

A Quantitative Survivability Evaluation Model for Wireless Sensor Networks

Xueping Li, *IEEE*, and Dengfeng Yang

Abstract—A wireless sensor network (WSN) is vulnerable to security attacks due to the broadcast nature of transmission and the limited computation and communication capabilities of the sensor nodes. Many key agreement schemes are developed to enable encryption and authentication among sensor nodes to protect confidentiality, integrity, and availability of the communications and computations of WSNs. It is crucial to build a model to evaluate these schemes with regard to survivability of a WSN. In this paper, we propose a quantitative evaluation model for a typical pre-distribution key management scheme. Specifically, we evaluate the survivability of a WSN with regard to its three major attributes: resilience, resistance, and robustness. Simulation results are reported showing that how a WSN become survivable and how it can be improved.

Index Terms—Wireless Sensor Networks, Survivability

I. INTRODUCTION

A wireless sensor network (WSN) typically consists of a number of small autonomous sensing devices, each of which is called a sensor node with a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter/receiver [1]. WSNs have wide applications including military sensing and tracking, real-time traffic and pollution monitoring, and wildlife monitoring, etc. The sensor nodes can be deployed in controlled environments (such as home, office, warehouse, forest, etc.), and in uncontrolled and dangerous environments (such as battlefields, toxic regions, etc.). WSNs are vulnerable to security attacks due to the broadcast nature of transmission and the limited computation and communication capabilities of the sensor nodes. Key agreement schemes are developed to enable encryption and authentication among sensor nodes to protect confidentiality, integrity, and availability of the communications and computations of WSNs. It is crucial to build a model to accurately evaluate these schemes. In this paper, we propose a quantitative evaluation model for a typical pre-distribution key (PDK) management scheme with regard to survivability.

Survivability in WSN has six challenges [1]: (i) wireless nature of communication, (ii) resource limitation on sensor nodes, (iii) very large and dense WSN, (iv) lack of fixed infrastructure, (v) unknown network topology prior to deployment, (vi) high risk of physical attacks to unattended sensors. Moreover, in some deployment scenarios sensor nodes need to operate under adversarial condition. Thus, sensor nodes have

to adapt to their environments, and establish a robust network protocol to communicate with the control center. Currently the survivability research and development of WSN focus on two aspects: providing authentication and integrity of messages [2]–[6], and modeling of energy-efficient protocol [7]–[9]. The former is accomplished by applying some secure key based schemes. The latter is obtained by prolonging the lifetime of the WSN without considering the intrusion. Energy-efficient protocols, although needed in order to prevent the sensor nodes from exhaustion, do not provide protection against injection and impersonation intrusions.

Therefore, motivation of this paper is to evaluate a typical key distribution scheme by providing survivability evaluation metrics and based on which to present a way to enhance the survivability of a WSN. Previous survivability evaluation methods [10]–[12] focus on faults tolerance, although it is an aspect of the survivability of a network, these methods can not give a comprehensive analysis of the survivability of WSNs. In this paper, we propose a survivability analysis model by quantitatively evaluate its resilience, resistance and robustness.

In Section 2, we describe the overall WSN architecture that is assumed throughout the paper and the key managements schemes for the network [13], [14]. We define the quantitative evaluation metrics and conduct simulations in Section 3. Finally, we summarize our findings in Section 4.

II. PROBLEM STATEMENT

We consider a large scale wireless sensor network which is distributed in a hostile environment, e.g. a sensor network deployed in a battlefield for tracking enemy tanks. The network is composed of low-complexity sensor nodes, e.g. the Berkeley MICA motes, which have limited processing power, memory, storage space, and computation capability. The network includes a globally trusted base station, which is the ultimate destination for data streams from all the nodes.

A. Basic key pre-distribution Scheme

Based on the fact that all possible link keys in a network of size N can be represented as an $N \times N$ key matrix, Blom's scheme [15] uses a public $(\lambda + 1)N$ matrix G and a secret $N(\lambda + 1)$ symmetric matrix D which is generated over a finite field $GF(q)$ and where N is size of the network. Blom's scheme is λ -secure, meaning that keys are secure if no more than λ nodes are compromised. Matrix G must have $(\lambda + 1)$ linearly independent columns (i.e. Vandermonde matrix) to provide λ -secure property.

