Scaling Laws of Key Pre-distribution Protocols in Wireless Sensor Networks

Wenjun Gu, Sriram Chellappan, Xiaole Bai and Honggang Wang

***Abstract*—Many key pre-distribution (*KP*) protocols have been proposed and well accepted in randomly deployed wireless sensor networks (WSNs). Being distributed and localized, they are perceived to be scalable as node density and network dimension increase. While it is true in terms of communication/computation overhead, their scalability in terms of security performance is unclear. In this paper, we conduct a detailed study on this issue. In particular, we define a new metric called Resilient Connectivity (RC) to quantify security performance in WSNs. We then conduct a detailed analytical investigation on how *KP* protocols scale with respect to node density and network dimension in terms of RC in randomly deployed WSNs. Based on our theoretical analysis, we state two *scaling laws* of *KP* protocols. Our first scaling law states that *KP protocols are not scalable in terms of RC with respect to node density*. Our second scaling law states that *KP protocols are not scalable in terms of RC with respect to network dimension*. In order to deal with the un-scalability of the above two scaling laws, we further propose logical and physical group deployment respectively. We validate our findings further using extensive theoretical analysis and simulations.**

***Index Terms*—Sensor Networks, Information Security, Key Management, Resilience, Scalability**

I. Introduction

Many applications for Wireless Sensor Networks (WSNs) are envisaged in military, mission-critical and hostile environments. In such applications securing sensor communications from attackers is critical. The standard approach is to establish secure pairwise keys between communicating sensors. However, in many WSNs, deployment cannot be accurately determined or controlled, sensors have energy/ storage constraints, are easier to be captured etc. These features make key management challenging in WSNs. They also limit the applicability of traditional schemes like centralized key distribution center (large messaging overhead), installing a single master key to all nodes (poor resilience) etc. for WSNs. The disadvantage of using public key cryptography based schemes for WSNs is the significant computational overhead [1].

Currently, the well accepted approach for key management in WSNs is based on the idea of key pre-distribution [3]. In the simplest version, each sensor is pre-distributed with k distinct keys randomly chosen from a large pool of K keys, and nodes are deployed randomly in the network. After deployment, neighboring nodes use pre-distributed keys to establish a pairwise key between them either directly or using other nodes as proxies. The redundancy in key pre-distribution (k keys per sensor) enables nodes overcome deployment randomness, helping discover secure neighbors and proxies. Many key management protocol variants have been proposed based on key pre-distribution (called *KP* protocols) [3] [4] [5] [6] [7] [8] [9] [10] [11] [12] [13] [14] [15] [16] [17] [18] etc., each one improving features like *connectivity*, *resilience*, *overhead* etc. Note that while each *KP* protocol variant is different from the other in terms of certain parameters and features (discussed in detail later), the core idea of pre-distributing keys to sensors and pairwise key establishment among the sensors is the same in all protocol variants.

Motivation: An important requirement of key management protocols in WSNs is scalability. Many security aware WSN applications are envisaged where thousands of nodes are deployed. There are two key properties that determine network size in WSNs: *node density* (average number of neighbors per node) and *network dimension* (geographical size of the network). Being distributed and localized, communication and computational overhead increase in *KP* protocols is mild when node density increases. With higher node density, it is also believed that security performance improves, as nodes can now find more secure neighbors and proxies. In fact, many *KP* protocols assume a very high node density ($\geq$ 20 neighbors per node) with the notion that it enhances performance [3], [4], [5]. From the perspective of network dimension also, *KP* protocols are generally believed to be scalable.

In the context of secure communications however, the WSN is under attacks. In such situation, while an increase in number of nodes helps network side, it also enables malicious attackers to capture more nodes (to disclose more keys) and monitor more links in the network. There is hence a tug of war between the network and attackers in terms of how extra nodes (and keys) are leveraged by each other. Because of this war between two conflicting entities, the scalability of *KP* protocols in terms of security performance has not yet been comprehensively determined. In this paper, we address this issue.

Our Contributions: We have the following four contributions in this paper.

- We define a new metric called *Resilient Connectivity* (RC) to quantify security performance for all *KP* protocols. Formally, RC is the probability that two neighboring nodes can establish a *secure* pairwise key between them under attacks. This metric naturally considers both connectivity and resilience, two standard metrics used to evaluate security performance of KP protocols in

Wenjun Gu is currently with Microsoft, USA - E-mail: wenjgu@microsoft.com. Sriram Chellappan is with The Department of Computer Science at Missouri University of Science and Technology, Rolla, USA - Email: chellaps@mst.edu. Xiaole Bai and Honggang Wang are with The Department of Computer and Information Science, and The Department of Electrical and Computer Engineering respectively at University of Massachusetts, Dartmouth, USA - Email: {xbai, hwang1}@umassd.edu.

[1]Due to recent advances in sensor node hardware, public key based schemes are receiving attention lately in WSNs [1], [2].

previous literatures. To the best of our knowledge, ours is the first paper to propose a unified metric to evaluate the security performance of KP protocols.

- We conduct a comprehensive survey on state-of-the-art KP protocols, and make a detailed classification of all these protocols. In particular, we first identify and abstract the parameters that capture all the features that impact *RC* in any *KP* protocol. Then we classify all *KP* protocols based on different particular instances of these parameters, and derive the expressions for all the parameters in all the KP protocols.
- We rigorously derive a general expression for RC as the basis of our scalability study. Specifically, based on the derivations of the parameters that impact RC in all KP parameters, we obtain a general form expression of RC based on these parameters. Such general expression allows us to study KP protocol scalability effectively, and draw general conclusions for all protocols.
- We conduct a detailed analytical investigation on how *KP* protocols scale with respect to node density and network dimension in terms of RC in randomly deployed WSNs. Based on our theoretical analysis, we state two *scaling laws* for security performance of *KP* protocols. Our first scaling law states that *KP protocols are not scalable in terms of RC with respect to node density*. Our second scaling law states that *KP protocols are not scalable in terms of RC with respect to network dimension*. We also conduct extensive numerical analysis and simulations to further validate our results. In fact, our data show that for reasonable network, protocol and attack parameters, RC starts to monotonically decrease from node densities around 20, and tends to $zero$ quickly after that. Our data also demonstrate that RC rapidly tends to zero even for small values of network dimension (around $500m$). Besides the two scaling laws above, we also find that node density is a double-edged sword in that the increase of node density favors both network side and attack side. There exists an optimal value for node density that can achieve maximum RC. We are able to determine such optimal node density based on our theoretical analysis.
- Finally, we propose two types of group deployment to deal with the un-scalability of the above two scaling laws. In particular, we propose *logical* group deployment to deal with the un-scalability brought by node density, in which sensors are deployed in multiple rounds over the whole network. Since sensors in different rounds are pre-distributed with keys from disjoint key pools, the un-scalability issue brought by high node density is alleviated. On the other hand, we propose *physical* group deployment to deal with the un-scalability brought by network dimension, in which sensors are deployed in groups over different areas of the network. Since sensors in different groups are pre-distributed with keys from partially overlapped or disjoint key pools, the un-scalability issue brought by network dimension is alleviated.

We believe that our findings are fundamental and identify inherent limitations in existing understanding of key management in randomly deployed WSNs. We show that care should be taken during resource provisioning for secure WSNs. While focusing on protocol scalability in terms of overhead is important, we show it is equally (if not more) critical to also consider scalability in terms of security performance. Our work has quantitative significances too. When deployers may have a priori knowledge on attack intensities based on historical experience, our closed form expressions in this paper can be complemented with existing tools to derive optimum node densities and network dimensions for best performance.

The rest of our paper is organized as follows. In Section II, we present background on *KP* protocols, their variants, attack models and performance metrics. In Section III, we present analysis on the security performance of KP protocols. In Sections IV and V, we study how the *KP* protocols scale with respect to node density and network dimension respectively, including both theoretical analysis and simulation data. In Section VI, we propose two types of group deployment to deal with the un-scalability brought by the two scaling laws. We finally conclude our paper in Section VII.

II. Key Pre-distribution Protocols

In this section, we provide a background on Key Pre-distribution (*KP*) based protocols, attack models and performance metrics for secure communications in WSNs. We also classify the KP protocols based on several features.

