Expander Graph based Key Distribution Mechanisms in Wireless Sensor Networks

Seyit Ahmet Çamtepe
Computer Science Department
Rensselaer Polytechnic Institute
Troy, New York 12180
Email: camtes@cs.rpi.edu

Bülent Yener
Computer Science Department
Rensselaer Polytechnic Institute
Troy, New York 12180
Email: yener@cs.rpi.edu

Moti Yung
RSA Laboratories and
Computer Science Department
Columbia University
New York, NY 10027
email:moti@cs.columbia.edu

***Abstract*— Secure communications between large number of sensor nodes that are randomly scattered over a hostile territory, necessitate efficient key distribution schemes. However, due to limited resources at sensor nodes such schemes cannot be based on post deployment computations. Instead, pairwise (symmetric) keys are required to be pre-distributed by assigning a list of keys, (a.k.a. *key-chain*), to each sensor node. If a pair of nodes does not have a common key after deployment then they must find a *key-path* with secured links. The objective is to minimize the key-chain size while (i) maximizing pairwise key sharing probability and resilience, and (ii) minimizing average key-path length.**

This paper presents a *deterministic* key distribution scheme based on *Expander Graphs*. It shows how to map the parameters (e.g., degree, expansion, and diameter) of a *Ramanujan Expander Graph* to the desired properties of a key distribution scheme for a physical network topology.

I. Introduction

In this work, we consider key distribution problem in wireless sensor networks where large amount of resource limited sensor nodes are randomly scattered around an adversarial environment. There is no fixed infrastructure, and network configuration is unknown prior to deployment. Secure communication in such networks requires *symmetric keys* to be shared between communicating parties, therefore a key pre-distribution scheme is required where a list of keys (*key-chain*) is stored into sensors before the deployment. The keys stored on sensors must be selected so as to increase probability (*probability of key share*) that two neighboring nodes, which are within each other's radio range, have one or more keys in common. Nodes that do not have a key in common have to communicate through a path, called *key-path*, in which each pair of neighboring nodes shares a key. Sensor nodes are deployed in adversarial areas and they are subject to compromise. Key distribution algorithms need to provide good *resilience* meaning that compromise of a sensor node should not reveal information about the keys used in other parts of the network.

A trivial but extreme solution would be to store each node a unique pairwise key for each one of the $n-1$ other nodes in the network, total of $n-1$ pairwise keys stored on each sensor node. Every pair of nodes can find a unique pairwise key in their key-chains meaning that probability of key share and average key-path length are both one. This solution has perfect resilience since the keys compromised by capture of a sensor node are not used anywhere else in the network. But sensor nodes have limited storage and $n-1$ keys on each node for a large network of size n would be far beyond than a sensor node can handle.

Recently, a *random pairwise key scheme*, based on Erdos and Renyi's work on *random graphs*, is proposed [1] to address the storage problem while maintaining resilience property. In [1], each sensor node stores a random set of np pairwise keys to achieve probability p that two nodes are connected in a network with n nodes. Each node's identity (ID) is matched with np other randomly selected node IDs with probability p. A pairwise key is generated for each ID-pair, and is stored in both nodes' key-chain along with the ID of other party.

In this paper, we present a *deterministic pairwise key scheme* for addressing the storage problem with perfect resilience. Deterministic schemes have advantages over probabilistic ones because they provide shorter average key-path lengths by using smaller key-chains [2]. In particular, we show that expander graphs can be used to distribute pairwise keys to a sensor network. Our approach is based on (1) building an expander graph, and (2) storing the pairwise key k_{ij} at both sensor nodes i, j along with their IDs, if there is an edge (i, j) between nodes n_i and n_j in the expander graph. Thus the parameters such as minimum degree, maximum expansion and diameter of the expander graph determine properties of the key distribution scheme.