Xueping Li is with the Department of Industrial and Information Engineering, University of Tennessee, Knoxville, TN 37996-0700, USA (phone: 865-974-7648; fax: 865-974-0588; email: Xueping.Li@utk.edu).

Dengfeng Yang is with the Department of Industrial and Information Engineering, University of Tennessee, Knoxville, TN 37996-0700, USA (phone: 865-974-2040; fax: 865-974-0588; email: den.yang@gmail.com).

According to the property of Vandermonde matrix, a sensor node k just needs to store the k th column of G , so that the seed s^k at this node is stored which can regenerate the column, then every pair of nodes can calculate corresponding field of the matrix, and uses it as the link key. Key matrix is then defined as a symmetric matrix $K = (DG)^T G = G^T D^T G = G^T (DG)$. Sensor node S_i stores $column_i$ of size $(\lambda + 1)$ from matrix G as public information, and row_i of size $(\lambda + 1)$ from matrix $(DG)^T$ as secret information. A pair of sensor nodes (S_i, S_j) , first exchange their public information $column_i$ and $column_j$. The link key is then generated as $K_{ij} = row_i column_j$ and $K_{ji} = row_j column_i$ respectively as summarized in Fig. 1. The scheme requires costly multiplication of two vectors of size $(\lambda + 1)$ where the elements are as large as the corresponding cryptographic key size. Each sensor node broadcasts one message, and receives one message from each node within its radio range where messages carry a vector of size $(\lambda + 1)$.

B. Expanded key pre-distribution Scheme

Blom's scheme is the optimal scheme while at the expense of relatively large memory requirement and computation power. Therefore a more practical and survivable scheme is presented which achieves good survivability and much lower memory usage and processing energy. A relaxed scheme [14] is proposed which reduced the *complete* graph Blom presented to a *connected* network, therefore requires much less storage and computation.

Based on [14], we construct a matrix G as presented in previous section, and then generate ω random, symmetric matrices $D_1, D_2, \dots, D_\omega$ of size $(\lambda+1) \times (\lambda+1)$. Then matrices $A_i = (D_i \times G)^T$ can be obtained and $A_i(j)$ denotes the j th row of A_i . For each node, i.e. j τ ($2 < \tau < \omega$) distinct key spaces for the ω matrices are randomly chosen, and the j th row of A_i is stored, where $A_i(j)$ is secret, and the node j will never send it to any other node. According to Blom's scheme, two nodes can establish a common secret key if they both hold a common key space. Since A_i is an $N(\lambda + 1)$ matrix, $A_i(j)$ contains $(\lambda + 1)$ elements, therefore, each node just needs to store $(\lambda + 1) \times \tau$ elements in its memory.

C. Key agreement phase

After deployment, each node needs to determine which node shares a common key space and then sends message it. To accomplish it, assume that nodes i and j are neighbors, and have sent the broadcast HELLO messages. If they determine that they share a common space, say D_c , they can compute a pairwise private key using Blom's scheme: Initially node i has $A_c(i)$ and seed $G(i)$, node j has $A_c(j)$ and seed $G(j)$. After exchanging the seeds, node i can regenerate $G(j)$ and node j can regenerate $G(i)$; then the pairwise private key K_{ij} and K_{ji} between nodes i and j can be computed in the following manner by these two nodes, respectively: $K_{ij} = A_c(i) \times G(j) = A_c(j) \times G(i) = K_{ji}$. As long as a common share key is established, the two nodes can

communicate messengers without being eavesdropped by other intruders.

If two neighboring nodes i and j do not share a common key space, they can always find a path in the key sharing graph G_{ks} from i to j as long as G_{ks} is connected, i.e. i, v_1, \dots, v_1, j , and finally establish a common key for communication.

D. Threat model

There are a wide variety of threats to WSNs. We present a set of attack scenarios that are able to compromise one or more key spaces of a WSN. Researchers have pointed out that there is no sure and efficient way to readily detect a node capture [16]. Because of this, it is important to emphasize the network's survivability given a number of undetected node captures, in addition to the ability to recover from a single node capture at a time.

The attack scenario that possesses the greatest threat to the bottom tier of the network is the wormhole. In the wormhole attack [4], a captured node can build a false tunnel with another malicious node at a distant point, and creates the illusion that the two end points are very close to each other, by making tunneled packets arrive either sooner or with lesser number of hops compared to the packets sent over normal routes. The wormhole attack can affect network routing, data aggregation, and clustering protocols. Finally, it is worth noting that the wormhole attack can be launched even without having access to any cryptographic keys or compromising any legitimate node in the network. This problem can be solved by appending the node's identity in the messengers, i.e. $G(i)$. A captured node can not establish a tunnel with its neighbors without $G(i)$ and a private key $A_c(i)$.