A. Basic KP Protocol

1) Protocol Description: The seminal approach of key pre-distribution for randomly deployed sensor networks was first proposed in [3], where the idea is to provision a certain degree of *redundancy* in key sharing among sensors before deployment. After deployment, neighboring nodes leverage this redundancy to establish pairwise keys between them. There are two stages in this protocol. At the *key setup* stage, each node is pre-distributed with k distinct keys randomly chosen from a large pool of K keys, and nodes are deployed randomly in the network. We point out that the pre-distributed keys are typically not deleted after protocol execution [3] [4] [5] [6]. They will be used for pairwise key establishment during later node additions due to faults, failures etc. Fig. 1 shows a deployment instance of 10 nodes, where $k = 3$ and $K = 9$. Nodes inside the circle are within the communication range of node a. The pre-distributed keys for these nodes are also shown in Fig. 1. A list of basic parameters in the *KP* protocol and their notations are presented in Table I.

At the *pairwise key establishment* stage, neighboring nodes try to establish pairwise key in between using pre-distributed keys. First, each node obtains neighborhood key sharing information in its information area. The information area for a node is the area within which the node is aware of information on other nodes and their pre-distributed keys. We denote this parameter as A. For instance, the information area for node a in Fig. 1 is the area in its one hop communication range. If two neighbors already share a pre-distributed key (e.g., nodes a and b share key k_3), they establish a pairwise key directly. To do so, node a generates a random pairwise key

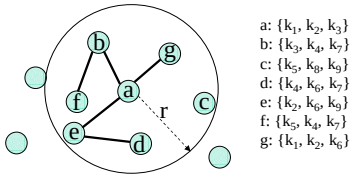

Fig. 1. An initial deployment of sensors pre-distributed with keys.

TABLE I
PARAMETERS IN KP PROTOCOLS

L	Network dimension
S	The area of network, $S = L \times L$
D	Node density (average number of nodes in communication disk)
N	The total number of nodes deployed, $N = DS/\pi r^2$
r	Communication range
k	The number of keys (key structures) distributed in a sensor
K	The total number of keys (key structures) in the pool
λ	The degree of key structure
A	The size of information area for a node
N_c	The number of nodes in a given sensor's information area
H	Maximum number of hops allowed on one key path
q	Minimum number of shared keys needed for a link to be usable
P_c	Probability for each node to be captured by the attacker

and sends it to node b encrypted with key k_3. However, two physical neighbors may not always share a pre-distributed key due to randomness in key pre-distribution and deployment. Here, the nodes will use *proxies* to construct key paths for pairwise keys. A random key share is transmitted on each key path, and is encrypted/decrypted hop by hop. The pairwise key is a combination (e.g., bitwise XOR) of all key shares. For example, nodes a and f can use node b as a proxy to construct a key path $a \rightarrow b \rightarrow f$ (since nodes b and f share keys k_4 and k_7 and are physical neighbors). Note that nodes a and c cannot establish a pairwise key between them, because they do not share any pre-distributed key and cannot find any proxy. Finally, pairwise keys are used to encrypt future communications between neighboring nodes.

2) Attack Models: The standard attack model used in WSNs is where the attacker attempts to decipher sensor communications [3] [4] [5] [6] etc. The attacker will launch two types of attacks. In *node capture attack*, the attacker physically captures a certain percent of nodes, and disclose their pre-distributed and pairwise keys. The probability of a node to be captured is P_c. In *link monitor attack*, the attacker monitors information on *all* network links *immediately* after deployment. Clearly, all communications to and from captured nodes are deciphered by the attacker. Also, by combining disclosed pre-distributed keys and messages recorded, the attacker can infer some pairwise keys between uncaptured nodes. For instance in Fig. 1, by capturing node g, the attacker obtains key k_2, and thus discloses the pairwise key between nodes a and e (without capturing either node), since the communication for establishing the pairwise key between nodes a and e is encrypted by k_2.

When multiple key paths are used to establish a pairwise key, the pairwise key is not disclosed unless all the key paths are compromised. A key path is compromised if one node on the path is captured or one link on the path is compromised. A link between two adjacent nodes on the key path is compromised if all shared pre-distributed keys between those two nodes are disclosed. An uncompromised key path is called as a $secure$ key path, and an undisclosed pairwise key is called as a $secure$ pairwise key. As we can expect, using multiple key paths to establish a pairwise key results in much higher resilience than using only one key path under attack. This is simply because the chance of attacker compromising all key paths decreases sharply with the number of key paths used. Although the basic scheme in [3] uses only one key paths for pairwise key establishment, in the remaining of the paper, we assume all schemes use multiple key paths for pairwise key establishment and conduct our analysis based on this. This assumption is beneficial only to the network side and does not affect our conclusion in this paper. For similar reason, we also assume all shared keys on a link are used for pairwise key establishment instead of one of the shared keys as used in the basic scheme in [3]. We emphasize that the above attack model is the de-facto one used in many key management works [2].

3) Performance Metrics: To evaluate performance of *KP* protocols, two metrics are used: *Connectivity* and *Resilience*. Connectivity is the probability that two physical neighbors establish a pairwise key between them. While the above definition refers to local connectivity one could also define global connectivity as probability that the entire network is securely connected, or as the percent of nodes in the largest connected component of the secure network. Since either definition of global connectivity relates to local connectivity [20], we focus on local connectivity (henceforth called *connectivity*) in this paper. The other metric is *resilience*, which is the conditional probability that the pairwise key between two physically neighboring nodes is not disclosed to the attacker given that such pairwise key exists between the two nodes. In other words, in computing resilience, we only consider those links that have pairwise keys established. The effect of links that dont have pairwise keys is considered in metric of connectivity above. The overall goal of any key management protocol is to achieve high connectivity and resilience.

B. KP Protocol Variants

In the above, we described the basic *KP* protocol in [3]. Many *KP* protocol variants have been proposed to enhance the basic protocol across several features. However, the core idea of two stages, namely, key pre-distribution to sensors followed by pairwise key establishment among sensors is same for all protocols. In this section, we describe these *KP* protocol variants based on the enhancement of the features in these two stages. A detailed classification KP protocols and the features (and corresponding specifics) that have been extended in those protocols are presented in Table II.

1) Enhancement in Key Setup Stage: The first feature is the nature of the pre-distributed keys. In the basic protocol [3], *random keys* are pre-distributed. In the *KP* protocol variant in [4], *unique pairwise keys* are distributed into pairs of sensors

[2]While some works like [19] assume a safe period (no node captures) after deployment, this assumption may not be always realistic in practice, and this attack model is not widely adopted.

TABLE II

CLASSIFICATION OF KP PROTOCOLS

Protocol Stages	Protocol Features		Protocols
	Type	**Specifics**	
key setup	nature of distributed keys	random keys	*basic protocol* [3], $q-composite$ [4], *direct/cooperative* [8], *probabilistic* [9], *deployment knowledge* [11], $PIKE$ [12], $RKEP$ [13], $configuration/intersection$ [15]
		unique pairwise keys	*random pairwise key* [4], *closest pairwise key* [7], GKE [16]
		random key structures	$multi-space$ [5], *random subset* [6], *grid based* [6], *location based* [7], *location aware* [10], *hexagonal grid* [14], *multivariate* [17] [18]
	key distribution method	random	*basic protocol* [3], $q-composite$ [4], *multivariate* [17] [18], $multi-space$ [5], *random subset* [6], *direct/cooperative* [8], *probabilistic* [9], $RKEP$ [13], *random pairwise key* [4], *closest pairwise key* [7]
		optimization design	$configuration/intersection$ [15]
		quorum based	*grid based* [6], $PIKE$ [12]
		grid based	*location based* [7], *location aware* [10], *deployment knowledge* [11], *hexagonal grid* [14], GKE [16]
	deployment knowledge	aware	*closest pairwise key/location based* [7], *location aware* [10], *deployment knowledge* [11], *hexagonal grid* [14], GKE [16]
		unaware	*basic protocol* [3], $q-composite/random\ pairwise\ key$ [4], $multi-space$ [5], *random subset/grid based* [6], *direct/cooperative* [8], *probabilistic* [9], $PIKE$ [12], $RKEP$ [13], $configuration/intersection$ [15], *multivariate* [17] [18]
pairwise key establishment	information area	within one hop	*basic protocol* [3], $q-composite$ [4], *random subset* [6], *closest pairwise key/location based* [7], *hexagonal grid* [14], *direct/cooperative* [8], $configuration$ [15], *multivariate* [17] [18]
		within multiple hops	*random pairwise key* [4], $multi-space$ [5], *probabilistic* [9], *location aware* [10], *deployment knowledge* [11]
		entire network	*grid based* [6], $PIKE$ [12], $RKEP$ [13], *intersection* [15], GKE [16]
	minimum number of shared keys on a usable link	1	all other protocols
		>1	$q-composite$ [4]
	maximum number of hops on one key path	1	*random pairwise key* [4], *direct* [8], *hexagonal grid* [14], $configuration$ [15]
		2	*grid based* [6], *closest pairwise key/location based* [7], *cooperative* [8], $PIKE$ [12], $RKEP$ [13], *intersection* [15]
		3	*location aware* [10], GKE [16]
		∞	*basic protocol* [3], $q-composite$ [4], $multi-space$ [5], *random subset* [6], *probabilistic* [9], *deployment knowledge* [11], *multivariate* [17] [18]

chosen randomly. Resilience is enhanced at the cost of poor connectivity in large scale networks under memory constraints. Works in [5] and [6] extend traditional crypto ideas in [21] and [22] respectively to distribute *key structures* (polynomials or matrix/vectors) instead of keys into sensors to enhance the resilience under low attack intensity.