A. Related Work

There are other novel approaches to distribute pairwise keys which use small amount of storage but sacrifice resilience. Basically, these solutions require sensor nodes to be pre-loaded with small amount of keying materials by using which a pair sensor nodes generates a pairwise key to secure their communication. Key matrix based solution in [3] requires each sensor to be pre-distributed with a column vector of a public matrix and a row vector of a private matrix. A pair of sensor nodes first exchanges their public column vectors, then generates the pairwise key. Several extensions to this scheme are proposed in [4] and [5] to improve resilience of the solution. In another approach, each sensor node is pre-

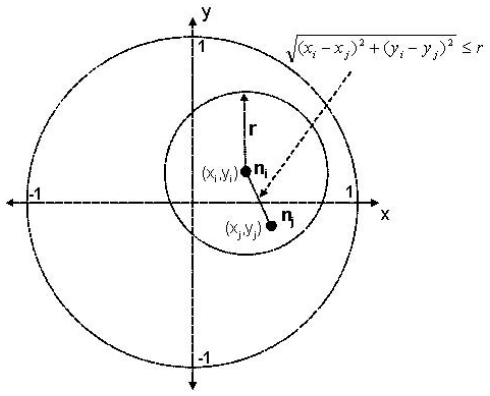

Fig. 1. Unit disk random graph to model sensor networks. For each sensor node n_i, an (x_i, y_i)-coordinate is selected uniformly at random within a unit disk of radius 1. If the nodes n_i and n_j are within each other's radio range, then there is a link in between.

distributed with a polynomial share [6]. A pair of sensor nodes uses these polynomial shares along with the identity of other party to generate the same pairwise key. Extensions to improve resilience of this scheme are proposed in [7] and [8]. Both of these approaches can resist only small amount of sensor node capture. Once the keying scheme is compromised, an adversary can obtain all pairwise keys used throughout the network.

A pairwise key can be used once by a pair of sensors. Other techniques involve keys which can be used by more than one pair of sensors. Basically, each sensor is preloaded with a chain of keys. Two sensors compare their key chains and use common keys to secure their communication. In random key distribution scheme, key chain for a sensor node is randomly selected from a large pool of keys without replacement [9], [10] and [1]. Deterministic approaches involve design of key chains by using combinatorial design techniques [2] and [11]. Complete survey of key distribution solutions in distributed wireless sensor networks can be found in [12].

B. Network Model

In this work, we consider distributed sensor networks where large number of resource limited sensor nodes are randomly scattered around an adversarial area. There is no infrastructure and post deployment configuration is unknown prior to deployment. Sensor nodes have identical processing, storage, battery life and communication resources. Once deployed, each sensor node discovers its neighbors within its radio range. It may be possible for a sensor to increase its transmission and receive power for limited period of time to discover new neighbors. Sensor nodes communicate with each other to exchange application data at data layer and routing information at control layer. Example to such networks can be military or environmental applications where large number of sensors are dropped from an airplane to an adversarial or hazardous environment.

We used unit disk random graphs to model sensor networks as in [13]. Application area is considered as a unit disk with radius 1 unit, and an (x,y)-coordinate within the disk is selected uniformly at random for each sensor node. Radio (transmit and receive) coverage area for each sensor node is assumed to be a circle with *radius* r (*radio range*) centered at its (x,y)-coordinate. If two nodes are within each other's radio range, then there is a link in between them as shown in Fig. 1. Such pairs of nodes are called *neighboring nodes*. Thus, sensor networks are modeled as geometric random graphs $G(r, n)$ on n vertices in which two vertices are adjacent if and only if their Euclidean distance is at most r. $G(r, n)$=$G(V, E_R)$ where V is the set of vertices representing sensor nodes ($|V| = n$) and E_R is the set of edges.