In the sinkhole attack, a captured node manages to attract routes from many neighbors to go through it thus acting as a sinkhole. This attack typically works by making the captured node look especially attractive for the surrounding nodes, for example, by claiming a short or a fast path to the base station. If the attacker succeeds, he can launch data traffic jam and can exhaust the energy. In the proposed scheme, the pairwise key agreement protocol provides information authentication and prevents sinkhole from happening.

In the ID spoofing and sybil attacks, an attacker presents one (ID spoofing) or more (sybil attack) spoofed identities to the network. Those identities could either be new fabricated identities or stolen identities from legitimate nodes. The Sybil attack can have many adverse impacts, such as multipath routing.

In this study, we treat a sensor node as compromised regardless of which threat model captures it.

III. EVALUATION METRICS

A. Definition

Various survivability definitions have been proposed in different disciplines, such as the following definition from [12] in our discussion, which emphasizes the time-varying behavior of the system after a failure or an attack occur: *Survivability is the capability of a system to fulfill its mission*

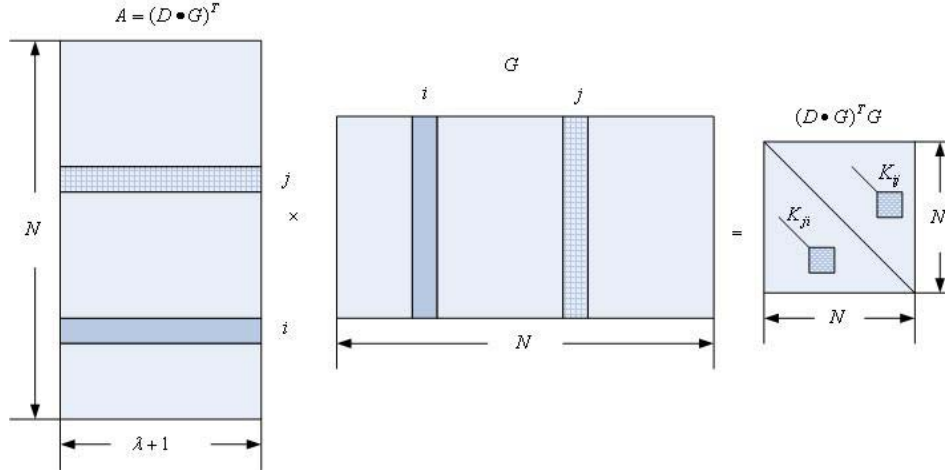


Fig. 1. Blom's keys generation scheme

in a timely manner, even in the presence of attacks or failures. Survivability goes beyond security and fault tolerance to focus on delivery of essential services, even when systems are penetrated or experience failures, and rapid recovery of full services when conditions improve.

While these definitions provide a good description of the concept of survivability, they do not have mathematical precision to lead to a quantitative determination of survivability. It is hard to determine whether a given system is survivable, and it is difficult to compare the survivability of two systems. For this reason, Knight [17] introduced a general definition of survivability for critical information systems: A survivability specification is a four-tuple, (E, R, P, M) where: E is a statement of the assumed operating environment for the system, R is a set of specifications each of which is a complete statement of a tolerable form of service that the system must provide, P is a probability mass function across the set of specifications, and M is a finite state machine.

For sensor networks which have many characteristics that make them more vulnerable to attacks than conventional wired computing equipment. Based on the definition of [17], we present several criteria that represent desirable characteristics in a key-setup scheme. A WSN with these characteristics could function properly at the presence of malicious attacks.

1) Resilience is given as either one of the following ways: (i) probability that a link is compromised when an adversary captures a node, (ii) number of nodes whose security credential are compromised when an adversary captures a node, or (iii) number of sensor nodes required to be captured to compromise whole WSN.

2) Resistance against node replication. Whether the adversary can insert additional hostile nodes into the network after obtaining some secret information (e.g. through node capture or infiltration). This is a serious attack since the compromise of even a single node might allow an adversary to populate the network with clones of the captured node to such an extent that legitimate nodes could be outnumbered and the adversary

can thus gain full control of the network.