The second feature is the method in pre-distributing keys. In the basic protocol [3], keys are distributed *randomly*. In [15], keys are distributed according to well known *optimization designs*, which helps increase chances of key sharing. In [6], *quorum based* methods are introduced to guarantee existence of a key path between any two nodes. In [7], nodes are deployed into *grids*, and keys distributed in non-adjacent grids are disjoint, while keys pre-distributed in adjacent grids have a certain degree of overlap. This enhances the chance that two nodes in adjacent grids share keys. The third feature is knowledge of deployment location. The basic *KP* protocol [3] does not assume nodes' deployment positions are known a priori. In works like [7], certain deployment knowledge is assumed to be known as a priori such that keys can be distributed based on location information to enhance chances of key sharing between neighboring nodes.

2) Enhancement in Pairwise Key Establishment Stage: The first feature we discuss in the pairwise key establishment stage is the information area of each node. In the basic protocol [3], each node is aware of the node/key information in its communication range. Thus the information area is within *one hop*. In [4], this feature is extended in that nodes are allowed to obtain node/key information in *multiple hops* to alleviate key path construction. In [6], nodes are even allowed to construct a key path using a proxy anywhere in the network. In effect, the information area in protocols becomes the *entire network*.

The second feature is the link usability on a key path. In most works, a link between two nodes is usable in key path construction as long as there is at least one shared key between those two nodes. However, in [4], $q-composite$ concept was introduced, which allows two neighboring nodes to use the link between them only if they share at least q keys. The resilience under low attack intensity (small value of P_c) is enhanced at the cost of lower resilience under higher attack intensity. The last feature is the number of hops allowed on a key path. In the basic protocol [3], a key

path can have arbitrary number of hops. However, in [4] [6] [10] etc., there are certain bounds on the maximum number of hops on a key path. Clearly this feature will affect the number of key paths constructed, and consequently affect the resilience of the pairwise keys established. More hops imply better chances of key establishment at the cost of increased communication/computation overhead and vice versa.

III. Derivation of Resilient Connectivity

In this section, we first introduce our security metric called *Resilient Connectivity* (RC), followed by its derivation. Before the derivation of RC, we identify and abstract all the parameters that impact RC in all KP protocols and list them in Table III. We then derive a general expression for RC incorporating these parameters to analyze *KP* protocols scalability. This generalizes our findings to all *KP* protocols.

A. Preliminaries

The traditional metrics to evaluate performance of *KP* protocols are *connectivity* and *resilience*. These two metrics are disjoint in that connectivity measures only the probability that physical neighbors can establish pairwise keys, irrespective of how secure these keys are from being disclosed by the attacker. Resilience measures only how secure the established pairwise keys between neighbors are from being disclosed by the attacker, irrespective of the probability of physical neighbors establishing pairwise keys between them. In order to quantify security performance, we combine the above two metrics and define a new one called *Resilient Connectivity* (RC). Formally, $RC = Connectivity \times Resilience$. There exists a strong physical meaning for RC, which is the probability that two physically neighboring sensors can communicate securely (with a *secure* pairwise key) under attacks. RC naturally encompasses both connectivity and resilience, and is our metric to evaluate the KP protocols scalability in terms of security performance.

We discussed various KP protocols in Section II. As discussed in Section II, since the core idea of all *KP* protocols follow two stages (key setup stage and pairwise key establishment stage), all their enhancements can be captured using certain parameters. We now introduce these parameters and derive their expressions. They will be used in our analysis later when we derive the expression of RC. Generalization of these parameters during RC derivation naturally generalizes our analysis to all *KP* protocols.

- *Key Setup Parameter ($P[E_i^{sk}], P_{dis}$)*: As described earlier, there are various natures in pre-distributed keys, such as, key structure distribution in [5] [6], unique pairwise key distribution in [4], optimization design based distribution in [15], and location aided key distribution in [7] [11]. They can all be captured by two parameters, $P[E_i^{sk}]$ and P_{dis}, which denote the probability that two neighboring sensors share exact i keys (or key structures), and the probability a single key (or key structure) is disclosed to the attacker respectively. The former captures the positive side of key redundancy in that it reflects the chance of direct key sharing and the chance of nearby proxies being helpful. The latter captures the negative side of key redundancy in that it reflects the chance that keys are disclosed by the attacker. In other words, two protocols with the same $P[E_i^{sk}]$ and P_{dis} will have the same security performance, irrespective of the nature of keys (or key structures) being pre-distributed.
- *Pairwise Key Establishment Parameters (A, H, q)*: The basic operation in pairwise key establishment is constructing key paths using the links with shared keys. Three parameters that naturally affect the security performance are: the amount of information obtained by each node for key paths construction, the longest key paths allowed to be constructed, and the minimum requirement for a link to be usable in key path construction. These three parameters can be captured by three parameters respectively: the size of information area (A), the maximum number of hops on one key path (H), and the minimum number of shared keys for a link to be usable (q). Large value of A or H makes more key paths available at the cost of communication/computation overhead. Large value of q achieves better resilience at low attack intensity at the cost of poorer resilience at high attack intensity [4].

In Table III, we show expressions of the above five parameters for various KP protocols. In Table III, *same grid*, *edge adj. grids* and *corner adj. grids* denote the case when two neighboring sensors are in the same grid, in two edge adjacent grids, and in two corner adjacent grids respectively. In Table III, l denotes the size of each grid, and $\mathcal{G}(N_1, N_2, p) = \sum_{i=N_2}^{N_1} \binom{N_1}{i} p^i (1-p)^{N_1-i}$, which is the probability that a key (or key structure) is disclosed where N_1 is the no. of captured nodes, N_2 is the minimum no. of captured nodes required for the key (or key structure) to be disclosed, and p is the probability that the key (or key structure) is distributed in a node. To summarize, we have identified and abstracted all parameters that impact RC in all *KP* protocols using the above five parameters. These parameters will be used in our analysis of RC in the next section. Since RC is our performance metric for scalability, our results can be generalized for *any KP* protocol by substituting appropriate expressions for these parameters for different protocols during the analysis.

Security being a critical topic has meant that there are still many works on key management in sensor networks following the idea of random key pre-distribution. Some recent optimizations include heterogenous sensor networks [23], [24], [25], mobile sensor networks [26], [27], [28], genetic algorithm based optimizations [29] etc. We believe that our analysis can be suitably extended to study the scalability of such optimizations as well.

B. Derivation of RC

We now discuss the derivation of RC for any general form of the above parameters. Certain other parameters, which are impacted by the parameters presented in Table III, will be used to derive RC and their notations are presented in Table IV. In our analysis, the attack model is the one discussed in Section II-A2. Table V gives the sequence of formulas in deriving RC. We present here a basic overview of the derivation process. A more detailed description is in the Appendix.