It is possible to relate radio range r to the connectivity of a network. Xue and Kumar in [14] examine number of neighbors needed for connectivity of wireless networks. They conclude that each node should be connected to $k = \Theta(\log n)$ nearest neighbors for the network to be asymptotically connected with probability one as $n \to +\infty$. Xue and Kumar have two basic results: (i) If each node is connected to less than $0.074 \log n$ nearest neighbors then the network is asymptotically disconnected with probability approaching to one as n increases, and (ii) if each node is connected to more than $5.1774 \log n$ nearest neighbors then the network is asymptotically connected with probability approaching to one as n increases. They consider a network where n sensor nodes are randomly placed in a unit area, and where each node has a radio range r, a tunable radio transmission range parameter $C > 0$. After rescaling to the unit disk [13]:

$$k = p\ n = C \log n$$

$$p = \frac{\pi\ r^2}{\pi} = \frac{C \log n}{n} \tag{1}$$

$$r = \sqrt{\frac{C \log n}{n}} \tag{2}$$

Diameter d of the random graphs is another metric that we are interested in. It is the maximum length of the shortest paths between two vertices. Ellis *et al.* in [13, Theorem 7] use the results of Xue and Kumar to show that unit disk random graph $G(r, n)$ is connected with diameter at most $(4+o(1))/r$ when $C > 5.11$.

C. Adversarial Model

In this work, we assume that sensor nodes are distributed in an adversarial environment. Adversaries do not have resource limitations and has access to whole network. They can perform wide variety of wireless attacks such as passive eavesdropping attacks, active man-in-the-middle attacks and stealth attacks [15]. Adversaries can capture and physically damage the sensor nodes. Once a sensor node is captured, the information stored in it is compromised. Adversaries can deploy any number of malicious sensors through which they can perform collaborative attacks.

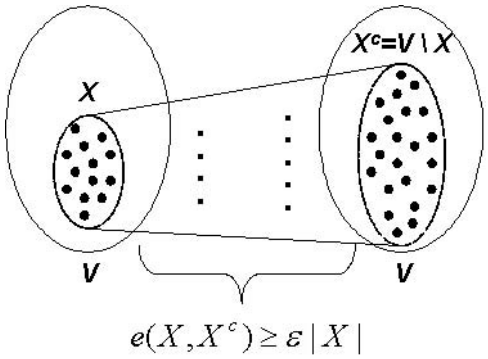

Fig. 2. Expander graphs with expansion coefficient ϵ. $\forall\ X \subset V$ where $|X| \leq |V|/2$, $e(X, X^c) \geq \epsilon|X|$

D. Our Contributions and Organization of the paper

The main contribution of this paper is a deterministic approach to key distribution problem. We bring in a novel deterministic construction methodology from *Expander Graphs* to address key distribution problem. Although, *Expander Graphs* are widely used in other application areas such as communication network design, error correcting codes, deterministic emulation of random behavior and digital stream authentication, best to our knowledge this work is the first to apply *Expander Graphs* to key distribution problem in distributed wireless sensor networks.

In addition, we derive a formula (Equation 6) that establishes a relationship between number of nodes n, size of key chain $s+1$, tunable radio transmission range parameter C, and radio range r of sensor nodes. Given any three of these parameters, the equations provide optimum value for the fourth.

This paper is organized as follows: In Section II we introduce the basics in expander graphs and their constructions. In Section III we show how to map the expander graph parameter to a key distribution scheme with desired properties. In Section IV we present our analysis and computational results. Finally in Section V we conclude with a brief discussion.

II. Background

A. Basics

Informally, an *expander* is a regular (all vertices have the same degree) multi-graph (with multiple edges between vertices) in which any subset of vertices has a large number of neighbors. It is highly connected, meaning that it is easy to get from any vertex to any other in few steps. Thus, it has small diameter, small degree and many alternate disjoint paths between vertices. Definition 1 and Fig. 2 provides formal definition.

Definition 1: ([16], [17], [18]) A graph $G = (V, E)$ is said to be *ϵ-edge-expander* if for every partition of the vertex set V into X and $X^c = V \backslash X$, where $|X| \leq |V|/2$, the number of *cross edges* is $e(X, X^c) \geq \epsilon|X|$. ϵ is called *expansion coefficient*.