3) Key connectivity considers probability that two (or more) sensor nodes store the same key or keying material to be able to establish pair-wise keys.

4) Recovery requires that a survivable system to be able to quickly incorporate lessons learned from failures, evolve, and adapt to emerging threats [18].

B. Quantitative metrics

We evaluate the multiple-space key pre-distribution scheme in terms of its survivability against node capture and attacks based on the definition above. Thus, we define the three major attributes of survivability as following: (1) When x nodes are captured, what is the probability that at least one key space is broken? This analysis shows the network's resilience with x nodes are captured. (2) When x nodes are captured, what fraction of the additional communication also becomes compromised? This analysis shows the networks's resistance against the x nodes' being captured. (3) When x nodes are captured, what is the probability of the actual local two nodes share at least one key space? This analysis shows the networks's robustness against the x nodes' being captured. In our analysis, we assume that the adversary has no a priori knowledge of the keys carried by each sensor and we therefore model the attacker as compromising random nodes. Based on the work by [13] and [14], we define the following metrics.

1) *Resilience*: The quantitative formulation of resilience is the probability of at least one space being broken. We define our unit of memory as the size of a secret key (e.g., 64 bits). In Blom's scheme, for a space to be λ -secure each node needs to use memory of size $\lambda+1$. Therefore, if the memory usage is m and each node needs to carry τ spaces, the value of λ should be $\lfloor \frac{m}{\tau} \rfloor - 1$. We use this value for λ in the following analysis. Let S_i be the event that the i th key space is compromised (for $i \in (1, 2, \dots, \omega)$), let C_x be the event that x nodes are compromised in the network. We have the probability of at

least on space is broken:

$$Pr(\text{at least one space is broken}|C_x) = \frac{Pr(S_1 \cup S_2 \cup \dots \cup S_\omega|C_x)}{Pr(C_x)} \quad (1)$$

According to the union bound, we obtain

$$Pr(S_1 \cup S_2 \cup \dots \cup S_\omega|C_x) \leq \sum_{i=1}^{\omega} Pr(S_i|C_x) \quad (2)$$

Due to the fact that each key space is broken with equal probability independently, we have

$$\sum_{i=1}^{\omega} Pr(S_i|C_x) = \omega Pr(S_1|C_x) \quad (3)$$

Where $Pr(S_1|C_x)$ represents the probability of the first key space being compromised when x nodes are compromised. Because each node carries information from τ spaces, the probability that each compromised node carries information about the first key space is $\gamma = \frac{\tau-1}{\omega-1}$. Therefore, after x nodes are compromised, the probability that exactly j of these x nodes contain information about the first key space is $C_j^x \gamma^j (1-\gamma)^{x-j}$. Since each key space can be broken only after at least $\lambda+1$ nodes are compromised (by the λ -secure property of the underlying Blom's scheme), we have the following result:

$$Pr(S_1|C_x) = \sum_{j=\lambda+1}^x C_j^x \gamma^j (1-\gamma)^{x-j} \quad (4)$$

Combining inequality (2) and Eq.(4), we obtain the following upper bound:

$$\begin{aligned} Pr(\text{at least one space is broken}|C_x) &\leq \omega \times \sum_{j=\lambda+1}^x C_j^x \gamma^j (1-\gamma)^{x-j} \\ &= \omega \times \sum_{j=\lambda+1}^x C_j^x \left(\frac{\tau-1}{\omega-1}\right)^j \left(1 - \frac{\tau-1}{\omega-1}\right)^{x-j} \end{aligned} \quad (5)$$

Therefore, the resilience of the system is $P_{Resilience} = 1 - Pr(\text{at least one space is broken}|C_x)$. The simulation results are shown in Fig. 2. Four different cases are shown, where the memory usage is set to 150, and from left to right the pairs of τ and ω are (4, 40)(4, 50)(3, 40)(3,50), respectively. We can see that increasing ω and decreasing τ will improve a WSN's resilience.

2) *Resistance*: Resistance is the survivable ability of the rest system with the effect of capture of x sensor nodes by an adversary. In quantitative, the fraction of additional communication that an adversary can compromise based on the information retrieved from the x captured nodes can describe this requirement. The smaller the fraction is, the bigger the resistance ability against attacks is.