TABLE III
PARAMETERS OF KP PROTOCOLS THAT AFFECT RC

Protocols	$P[E_i^{sk}]$	P_{dis}	A	H	q
basic protocol [3]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	∞	1
q − composite [4]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	∞	≥ 1
random pairwise key [4]	$\begin{cases} 1-\frac{k}{N} & i=0 \\ \frac{k}{N} & i=1 \\ 0 & i>1 \end{cases}$	$1-\binom{N-2}{NP_c}/\binom{N}{NP_c}$	$\geq \pi r^2$	1	1
multi − space [5]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	$\geq \pi r^2$	∞	1
random subset [6]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	∞	1
grid based [6]	$\begin{cases} 1-\frac{2(\sqrt{N}-1)}{N-1} & i=0 \\ \frac{2(\sqrt{N}-1)}{N-1} & i=1 \\ 0 & i>1 \end{cases}$	$\mathcal{G}(2\sqrt{N}-1, \lambda+1, \frac{1}{\sqrt{N}})$	S	2	1
closest pairwise key [7]	$\begin{cases} \frac{r^2 k}{l^2 D} & i=1 \\ 1-\frac{r^2 k}{l^2 D} & i=0 \\ 0 & otherwise \end{cases}$	$1-\binom{N-2}{NP_c}/\binom{N}{NP_c}$	πr^2	2	1
location based [7]	$\begin{cases} \binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2 & same/edge\ adj.\ grid(s) \\ 0 & otherwise \end{cases}$	$\mathcal{G}(\frac{5P_c Dl^2}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	2	1
direct/cooperative [8]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	1, 2	1
probabilistic [9]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	$\geq \pi r^2$	∞	1
location aware [10]	$\begin{cases} \binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2 & same\ grid \\ \frac{8Dl^2}{\pi r^2} & edge/corner\ adj. \\ 0 & otherwise \end{cases}$	$1-\binom{N-2}{NP_c}/\binom{N}{NP_c}$	$9l^2$	3	1
deployment knowledge [11]	$\begin{cases} \binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2 & same\ grid \\ \frac{\sum_{j=0}^{k-i}\binom{aK}{i}\binom{aK-i}{j}\binom{(1-a)K}{k-i-j}\binom{K-i-j}{k-i}}{\binom{K}{k}^2} & edge\ adj. \\ \frac{\sum_{j=0}^{k-i}\binom{bK}{i}\binom{bK-i}{j}\binom{(1-b)K}{k-i-j}\binom{K-i-j}{k-i}}{\binom{K}{k}^2} & corner\ adj. \end{cases}$	$\mathcal{G}(\frac{2P_c Dl^2}{\pi r^2}, \lambda+1, \frac{k}{K})$	$9l^2$	∞	1
$PIKE$ [12]	$\begin{cases} 1-\frac{2(\sqrt{N}-1)}{N-1} & i=0 \\ \frac{2(\sqrt{N}-1)}{N-1} & i=1 \\ 0 & i>1 \end{cases}$	$1-\binom{N-2}{NP_c}/\binom{N}{NP_c}$	S	2	1
$RKEP$ [13]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	S	2	1
hexagonal grid [14]	*depend on grid shape, refer to* [14] *for details*	$\mathcal{G}(\frac{P_c DSg^n g}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	1	1
configuration [15]	$\begin{cases} 1 & i=1 \\ 0 & i\neq 1 \end{cases}$	$1-\binom{N-Nk/K}{N_c}/\binom{N}{N_c}$	πr^2	1	1
intersection [15]	$\begin{cases} \frac{k(Nk/K-1)}{N-1} & i=1 \\ 1-\frac{k(Nk/K-1)}{N-1} & i\neq 1 \end{cases}$	$1-\binom{N-Nk/K}{N_c}/\binom{N}{N_c}$	S	2	1
GKE [16]	$\begin{cases} 1 & i=1, same\ grid \\ \frac{k^2}{n_g^2} & i=1, different\ grids \\ 0 & i\neq 1 \end{cases}$	$1-\binom{N-2}{NP_c}/\binom{N}{NP_c}$	S	3	1
multivariate [17] [18]	$\binom{K}{i}\binom{K-i}{2(k-i)}\binom{2(k-i)}{k-i}/\binom{K}{k}^2$	$\mathcal{G}(\frac{P_c DS}{\pi r^2}, \lambda+1, \frac{k}{K})$	πr^2	∞	1

In Table V (1), $P[E_{\not\rightarrow}^A]$ is the probability that an arbitrary uncaptured node (say node a) cannot construct a secure key path to its uncaptured physical neighbor (say node b) within a's information area (A). $P[E_{\not\leftarrow}^A|E_{\not\rightarrow}^A]$ is the probability that uncaptured node b cannot construct a secure key path to uncaptured node a within b's information area given that node a cannot construct a secure key path to node b within a's information area (A). Consequently, $(1-P[E_{\not\rightarrow}^A]P[E_{\not\leftarrow}^A|E_{\not\rightarrow}^A])$ is the probability that two arbitrary uncaptured neighboring nodes a and b are able to construct a secure key path in between. This value, times the probability that nodes a and b are themselves not captured (i.e., $(1-P_c)^2$) is RC. A detailed description of the derivation can be found in the Appendix.

Remarks: Note that $RC = Connectivity \times Resilience$. While there have been prior works on analyzing connectivity [3], [5], no rigorous analysis on resilience has been conducted, except on the expected percent of disclosed pre-distributed keys. The difficulty is due to significant complexities in considering the nodes/keys overlaps among multiple key paths. In this paper, we have rigorously derived RC, and $Connectivity$ can be derived in the same way as RC by just substituting $P_c = 0$. If solely $Resilience$ is interested, it can naturally be analyzed via $Resilience = RC/Connectivity$. To the best of our knowledge, ours is the first work that enables *Resilience* of *KP* protocols to be analyzed.

IV. SCALING LAW ONE: SCALABILITY WITH RESPECT TO NODE DENSITY

A. The Scaling Law

We now present our first finding on the scalability of *KP* protocols with respect to node density in terms of RC. Based on the derivation of RC in Section III-B, we can treat RC as a function of node density D (denoted as $RC(D)$), given other parameters fixed. We now have the following theorem:

Theorem 1: For any KP protocol $(E_i^{sk}, P_{dis}, A, H, q)$, network parameters (S, r) , attack intensity $(P_c > 0)$, (1) $\exists D_1, D_2 : D_1, D_2 \in (0, +\infty), D_1 > D_2 : RC(D_1) < RC(D_2)$; (2) $lim_{D\to+\infty} RC(D) = 0$ (Proof in [30]).

TABLE V
RC DERIVATION FORMULAS

$$RC = (1-P_c)^2(1-P[E^A_{\not\rightarrow}]P[E^A_{\not\leftarrow}|E^A_{\not\rightarrow}]), \quad (1)$$

where

$$P[E^A_{\not\rightarrow}] = 1 - P[E^A_{\rightarrow}] = 1 - \sum_{i=1}^{H} P[E^A_{\rightarrow i}], \quad (2)$$

$$P[E^A_{\not\leftarrow}|E^A_{\not\rightarrow}] = 1 - \frac{\sum_{i=1}^{H} P[E^A_{\rightarrow i}] - \sum_{i=1}^{H} P[E^{A_o}_{\rightarrow i}]}{1-\sum_{i=1}^{H} P[E^{A_o}_{\rightarrow i}]}, \quad (3)$$

$$P[E^A_{\rightarrow 1}] = 1 - \sum_{i=0}^{k} \Big(P[E_i^{sk}]P[E_i^{dis}] \Big), \quad (4)$$

$$P[E^A_{\rightarrow 2}] = (1 - P[E^A_{\rightarrow 1}]) \sum_{N_c=0}^{N-2} \Big[\mathcal{F}(N-2, N_c, \tfrac{A}{S}) \sum_{n_1=1}^{N_c} \Big(\mathcal{F}(N_c, n_1, P_1) P_2(n_1) \Big) \Big], \quad (5)$$

$$P[E^A_{\rightarrow i}] = (1 - P[E^A_{\rightarrow 1}]) \sum_{N_c=0}^{N-2} \Big[\mathcal{F}(N-2, N_c, \tfrac{A}{S}) \sum_{n_1=1}^{N_c-i+2} \Big(\mathcal{F}(N_c, n_1, P_1)(1 - \tfrac{A_o}{A} P[E^A_{\rightarrow 1}])^{n_1} \mathcal{H}(i-1, N_c, n_1) \Big) \Big] \quad (i > 2) \quad (6)$$

$$P[E_i^{dis}] = \begin{cases} 1 & i < q \\ \sum_{m=i}^{K} \mathcal{F}(K, m, P_{dis}) \binom{m}{i} / \binom{K}{i} & i \geq q \end{cases}, \quad (7)$$

$$\mathcal{F}(N_1, N_2, p) = \binom{N_1}{N_2} p^{N_2} (1-p)^{N_1 - N_2}, \quad (8)$$

$$\mathcal{H}(i-j, N_c, n_1, n_2, \cdots, n_j) = \sum_{n_{j+1}=1}^{n_{j+1}^{max}} P_3(n_{j+1}) \mathcal{H}(i-j-1, N_c, n_1, \cdots, n_{j+1}), \quad \text{for } 1 \leq j \leq i-2, \quad (9)$$

$$\mathcal{H}(1, N_c, n_1, \cdots, n_{i-1}) = 1 - (1 - A_o P[E^A_{\rightarrow 1}]/A)^{n_{i-1}}, \quad (10)$$

$$P_1 = P[E^A_{\rightarrow 1}](1 - P_c), \quad (11)$$

$$P_2(n_1) = 1 - (1 - A_o P[E^A_{\rightarrow 1}]/A)^{n_1}, \quad (12)$$

$$P_3(n_i) = \mathcal{F}(N_c - \sum_{j=1}^{i-1} n_j, n_i, 1 - (1 - A_o P[E^A_{\rightarrow 1}]/A)^{n_{i-1}})(1 - A_o P[E^A_{\rightarrow 1}]/A)^{n_i}. \quad (13)$$