Definition 1 can also be interpreted as: in every cut in G, the number of cut edges is at least proportionate to the size of smaller side. One problem with the expanders is given by Theorem 2.

Theorem 2: ([19]) The following computational problem is *co-NP*: given a graph G, and $\epsilon > 0$, is G an *ϵ-edge-expander*?

Although almost all random bipartite graphs are expanders, we would like to deterministically construct expanders which have maximum possible *expansion coefficient* ϵ while vertex degrees are bounded above by a constant. For that, we need to understand relation between expansion of a graph and eigenvalues of its adjacency matrix.

Graph $G(V, E)$ with n vertices can be represented as an *adjacency matrix* $A(G)$ of order $(n \times n)$ where $a_{ij} = 1$ if there is an edge from node i to node j in $G(V, E)$ and $a_{ij} = 0$ otherwise. The eigenvalues $\lambda_0, \lambda_1, \ldots, \lambda_{n-1}$ of $A(G)$ are called the *spectrum* of graph G. Spectrum of a k-regular graph has the property that $\lambda_0 = k \geq \lambda_1 \geq \ldots \geq \lambda_{n-1}$. The difference between first two eigenvalues, $(\lambda_0 - \lambda_1)$ is called *spectral gap*. Theorem 3 provides relation between spectral gap and expansion coefficient ϵ where larger spectral gap $(\lambda_0 - \lambda_1)$ implies higher expansion. Thus, we would like to have λ_1 as small as possible. Theorem 4 shows a bound for the eigenvalue λ_1 but *Ramanujan expander graphs* described in the next section are k-regular graphs with better expansion where $\lambda_1 \leq 2\sqrt{k-1}$.

Theorem 3: (Tamner, Alon, Milman)([16])

$$\frac{k - \lambda_1}{2} \leq \epsilon \leq \sqrt{2k(k - \lambda_1)}. \tag{3}$$

Theorem 4: (Alon, Boppana)([16]) For every $k - regular$ graph:

$$\lambda_1 \geq 2\sqrt{k-1} - o(1). \tag{4}$$

B. Ramanujan Graphs and Their Construction

Ramanujan graphs are asymptotically optimal and best known explicit expanders [20] where $|\lambda_i| \leq 2\sqrt{k-1}$ for $(1 \leq i \leq n-1)$. A Ramanujan graph $X^{s,t}$ is a k-regular graph with $n = t+1$ nodes where $k = s+1$, and both s and t are primes congruent to 1 (mod 4). It can be constructed as:

1) Generate vector $\overrightarrow{a_j} =< a_0, a_1, a_2, a_3 >$ for $0 \leq j \leq s$ where:
   a) $a_0 \in \mathcal{N}$ is an odd number
   b) $a_1, a_2, a_3 \in \mathcal{Z}$ are even numbers
   c) $a_0^2 + a_1^2 + a_2^2 + a_3^2 = s$
2) Generate matrix γ_j with vector $\overrightarrow{a_j}$ for $0 \leq j \leq s$ where:
   a) $\gamma_j = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}$ for $i^2 \equiv$ -1 (mod t)
   b) $\gamma_j(z) = \frac{(a_0+ia_1)z+(a_2+ia_3)}{(-a_2+ia_3)z+(a_0-ia_1)}\ (mod\ t)$ for $z \in \mathcal{N}$
3) For nodes $z = 0$ to $z = t+1$
   a) Generate $k = s+1$ neighbors as $\gamma_j(z)$ for $0 \leq j \leq s$