First we compute the probability that any one of the additional communication links is compromised after x nodes

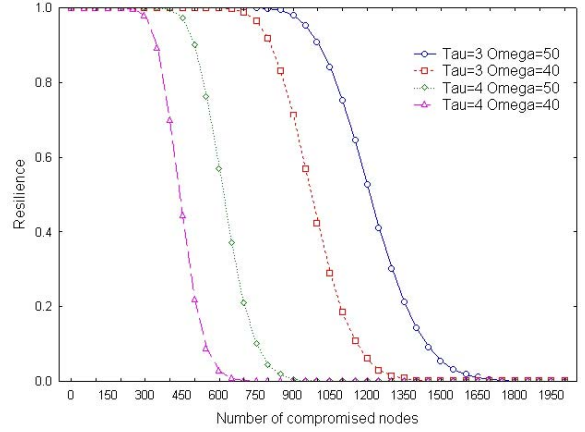


Fig. 2. Resilience v.s. number of compromised nodes given ($\tau = 4, \omega = 40$), ($\tau = 4, \omega = 50$), ($\tau = 3, \omega = 40$), ($\tau = 3, \omega = 50$) respectively.

are captured. Note that we only consider the links in the key-sharing graph, and each of these links is secured using a pairwise key computed from the common key space shared by the two nodes of this link. We should also note that after the key setup stage, two neighboring nodes can use the established secure links to agree upon another random key to secure their communication. Because this key is not generated from any key space, the security of this new random key does not directly depend on whether the key spaces are broken. However, if an adversary can record all communication during the key setup stage, he/she can still compromise this new key after compromising the corresponding links in the key-sharing graph. Let c be a link in the key-sharing graph between two uncompromised nodes, and let K be the communication key used for this link. Let S_i denote the i th key space, and let B_i represent the joint event that K belongs to S_i and S_i is compromised. We use the notation $K \in S_i$ to represent that key K was derived using S_i . The probability of c being compromised given the compromise of x other nodes is:

$$Pr(c \text{ is broken}|C_x) = Pr(B_1 \cup B_2 \cup \dots \cup B_\omega|C_x) \quad (6)$$

Since c uses only one key, events B_1, \dots, B_ω are mutually exclusive, therefore,

$$\begin{aligned} Pr(c \text{ is broken}|C_x) &= \sum_{i=1}^{\omega} Pr(B_i|C_x) \\ &= \omega Pr(B_1|C_x) \end{aligned} \quad (7)$$

According to the conditional probability,

$$\begin{aligned} &Pr(c \text{ is broken}|C_x) \\ &= \frac{Pr((K \in S_1) \cap (S_1 \text{ is compromised})|C_x)}{Pr(C_x)} \end{aligned} \quad (8)$$

Since the event $(K \in S_1)$ is independent of the events C_x and

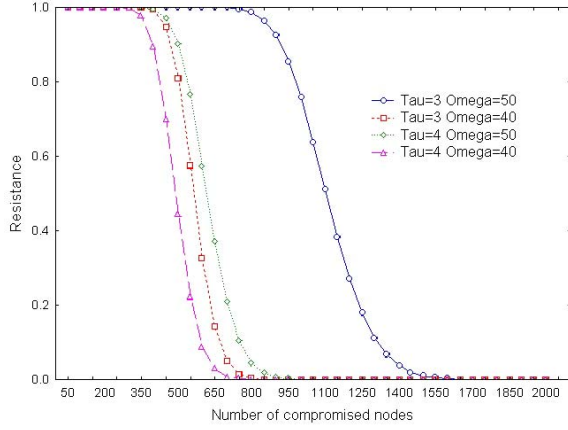


Fig. 3. Resistance v.s. number of compromised nodes given $(\tau = 4, \omega = 40)$, $(\tau = 3, \omega = 40)$, $(\tau = 4, \omega = 50)$, $(\tau = 3, \omega = 50)$