TABLE IV
NOTATIONS FOR *RC* DERIVATION

RC	Resilient Connectivity
E_i^{sk}	The event that two nodes share i keys (key structures)
P_{dis}	The probability that a key (key structure) is disclosed
A	The size of information area for a node
A_o	The expected overlapping area created by two information areas of two neighboring nodes, $A_o = 0.5865A$ [4] when A is a disk
H	The maximum number of hops allowed on one key path
q	The minimum number of shared keys for a usable link
$E^A_{\rightarrow}$	The event that, given two uncaptured neighboring nodes a and b, node a can construct one secure key path to node b with all proxies in a's information area A. $E^A_{\not\rightarrow}$ denotes its negative
$E^A_{\leftarrow}$	The event that, given two uncaptured neighboring nodes a and b, node b can construct one secure key path to node a with all proxies in b's information area A. $E^A_{\not\leftarrow}$ denotes its negative
$E^A_{\rightarrow i}$	The event that, given two uncaptured neighboring nodes a and b, node a can construct one secure key path to node b with minimum hops i with all proxies in a's information area A
E_i^{dis}	The event that all i shared keys (key structures) between two nodes are disclosed to the attacker
$P[E]$	Probability of occurrence of event E

The first part of Theorem 1 states that for any non-zero node capture probability P_c, performance of KP protocols does not always increase with node density D. There exists densities D_1 and D_2, where RC at a smaller node density is higher than RC at larger node density for any protocol and network parameters. The second part of the theorem further states that $RC \to 0$ when $D \to \infty$. It implies there is a finite value of node density D to achieve optimal performance for any KP protocol. To conclude, KP protocols are not scalable with respect to node density in terms of security. Based on the theorem above, we have the first scaling law for *KP* protocols.

Scaling Law 1: **KP protocols are not scalable in terms of RC with respect to node density.**

The fundamental explanation for the unscalability of *KP* protocols stems from *redundancy* in key pre-distribution inherent in all *KP* protocols, and the presence of attacks. Each sensor is provisioned with multiple keys, and each key is usually shared by multiple sensors. Clearly, redundancy helps the network side overcome deployment randomness to discover more secure neighbors and proxies. However, this redundancy can be a double-edged sword. Attackers can also leverage redundancy to disclose more keys and communications. This redundancy is further amplified when node density increases. When the node density (D) increases, the number of nodes (N) and the number of captured nodes (N_c) increase. We can then show that $P_{dis} \to 1$ (from the expressions for P_{dis} in Table III) when number of captured nodes increases. When $P_{dis} \to 1$, we can see from equation (7) in Table V that $P[E_i^{dis}] \to 1$. Thus from equations (2) to (6), we can see that $RC \to 0$. This conclusion holds for all KP schemes since all the expressions of P_{dis} in Table III approach 1 when one of the three parameters (D, N, N_c) approaches infinity. As pointed above, this is due to redundancy in key pre-distribution, which when amplified, causes degradation in RC.

B. Numerical Results

In the following, we conduct extensive numerical studies on the sensitivity of resilient connectivity (RC) to node density (D) for different protocol variants under varying node capture probabilities (P_c), number of keys (k, K), maximum number of hops allowed in a key path (H), key structure degree (λ) and probability of key sharing ($P[E_i^{sk}]$). Furthermore, we also demonstrate the soundness of our analysis by comparing its fidelity with simulation data. Unless otherwise stated, the following are default values: $D = 15$, $S = 1000m \times 1000m$, $r = 10m$, $P_c = 0.005$, $k = 100$, $K = 30000$, $\lambda = 0$, $A = \pi r^2$, $H = \infty$, $q = 1$. By default, keys are pre-distributed randomly [3] without deployment knowledge.

The first observation we make from Figs. 2 to 5 is that RC does not monotonically increase with D. Secondly, in all figures there is a particular point in density, beyond which RC monotonically decreases. We denote this D as density threshold D_{th}. In fact, D_{th} indicates the critical point at which the attacker defeats the network in the tug of war between

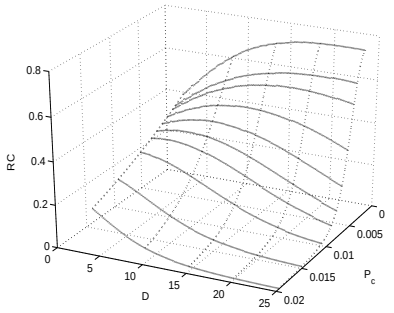

Fig. 2. RC vs. D under different P_c

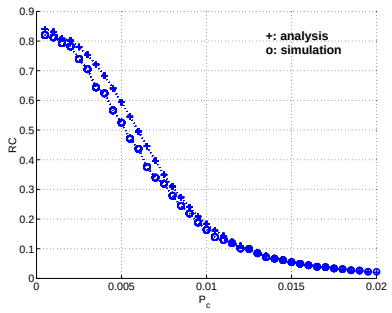

Fig. 3. Comparison of analysis and simulation data

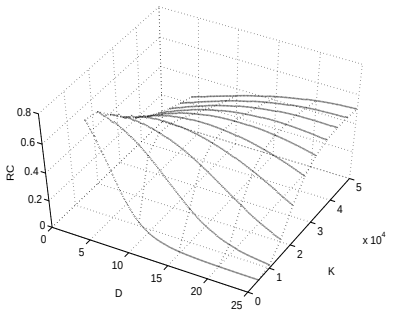

Fig. 4. RC vs. D under different K

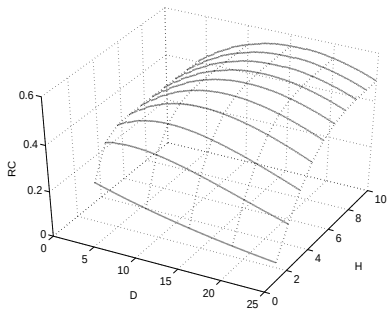

Fig. 5. RC vs. D under different H

them (discussed above) in terms of redundancy exploitation. As we discuss below, the result of this war (D_{th}) is different for different protocols and parameters.

In Fig. 2, we study RC vs. D under different P_c. When P_c is large, RC decreases from lower values in density (smaller D_{th}). This is because a large P_c means a powerful attacker. Increasing density means the attacker can capture more nodes and disclose more keys. Consequently D_{th} is low (near $zero$) when P_c is large. However, when P_c decreases it implies a moderate attacker. Increasing density (up to a point) will better facilitate the network side, and D_{th} thus increases. For example, when $P_c = 0.005$, RC increases up to $D_{th} = 15$ before decreasing. When P_c decreases further, D_{th} increases. To demonstrate the soundness of our analysis, we report data comparing numerical and simulation data for the case of RC vs. P_c in Fig. 3 (other parameters are default). As we can see, the numerical data match very well with simulation data. We note that simulation data are lower than analysis data due to network boundary effect.

In Figs. 4 and 5, we study RC vs. D under different K and H. When K and H are small, D_{th} is small. This is once again because attack impacts are stronger than network benefits leading to more pairwise keys disclosed under smaller K (key pool size) and smaller H (number of hops) even at low densities. Increasing density further will better facilitate the attacker. When K and H are large, the attacker effectiveness decreases, which increases D_{th}. We point out that there is a relationship between K and k from the perspective of key disclosure. A small k means fewer keys are disclosed per node capture and vice versa. This effect is opposite to that of K. The trend is: when k is small D_{th} is large, and when k is large D_{th} is small. Note however that RC increases with K for a fixed value of D upto a certain point only. Beyond a certain value of K, RC starts to decrease for any given D, as connectivity starts going down significantly.

Note that, we used the basic communication model here, where the sensor's communication range is a circular disc. In [30], we conduct further investigations on RC vs. D under irregular communication models like Degree of Irregularity (DOI) model [31]. We observe that all our findings and trends still hold true. Interested readers may refer to [30].

C. Discussions

We wish to emphasize here an important observation from the above figures. Note that RC monotonically increases upto D_{th}, after which it monotonically decreases in all figures. Towards this extent, we state the following conjecture:

Conjecture: For any KP protocol $(E_i^{sk}, P_{dis}, A, H, q)$, any network parameters (S, r) and any attack intensity $(P_c > 0)$, (1) there is one and only $D_{th} \in (0, +\infty)$ where RC is maximum; (2) $\forall D_1, D_2 : D_1 < D_2 < D_{th} : RC(D_1) < RC(D_2)$; (3) $\forall D_1, D_2 : D_1 > D_2 > D_{th} : RC(D_1) < RC(D_2)$.

