for the others schemes in turns are calculated and concluded as follows:

- L. Eschenauer et al. [18] $= 0.039 \times 0.25 + 0.119 \times 0.25 + 0.269 \times 0.049 + 0.218 \times 0.273 + 0.352 \times 0.450 = 0.270595$
- C. Blundo et al. [9] $= 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.095 + 0.218 \times 0.265 + 0.352 \times 0.192 = 0.170659$
- S. Zhu et al. [19] $= 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.269 + 0.218 \times 0.041 + 0.352 \times 0.069 = 0.125337$

Table 5: Relative weights of each metric for pair-wise comparison matrix of these schemes

	$B_S Avg.$	$B_K Avg.$	$B_R Avg.$	$B_M Avg.$	$B_C Avg.$
[8]	0.25	0.25	0.049	0.273	0.180
[18]	0.25	0.25	0.049	0.273	0.450
[9]	0.125	0.125	0.095	0.265	0.192
[19]	0.125	0.125	0.269	0.041	0.069
[20]	0.125	0.125	0.269	0.038	0.069
[21]	0.125	0.125	0.269	0.110	0.039
	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$	$\Sigma Avg = 1$

- M. Shehab et al. [20] $= 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.269 + 0.218 \times 0.038 + 0.352 \times 0.069 = 0.124683$

- S. Slijepcevic et al. [21] $= 0.039 \times 0.125 + 0.119 \times 0.125 + 0.269 \times 0.269 + 0.218 \times 0.110 + 0.352 \times 0.039 = 0.129819$

Comparing the final 6 value of the vectors, we get the biggest vector: L. Eschenauer et al. [18] and the least vector: M. Shehab et al. [20].

The scheme in [18] is superior to the traditional key pre-distribution schemes. Because it presents a new key management scheme for large scale distribution sensor network. All such schemes must be extremely simple given the sensor-node computation and communication limitations. Their approach is also 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 in [20] is suitable for limited computation and energy capability sensor network.

Its proposed key generation algorithm is based on low cost hashing functions that enable the efficient key generation. Its key distribution protocol also is energy efficient. So this scheme is satisfy with the energy limitation problem 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.

5. CONCLUSIONS

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 different 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 choose suitable key management scheme under different wireless sensor network scenario requirements. Furthermore, we also show six typical key management schemes from the six classify aspects. Under assumed network scenarios, we can know the best scheme and the worst one via their final calculated values.

Formalizing decision making where there are a limited number of choices but each has a number of attributes and it is difficult to formalize some of those attributes. Obviously, AHP can prevent subjective judgment errors and increase the likelihood that the results are reliable. And AHP provides useful insight into the trade-offs embedded in a decision making problem.

6. REFERENCES

[1] J. Lopez, J. Y. Zhou, *Overview of wireless sensor network security*, in: IOS Press, 2008.

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

[3] S. A. CAMTEPE, B. Yener, *Key management in wireless sensor network*, in: IOS Press, 2008.

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

[5] J. Hwang, I. Syamsuddin, *Information Security Policy Decision Making: An Analytic Hierarchy Process Approach*, in: 2009 Third Asia International Conference on Modelling and Simulation, pp.158-163, 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*, in: Computer Communications, 30, 2007, pp. 2314-2341.

[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: IEEE Symp. Security and Privacy, 2003, p.197.

[9] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, *Perfectly-secure key distribution for dynamic conferences*, in: Crypto, 1992.

[10] D. Chakrabarti, S. Maitra, B. Roy, *A key pre-distribution scheme for wireless sensor networks: Merging blocks in combinatorial design*, in: Lecture notes in computer science ISSN 0302-9743.

[11] T. Ito, H Ohta, N Matsuda, T. Yoneda, *A key pre-distribution scheme for secure sensor network using probability density function of node deployment*, in: Proceedings of the 3rd ACM.

[12] L. Gong, D. J. Wheeler, *A matrix key distribution schemes*, in: Journal of Cryptology 2(1) (1990) 51-59.

[13] B. Dutertre, S. Cheung, J. Levy, *Lightweight key management in wireless sensor networks by leveraging initial trust*, in: Tech. Rep. SRI-SDL-04-02, System Design laboratory(2004).

[14] C. Fei. *Pair-wise Key Management in Wireless Sensor Network*, in: Computer Simulation[J],Vol22-5,2005.

[15] H. Soussi, M. Hussain, H. Afifi, D. Seret. *IKEv1 and*

IKEv2: A Quantitative Analyses, in: World Academy of Science, Engineering and Technology6 2005.

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

[17] *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: ACM Conf. Computer and Commun. Security, pp. 41-47, 2002.

[19] S. Zhu, S. Setia, S. Jajodia, *Leap:Efficient security mechanisms for large-scale distirbuted sensor networks*, in: ACM Conf. Computer and Commun. Security, pp. 62-72, 2003.

[20] M.Shehab, E.Bertino, A.Ghafoor, *Efficient hierarchical key generation and key diffusion for distribution for distributed sensor networks*, in: IEEE Int. Conf. Sensor and Ad Hoc Commun. and Netw., pp. 76-84, 2005.

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

[22] A. Casaca, D. Westhoff, *Scenario Definition and Initial Threat Analysis*, in: UbiSec and Sens Deliverable D0.1, 2006

[23] D.Liu, P.Ning, *Location-based pairwise key establishments for static sensor networks*, in: Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks, 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: ACM Workshop on Security of Ad Hoc and Sensor Network,2004

[26] D. Hwang, B. Lai, I. Verbauwhede, *Energy-memory-security tradoffs in distributed sensor networks*, in: ADHOC-NOW, LNCS, 2004

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

[28] S. A. Camtepe, B. Yener, *Combinatorial design of key distribution mechanisms for wireless sensor networks*, in: ESORICS, 2004

[29] M. Ramkumar, N. Memon, *An efficient random key pre-distribution scheme*, in: IEEE Global Telecommunications Conference, 2004

[30] G. Jolly, M. C. Kuscu, P. Kokate, M. Younis, *A low-energy key management protocol for wireless sensor networks*, in: Eighth IEEE International Symposium on Computers and Communication, 2003

[31] A. Chadha, Y. Liu, S. K. Das, *Group key distribution via local collaboration in wireless sensor networks*, in: IEEE Int. Conf. Sensor and Ad Hoc Commun. and Netw., 2005

[32] A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, *Spins: Security protocols for sensor networks*, in: Wireless Networks 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 Symp., 2003

[34] M. Bohge, W. Trappe, *An authentication framework for hierarchical ad hoc sensor networks*, in: ACM WiSe, 2003

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