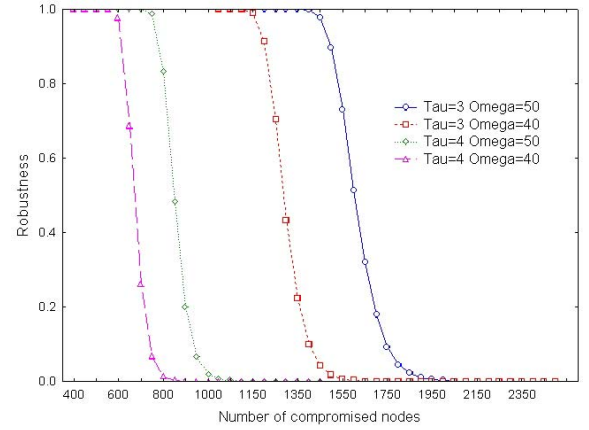


Fig. 4. Robustness v.s. number of compromised nodes when $(\tau = 3, \omega = 40)$, $(\tau = 3, \omega = 50)$, $(\tau = 43, \omega = 40)$, $(\tau = 4, \omega = 50)$

$(S_1$ is compromised),

$$\begin{aligned} & Pr(c \text{ is broken} | C_x) \\ &= \frac{Pr(K \in S_1) \times Pr((S_1 \text{ is compromised}) \cap C_x)}{Pr(C_x)} \quad (9) \\ &= Pr(K \in S_1) \times Pr((S_1 \text{ is compromised}) | C_x) \end{aligned}$$

$Pr((S_1 \text{ is compromised}) | C_x)$ can be obtained in Eq. (4). The probability that K belongs to space S_1 is the probability that link c uses a key from space S_1 . Since key spaces are uniformly from the ω possibilities, we have:

$$\begin{aligned} Pr(K \in S_1) &= Pr(\text{the link } c \text{ uses a key from space } S_1) \\ &= \frac{1}{\omega} \end{aligned} \quad (10)$$

Therefore,

$$\begin{aligned} Pr(c \text{ is broken} | C_x) &= \omega Pr(B_1 | C_x) \\ &= \omega \frac{1}{\omega} Pr((S_1 \text{ is compromised}) | C_x) \\ &= Pr((S_1 \text{ is compromised}) | C_x) \\ &= \sum_{j=\lambda+1}^x C_j^x \left(\frac{\tau-1}{\omega-1}\right)^j \left(1 - \frac{\tau-1}{\omega-1}\right)^{x-j} \end{aligned} \quad (11)$$

Therefore, the resistance ability is $P_{Res} = 1 - Pr(c \text{ is broken} | C_x)$. Fig. 3 shows four different cases, where the memory usage is set to 150, and from left to right the pairs of τ and ω are $(4, 40)$, $(3, 40)$, $(4, 50)$, $(3, 50)$, respectively. We can see that smaller τ and larger ω lead to higher resistance.

3) *Robustness*: The quantitative formulation of robustness is the probability of at least one space being connected when x nodes are captured, which shows the robustness of the sensor network to provide information service when coming across attacks. Using the similar method, Let S_i be the event that the i th key space is compromised (for $i \in 1, 2, \dots, \omega$), let C_x be the event that x nodes are compromised in the network, and

set $\gamma = \frac{\tau}{\omega}$. We have the probability of at least on space is connected:

$$\begin{aligned} Pr(\text{at least one space is connected} | C_x) &= \\ &= 1 - Pr(\text{all spaces are compromised} | C_x) \quad (12) \\ &= 1 - Pr(S_1 \cap S_2 \cap \dots \cap S_\omega | C_x) \end{aligned}$$

According to the union bound, we obtain

$$\begin{aligned} Pr(S_1 \cap S_2 \cap \dots \cap S_\omega | C_x) \\ \geq \prod_{i=1}^{\omega} Pr(S_i | C_x) \end{aligned} \quad (13)$$

Due to the fact that each key space is broken with equal probability and is independence, we have

$$\prod_{i=1}^{\omega} Pr(S_i | C_x) = (Pr(S_1 | C_x))^{\omega} \quad (14)$$

Combining inequality (13) and Eq.(4), we thus obtain the following upper bound:

$$\begin{aligned} Pr(\text{at least one space is connected} | C_x) \\ \leq 1 - \left(\sum_{j=\lambda+1}^x C_j^x \gamma^j (1-\gamma)^{x-j} \right)^{\omega} \end{aligned} \quad (15)$$

As shown in Fig. 4, when the memory usage is set to 150, ω is set to 50, and τ is set to 3, the value λ is 49. In order to break the whole sensor network with a high probability, an adversary needs to capture more than 1620 nodes. Suppose a WSN application has a sensor density of 1 node per 10 m^2 , according to the result, the adversary must control an area of 16200 m^2 to destroy the network totally, it is infeasible and uneconomical in real application.