A rigorous proof of this conjecture is still open. Here we provide an informal argument. An increase in node density will be leveraged by both network and attacker. From the perspective of RC, it means improved connectivity or decreased resilience respectively. The overall impact to RC is contingent on which factor dominates this tug of war. Initially, increase in node density improves connectivity significantly, which increases RC. Considering there is an upper bound on connectivity in the network (at most one), there is a point from which resilience degradation always dominates with increase

in density, resulting in the density threshold (D_{th}) from which RC monotonically decreases. However as our data show, D_{th} itself is sensitive to the protocol, attack and network parameters. Given all the parameters, we are able to determine the optimal node density to achieve maximum RC based on our analysis in Section III-B.

V. Scaling Law Two: Scalability with respect to Network Dimension

A. The Scaling Law

Based on our earlier derivation of RC in Section III-B, we see that RC is dependent on network dimension S. In the following, we denote $RC(S)$ as resilient connectivity for a network with dimension S, with other parameters fixed. We now have the following theorem:

Theorem 2: For any KP protocol $(E_i^{sk}, P_{dis}, A, H, q)$, network parameters (D, r), attack intensity $(P_c > 0)$, (1) $\forall S_1, S_2 : S_1 > S_2, RC(S_1) < RC(S_2)$; (2) $lim_{S\to+\infty} RC(S) = 0$ (Proof in [30]).

Theorem 2 states that for any non-zero node capture probability P_c, performance monotonically decreases (to 0) as network dimension increases for any protocol and network parameters. This demonstrates the unscalability of ***KP*** protocols in terms of security performance with respect to network dimension. Based on the theorem above, we have the second scaling law for ***KP*** protocols.

Scaling Law 2: **KP protocols are not scalable in terms of RC with respect to network dimension.**

When network dimension increases, the number of nodes increases. This increases the redundancy in key sharing among nodes leveraged by the attacker, which is the fundamental reason for the unscalability of KP protocols with respect to network dimension. Specifically, when the network dimension (S) increases, the number of nodes (N) and the number of captured nodes (N_c) increase. Similar to the discussions in Section IV, $P_{dis} \to 1$ when the number of captured nodes increases. This further results in the fact that $P[E_i^{dis}] \to 1$ and $RC \to 0$. This conclusion holds for all KP schemes since all the expressions of P_{dis} in Table III approach 1 when one of the three parameters (S, N, N_c) approaches infinity.

B. Numerical Results

In the following, we conduct a numerical study on the sensitivity of resilient connectivity (RC) to network dimension ($S = L \times L$) under different density D. Other parameters are set as default. In Fig. 6, we observe that RC monotonically decreases as L increases for all D. We also see that density threshold D_{th} (discussed earlier) decreases as L increases. This is because when network dimension is larger, more nodes are captured, resulting in more powerful attack impacts (even at low densities). Consequently RC decreases from an early D_{th} as L increases and vice versa.

Due to space limitation, we do not show the sensitivity of RC to L under other network parameters (e.g., P_c, K, k and H). Basically, the impact of the above network parameters on RC here is similar to that we discussed in Section IV.

VI. Group Deployment

In this section, we propose two types of group deployment, that are, *logical* group deployment and *physical* group deployment, to deal with the un-scalability of ***KP*** protocols with respect to node density and network dimension respectively.

A. Logical Group Deployment

As we discussed in Section IV, high node density could result in security degradation in ***KP*** protocols. This is because given network dimension, average number of captured nodes increases with node density. As more nodes become captured, the attacker can compromise a larger percentage of pre-distributed keys and compromise secure communications in the network to a larger extent. Clearly decreasing node density is helpful. Unfortunately, high node density is required in many applications for sensing and connectivity under faults/ failures.

Intuitively, it seems a dilemma to achieve high security performance in WSNs requiring high node density. However, the above two factors do not necessarily contradict with each other. High node density hurts secure communications not because there are too many nodes in a unit area, but because there are too many nodes in a unit area *whose pre-distributed keys come from a single key pool*. If we maintain the number of nodes in a unit area, while decreasing the number of nodes sharing a single key pool in a unit area, we can achieve both high security and high performance simultaneously.

In this paper, we propose *logical* group deployment to achieve high node density without sacrificing secure communications. In particular, we deploy sensor nodes in multiple rounds. In each round, certain number of sensors are deployed to the whole network, and these sensors are pre-distributed with keys from the same key pool. On the other hand, sensors deployed in different rounds are pre-distributed with keys from disjoint key pools. In other words, sensors are deployed in multiple logical groups, any two of which share no pre-distributed keys. By deploying nodes in this way, we can achieve arbitrarily high node density (with multiple rounds), while at the same time achieve high security as security is decided by the node density in a single round.

Our logical group deployment resolves the dilemma between high node density and high security at the cost of two nodes in different rounds not being able to communicate with each other. This is because sensors in different rounds use disjoint key pools, and cannot establish a pair-wise key in between. However, this will not be an issue as long as the node density determined by each round is high enough to achieve node connectivity within each round with high probability. In many applications, a sensor does not need to communicate with *all* its neighbors. It suffices if each node can communicate with a few neighbors to achieve connectivity and redundancy. However, in the case of low density in the network (due to maybe faults/ failures), or if the base-station desires collaboration between nodes in multiple rounds, we can extend our logical group deployment to let any two key pools in two different groups to have a small percentage of overlap (e.g., 20%) so that sensors in different groups can still

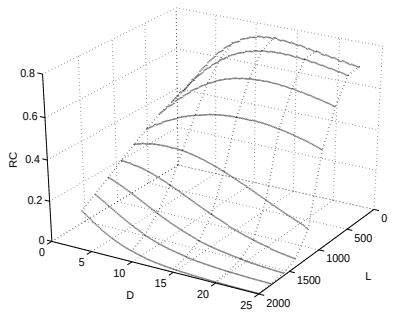

Fig. 6. RC vs. L under different D

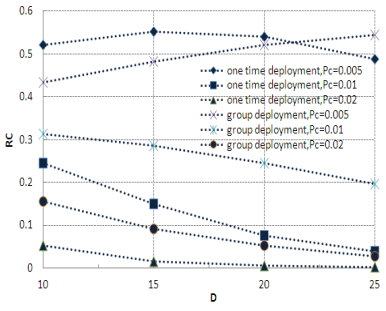

Fig. 7. RC vs. D under logical group deployment with different P_c

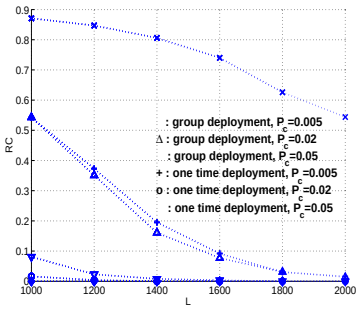

Fig. 8. RC vs. L under physical group deployment with different P_c

establish pair-wise keys in between. The overlap is small so that security will not be compromised much. In some sense, the latter technique actually sets K to a very high value, which as argued above improves RC when node density increases.

In Fig. 7, we study the sensitivity of RC to node density (D) under different P_c for *KP* protocols for traditional one time deployment and our logical group deployment. The node density decided by all sensor nodes is D, and other parameters are set as default. Under logical group deployment, we divide sensors in two rounds with the same size, and the two key pools in two rounds are disjoint. We can see that when node density is high, RC is better in logical group deployment compared to that of traditional one time deployment, especially when node capture probability is high. However, when node density is low, RC in logical group deployment may even be worse than that in traditional one time deployment, especially when node capture probability is low. This is because under low node capture probability, the threshold density is high. RC increases with node density, in which case logical group deployment should not be used. To sum up, our logical group deployment helps to enhance security performance when node density is high. This also justifies that the adoption of our logical group deployment under high node density will not hurt connectivity much as node density in each round is still high enough.

B. Physical Group Deployment

As we discussed in Section V, large network dimension could result in security degradation in *KP* protocols. This is because given node density, the average number of captured nodes increases with the network dimension. The more nodes become captured, the larger percentage of pre-distributed keys the attacker can compromise and to a larger extent the attacker can compromise the secure communications in the network. Decreasing network dimension certainly helps, however, many sensor networks are envisaged to be deployed in large area, such as the battlefields or international borders.

Intuitively, it seems to be difficult to achieve high security performance in sensor networks with large network dimension. However, the above two factors do not necessarily contradict with each other either. Large network dimension hurts secure communications not simply because there are too many nodes in the whole network, but because there are too many nodes in the network *whose pre-distributed keys come from a single key pool*. If we can maintain the total number of nodes in the network, while decreasing the number of nodes sharing a single key pool in the network, we are able to achieve both high security and large network dimension simultaneously.

In this paper, we propose *physical* group deployment to achieve large network dimension without sacrificing secure communications. In particular, we deploy sensor nodes in multiple groups. In each group, certain number of sensors are deployed to a specific area of the network, and these sensors are pre-distributed with keys from the same key pool. On the other hand, sensors in different groups are deployed in different areas of the network, and are pre-distributed with keys from partially overlapped or disjoint key pools. A simple example is first dividing the network into multiple disjoint grids, and then deploying one group of sensors in each grid. By deploying nodes in this way, we can achieve arbitrarily large network dimension (with multiple groups), while at the same time achieve high security as security is mainly decided by the dimension of a single group [3].

In our physical group deployment, we assume the knowledge as to which sensor belongs to which group is known as a priori, which is a common assumption in KP protocols [11] [32]. Sensors in adjacent groups share different key pools with limited overlap to facilitate neighbor group communications, while key pools of non-adjacent groups share no overlap. To derive RC under group deployment for general KP protocols, we point out that there are two types of relationships between two adjacent groups, i.e., edge adjacent or corner adjacent. The derivation of RC under group deployment thus has to consider the key pool overlaps between adjacent edges, which is not the case in traditional one time random deployment discussed in Section III. The derivations of RC under group deployment are not presented here due to space limitation. Interested readers may refer to [30] for derivations.

In Fig. 8, we study the sensitivity of RC to network dimension (L) under different P_c for *KP* protocols for traditional one time deployment and our physical group deployment. The

[3]Note that, an overlap of keys among physically neighboring groups is not mandatory in applications involving mobile base stations or even multiple base stations, as long as sensors in one group can communicate with a base-station without the aid of neighboring groups. In this case, RC will only improve further.

overall network dimension is $L \times L$. Under physical group deployment, we divide the network into four groups, each has dimension $L_{grid} = L/2$. By default, we set the percent of key overlaps among edge adjacent and corner adjacent grids as $\alpha = 0.20$ and $\beta = 0.05$ respectively (as in [11]). We see that RC is consistently better in physical group deployment compared to that of traditional one time deployment. Thus, physical group deployment always helps enhance security, which is a little different from the case in logical group deployment we discussed above.

Summary: To summarize, our strategies for logical and physical group deployment alleviate concerns on decreasing RC with increasing node density and network dimension. For a given set of parameters, when it may be impossible to increase RC beyond a point for flat (or homogeneous) deployments, our group deployment strategies can improve RC. Note that increase in RC in group deployment has application level constraints like no. of groups, no. of nodes in each group, no. of keys in each group and overhead. Under such constraints our analysis can help deployers make informed decisions on RC increase, and managing constraints imposed by the network, its operation and overhead.

VII. Final Remarks

In this paper, we conducted an investigation on scalability of key pre-distribution (*KP*) protocols in randomly deployed WSNs. We find that *KP* protocols are not scalable in terms of security performance, due to redundancy in key distribution. The significances of our work also extend to other network systems that utilize redundancy. In secure overlay forwarding systems [33], while redundancy in system connectivity enables clients to find more paths to the server, attackers can leverage high connectivity to disclose the server rapidly (and attack it). For file sharing systems [34], while content replication enhances load sharing, it can be exploited to disrupt system quality by corrupting popular files. Our work here can be extended to such systems to understand their tradeoffs and provision resources carefully.

References

[1] D. J. Malan, M. Welsh, and M. D. Smith, "A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography," in *Proceedings of 1st IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, October 2004.

[2] A. S. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, "Energy analysis of public-key cryptography for wireless sensor networks," in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom)*, March 2005.

[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS)*, November 2002.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proceedings of IEEE Symposium on Research in Security and Privacy*, May 2003.

[5] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, October 2003.

[6] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS)*, October 2003.

[7] ——, "Location-based pairwise key establishments for relatively static sensor networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, October 2003.

[8] R. D. Pietro, L. V. Mancini, and A. Mei, "Random key-assignment for secure wireless sensor networks," in *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, October 2003.

[9] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: a probabilistic approach," in *Proceedings of the 11th IEEE International Conference on Network Protocols (ICNP)*, November 2003.

[10] D. Huang, M. Mehta, D. Medhi, and L. Harn, "Location-aware key management scheme for wireless sensor networks," in *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, October 2004.

[11] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proceedings of the 23rd IEEE Conference on Computer Communications (INFOCOM)*, March 2004.

[12] H. Chan and A. Perrig, "Pike: peer intermediaries for key establishment," in *Proceedings of the 24th IEEE Conference on Computer Communications (INFOCOM)*, March 2005.

[13] A. Wacker, M. Knoll, T. Heiber, and K. Rothermel, "A new approach for establishing pairwise keys for securing wireless sensor networks," in *Proceedings of the 3rd ACM Conference on Embedded Networked Sensor Systems (Sensys)*, November 2005.

[14] Z. Yu and Y. Guan, "A key pre-distribution scheme using deployment knowledge for wireless sensor networks," in *Proceedings of the 4th International Conference on Information Processing in Sensor Networks (IPSN)*, April 2005.

[15] J. Lee and D. R. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks," in *Proceedings of IEEE Wireless Communications and Networking Conference (WCNC)*, March 2005.

[16] L. Zhou, J. Ni, and C. V. Ravishankar, "Efficient key establishment for group-based wireless sensor deployments," in *Proceedings of ACM Workshop on Wireless Security (WiSe)*, September 2005.

[17] F. Delgosha and F. Fekri, "Key predistribution in wireless sensor networks using multivariate polynomials," in *Proceedings of the 2nd IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks (SECON)*, September 2005.

[18] ——, "Threshold key-establishment in distributed sensor networks using a multivariate scheme," in *Proceedings of the 25th IEEE Conference on Computer Communications (INFOCOM)*, April 2006.

[19] K. Ren, W. Lou, and Y. Zhang, "Leds: Providing location-aware end-to-end data security in wireless sensor networks," in *Proceedings of the 25th IEEE Conference on Computer Communications (INFOCOM)*, April 2006.

[20] J. Spencer, *The Strange Logic of Random Graphs, Algorithms and Combinatorics 22*. Springer-Verlag, 2000.

[21] R. Blom, "An optimal class of symmetric key generation systems," *Advances in Cryptology: Proceedings of EUROCRYPT'84 (Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, eds.), LNCS 209*, pp. 335-338, 1985.

[22] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," *Advances in Cryptology (CRYPTO'92) LNCS 740*, pp. 471-486, 1993.

[23] A. Poornima and B. Amberker, "Key Management Schemes for Secure Communication in Heterogeneous Sensor Networks," in *International Journal of Recent Trends in Engineering*, 2009.

[24] Y. Zhang, W. Yang, K. Kim, and M. Park, "An AVL Tree-Based Dynamic Key Management in Hierarchical Wireless Sensor Network," in *International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP)*, 2008, pp. 298–303.

[25] T. Landstra, M. Zawodniok, and S. Jagannathan, "Energy-efficient hybrid key management protocol for wireless sensor networks," in *IEEE Conference on Local Computer Networks (LCN)*, 2007.

[26] S. Choi, V. Sarangan, and S. Trost, "Key management in wireless sensor networks with inter-network sensor roaming," in *33rd IEEE Conference on Local Computer Networks (LCN)*, 2008.

[27] K. Kifayat, M. Merabti, Q. Shi, and D. Llewellyn-Jones, "Group-based key management for Mobile Sensor Networks," in *IEEE Sarnoff Symposium*, 2010, pp. 1–5.

[28] Y. Lee and S. Lee, "A New Efficient Key Management Protocol for Wireless Sensor and Actor Networks," *Arxiv preprint arXiv:0912.0580*, 2009.

[29] C. Wang, T. Hong, G. Horng, and W. Wang, "A ga-based key-management scheme in hierarchical wireless sensor networks," in *International Journal of Innovative Computing, Information and Control*, 2008.

[30] W. Gu, X. Bai, and S. Chellappan, "Scaling laws of key pre-distribution protocols in wireless sensor networks," http://web.mst.edu/∼chellaps/papers/11ScalingLawTRSub.pdf, Tech. Rep., January 2011.

[31] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. F. Abdelzaher, "Range-free localization schemes for large scale sensor networks," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (Mobicom)*, September 2003.

[32] D. Liu, P. Ning, and W. Du, "Group-based key pre-distribution in wireless sensor networks," in *Proceedings of ACM Workshop on Wireless Security (WiSe)*, September 2005.