C. Enhanced scheme

According to quantitative results and Fig. 2, 3, and 4, we find that the larger the value of ω is, the smaller of the τ is, the more resilient, resistant and robust the network is. An direct explanation is that a larger key space ω can provide more choices for the base station and nodes, and a smaller random multi-key space τ decreases the probability of overlap of selected key and intruded key, then improve

the survivability of the system. Therefore, considering the trade-off between the computation limitation and survivability requirement, decreasing the multiple key space τ to 2 and increasing ω to 50 can improve the survivability of the system, given a fixed network size N , i.e.10,000.

IV. CONCLUSION

In this paper, we have proposed a survivability quantitative evaluation method based on a typical key pre-distribution scheme for WSN. We argue that a survivable sensor network should have the following features: 1) Resilience, the probability that a link is uncompromised when an adversary captures one or more nodes; 2) Resistance against node replication. 3) Robustness provides services against attacks. Through analytical and simulation results, we have shown that this evaluation method can be used as a quantitative standard to judge whether a WSN is survivable or not before it is deployed. Furthermore, we have also shown that increasing the key space and decreasing the multiple key space would improve the survivability of WSNs.

REFERENCES

- [1] S. A. Camtepe and B. Yener, "Key distribution mechanisms for," Rensselaer Polytechnic Institute, Computer Science Department, Tech. Rep., 2005, technical Report TR-05-07.
- [2] B. Carbunar, I. Ioannidis, and C. N-Rotaru, "Janus: Towards robust and malicious resilient routing in hybrid wireless networks," ACM Workshop on Wireless Security, October 2004.
- [3] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, pp. 293–315, January 2003.
- [4] I. Khalil, S. Bagchi, and C. N-Totaru, "Dicas: Detection, diagnosis and isolation of control attacks in sensor networks," in *IEEE Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm) 2005*, September 2005.
- [5] D. T. A.Perrig, R. Canetti and D. Song, "The tesla broadcast authentication protocol," *RSA CryptoBytes*, vol. 5, no. 2, pp. 2–13, 2002.
- [6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar, Eds., *SPINS: Security Protocols for Sensor Networks*. Proc. of ACM Mobicom'01, 2001.
- [7] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: an energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks," in *Proceedings of the ACM International Conference on Mobile Computing and Networking*. Rome, Italy: ACM, July 2001.
- [8] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," in *Proceedings of the Hawaii International Conference on Systems Sciences*, January 2000.
- [9] A. Wang and A. Chandrakasan, "Energy-efficient dsps for wireless sensor networks," ICASSP, 2001.
- [10] D. Chen, S. Garg, and K. S. Trivedi, "Network survivability performance evaluation: A quantitative approach with applications in wireless adhoc networks," MSWiM'02, Atlanta, Georgia, USA., September 2002.
- [11] V. B. M. Y. Liu and K. S. Trivedi, Eds., *Survivability Analysis of Telephone Access Network*. Proc. of 15th IEEE International Symposium on Software Engineering, 2004.
- [12] B. Ellison, D. A. Fisher, R. C. Linger, H. F. Lipson, T. Longstaff, and N. R. Mead, "Survivable network systems: An emerging discipline," Software Engineering Institute, Carnegie Mellon University, Tech. Rep., 1999.
- [13] H.Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," IEEE Symposium on Security and Privacy, Berkeley, CA., 2003, 197C213.
- [14] W. Du, J. Deng, Y. S. Han, and P. Varshney, "A pairwise key predistribution scheme for wireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003.
- [15] R. Blom, Ed., *An optimal class of symmetric key generation systems*, vol. 209, Proceedings of EUROCRYPT 84. Springer-Verlag, Berlin, 1985, lecture Notes in Computer.
- [16] M. Chorzempa, J. Park, and M. Eltoweissy, "Ipccc '05," in *24th IEEE International Performance Computing and Communications Conference*, 2005.
- [17] J. Knight, K. J. Sullivan, M. C. Elder, and C. Wang, "Survivability architectures: Issues and approaches," in *DARPA Information Survivability Conference and Exposition (DISCEX 2000)*, Hilton Head, SC, January 2000.
- [18] J. Sterbenz and R. Krishnan, "Survivable mobile wireless networks: Issues, challenges, and research directions," Wise'02, September 2002, atlanta, Georgia, USA.