[33] A. D. Keromytis, V. Misra, and D. Rubenstein, "Sos: secure overlay services," in *Proceedings of the 20th Special Interest Group on Data Communications (SIGCOMM)*, August 2002.

[34] S. Rhea, B. Godfrey, B. Karp, J. Kubiatowicz, S. Ratnasamy, S. Shenker, I. Stoica, and H. Yu, "Opendht: A public dht service and its uses," in *Proceedings of the ACM Special Interest Group on Data Communications (SIGCOMM)*, 2005.

APPENDIX

Theoretical Derivation for RC: From Table V, we have, $RC = (1-P_c)^2(1-P[E^A_{\not\rightarrow}]P[E^A_{\not\leftarrow}|E^A_{\not\rightarrow}])$, where $P[E^A_{\not\rightarrow}]$ is the probability that an arbitrary node (node a) cannot construct a secure key path to its physical neighbor (node b) within a's communication disk (A). $P[E^A_{\not\leftarrow}|E^A_{\not\rightarrow}]$ is the probability that given two uncaptured neighboring nodes a and b, node b cannot construct a secure key path to node a with all proxies in b's information area A given that node a cannot construct a secure key path to node b with all proxies in a's information area A. We introduce a new term, $P[E^{A_o}_{\rightarrow}]$, which is the probability that node a can construct a secure key path to node b with all proxies along the path within the overlapping communication disks (A_o) of these two nodes. We have $P[E^A_{\not\leftarrow}|E^A_{\not\rightarrow}] = P[E^A_{\not\leftarrow}|E^{A_o}_{\not\rightarrow}]$. We first derive $P[E^A_{\not\rightarrow}]$. We have $P[E^A_{\not\rightarrow}] = 1 - P[E^A_{\rightarrow}]$. Based on definition of $E^A_{\rightarrow i}$, we have the expression in Table V (2).

We now derive $P[E^A_{\not\leftarrow}|E^{A_o}_{\not\rightarrow}]$. We have $P[E^A_{\not\leftarrow}|E^{A_o}_{\not\rightarrow}] = 1 - P[E^A_{\leftarrow}|E^{A_o}_{\not\rightarrow}] = 1 - P[E^A_{\rightarrow}|E^{A_o}_{\not\rightarrow}]$. By Bayer's Theorem, $P[E^A_{\rightarrow}]$ can be represented as $P[E^A_{\rightarrow}] = P[E^{A_o}_{\rightarrow}]P[E^A_{\rightarrow}|E^{A_o}_{\rightarrow}] + P[E^{A_o}_{\not\rightarrow}]P[E^A_{\rightarrow}|E^{A_o}_{\not\rightarrow}]$, where $P[E^{A_o}_{\rightarrow}] = \sum_{i=1}^{H} P[E^{A_o}_{\rightarrow i}]$ and $P[E^A_{\rightarrow}|E^{A_o}_{\rightarrow}] = 1$ (A_o is a subset of A). We then obtain the expression in Table V (3). Now we derive $P[E^A_{\rightarrow i}]$ and $P[E^{A_o}_{\rightarrow i}]$. Recall that $P[E^A_{\rightarrow i}]$ is the probability that node a can construct a secure key path to a physical neighbor node b within communication disk of node a with minimum hops i given both nodes a and b are uncaptured. The expression for this when $i = 1$ is given by Table V (4). Note that $P[E^{sk}_i]$ is given in Table III and $P[E^{dis}_i]$ is given in Table V (7) , where P_{dis} is given in Table III.

The probability that, given two nodes within the communication disk of node a, denoted as nodes b and c, node b is a physical neighbor of node c and node b shares at least one pre-distributed key with node c, is $A_o P[E^A_{\rightarrow 1}]/A$. This will be used in deriving $P[E^A_{\rightarrow i}]$ $(i > 1)$ below. To derive $P[E^A_{\rightarrow i}]$ $(i > 1)$, we divide nodes in the communication disk of node a (except nodes a and b) into disjoint groups $G(a, j)$ $(j \geq 1)$. A node s is in group $G(a, j)$ if node a can construct a secure key path from itself to node s within the communication disk of node a with minimum j hops. We first derive $P[E^A_{\rightarrow 2}]$. Considering there are $N-2$ other nodes in the network excluding nodes a and b, the probability that there are N_c nodes, excluding node b, in the communication disk of node a is $\mathcal{F}(N-2, N_c, A/S)$. Here $\mathcal{F}(N_1, N_2, p) = \binom{N_1}{N_2} p^{N_2}(1-p)^{N_1-N_2}$ in Table V (8) is the probability that there are N_2 out of total N_1 nodes in the communication disk of a node a given that p is the probability that a node in the network falls in the communication disk of the node a. Notice N_c is the number of physical neighbors, excluding node b, of node a. Given N_c nodes in the communication disk of node a, the probability that there are n_1 $(1 \leq n_1 \leq N_c)$ uncaptured nodes in $G(a, 1)$ is $\mathcal{F}(N_c, n_1, P_1)$, in which P_1 denotes $P[E^A_{\rightarrow 1}](1 - P_c)$ (Table V (11)). The probability that at least one of these n_1 nodes shares key with node b and is a physical neighbor of node b is $1-(1-A_o P[E^A_{\rightarrow 1}]/A)^{n_1}$, which is denoted as $P_2(n_1)$ in Table V (12). Hence, we have the expression in Table V (5).

We now analyze $P[E^A_{\rightarrow i}]$ for $i > 2$. Given N_c nodes in communication disk of node a, excluding node b, the probability that there are n_1 $(1 \leq n_1 \leq N_c - (i-2))$ uncaptured nodes in $G(a, 1)$ is $\mathcal{F}(N_c, n_1, P_1)(1-A_o P[E^A_{\rightarrow 1}]/A)^{n_1}$. Notice there is at least one uncaptured node in $G(a, j)$ $(2 \leq j \leq i-1)$, so n_1 can be $N_c - (i-2)$ at most. Besides there is no secure key path between nodes a and b within communication disk of node a with fewer than i hops. We denote $\mathcal{H}(i-j, N_c, n_1, \cdots, n_j)$ $(1 \leq j \leq i-1)$ as the probability that there is at least one secure key path from a node in $G(a, j)$ to node b with minimum hops $i-j$, given N_c nodes excluding node b in communication disk of node a and n_l nodes in $G(a, l)$ $(1 \leq l \leq j)$. Then we obtain the expression in Table V (6).

The expression of $\mathcal{H}(i-j, N_c, n_1, \cdots, n_j)$ $(1 \leq j \leq i-1)$ can be derived iteratively. Given n_j $(1 \leq j \leq i-1)$ nodes in $G(a, j)$ $(1 \leq j \leq i-1)$, the number of nodes in $G(a, j+1)$ is at most $N_c - \sum_{l=1}^{j} n_l - (i-j-2)$, denoted by n^{max}_{j+1}. Notice that, the probability there are n_i uncaptured nodes in $G(a, i)$ is in Table V (13). Thus, the probability that there is at least one secure key path from a node in $G(a, j)$ to node b with minimum hops $i-j$, given N_c nodes excluding node b in the communication disk of node a and n_l $(1 \leq l \leq j)$ nodes in $G(a, l)$ $(1 \leq l \leq j)$, is given in Table V (9).

According to the definition, $\mathcal{H}(1, N_c, n_1, \cdots, n_{i-1})$ is the probability that there is at least one secure key path from a node in $G(a, i-1)$ to node b with minimum hop 1, given N_c nodes excluding node b in the communication disk of node a and n_j $(1 \leq j \leq i-1)$ nodes in $G(a, j)$ $(1 \leq j \leq i-1)$. This is also the probability that at least one node in $G(a, i-1)$ shares a key with node b and is a physical neighbor of node b. Therefore, we have the expression in Table V (10). We now derive $P[E^{A_o}_{\rightarrow i}]$. Recall that $P[E^{A_o}_{\rightarrow i}]$ is the probability that a node can construct a secure key path to a physical neighbor node within the overlapped communication disks of both nodes, with minimum of i hops given both nodes are uncaptured. Consequently, instead of considering the total communication disk A, we only need to consider the overlapped area A_o , where $A_o = 0.5865A$ [4]. The derivation of $P[E^{A_o}_{\rightarrow i}]$ thus is the same as that for $P[E^A_{\rightarrow i}]$ except that we replace A by A_o . By substituting $P[E^A_{\rightarrow i}]$ and $P[E^{A_o}_{\rightarrow i}]$ into Table V (2) and V (3), we can obtain $P[E^A_{\not\rightarrow}]$ and $P[E^A_{\not\leftarrow}|E^A_{\not\rightarrow}]$, hence arriving at the closed form expression for RC in Table V (1).