Example 5: $X^{5,17}$ Ramanujan graph have $t + 1 = 18$ vertices where each one has degree of $s + 1 = 6$ including self loops and multi-edges. The $s + 1 = 6$ vectors will be:

$$\overrightarrow{a_0} =< 1, 2, 0, 0 > \quad \overrightarrow{a_1} =< 1, 0, 2, 0 >$$
$$\overrightarrow{a_2} =< 1, 0, 0, 2 > \quad \overrightarrow{a_3} =< 1, 0, 0, -2 >$$
$$\overrightarrow{a_4} =< 1, 0, -2, 0 > \quad \overrightarrow{a_5} =< 1, -2, 0, 0 >$$

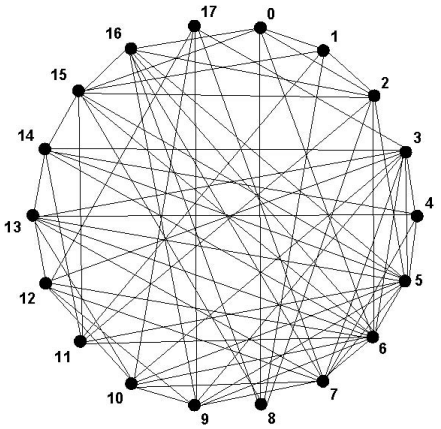

Fig. 3. Physical graph $G(r,n) = G(V, E_R)$ with 18 nodes.

Next, corresponding $s+1 = 6$ matrices of order 2×2 need to be generated. Clearly, $i^2 \equiv$ -1 (mod 17) yields $i = 4$, thus matrices will be:

$$\gamma_0 = \begin{pmatrix} 9 & 0 \\ 0 & -7 \end{pmatrix} \quad \gamma_1 = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}$$
$$\gamma_2 = \begin{pmatrix} 1 & 8 \\ 8 & 1 \end{pmatrix} \quad \gamma_3 = \begin{pmatrix} 1 & -8 \\ -8 & 1 \end{pmatrix}$$
$$\gamma_4 = \begin{pmatrix} 1 & -2 \\ 2 & 1 \end{pmatrix} \quad \gamma_5 = \begin{pmatrix} -7 & 0 \\ 0 & 9 \end{pmatrix}$$

Finally, $s + 1 = 6$ neighbors including self loops and multi-edges need to be found. For each node z where $0 \leq z \leq t + 1 = 18$:

z	$\gamma_0(z)$	$\gamma_1(z)$	$\gamma_2(z)$	$\gamma_3(z)$	$\gamma_4(z)$	$\gamma_5(z)$
0	0	2	8	9	15	0
1	6	14	1	1	11	3
2	12	10	0	14	0	6
3	1	16	12	15	5	9
4	7	4	5	10	4	12
5	13	3	14	4	8	15
6	2	7	10	8	16	1
7	8	15	11	13	6	4
8	14	5	6	0	0	7
9	3	0	0	11	12	10
10	9	11	4	6	2	13
11	15	1	9	7	10	16
12	4	9	13	3	14	2
13	10	13	7	12	13	5
14	16	12	2	5	1	8
15	5	0	3	0	7	11
16	11	6	16	16	3	14
17	0	2	8	9	15	0

Figure 4 shows $X^{5,17}$ Ramanujan graph where self loops and multi-edges are deleted.

III. Expander Graphs to Key Distribution

A. Construction

In this work, we use expander graphs to distribute pairwise keys to sensor nodes. Ramanujan graphs are asymptotically optimal expanders in providing highest expansion with smallest node degrees. Similarly, in key distribution we would like to store minimum amount of keys on each sensor node and would like each sensor node to share a key with as many other sensors as possible. We model physical sensor network as a geometric random graph $G(r,n) = G(V, E_R)$, and distribute keys based on Ramanujan expander graph $G(V, E_X) = X^{s,t}$ which is constructed as described in Section II-B for the same vertex set V of the physical graph $G(V, E_R)$. Self loops and multi-edges are replaced with randomly selected edges so that each node stores same amount of pairwise keys. For each edge in E_X of Ramanujan expander graph, sensor nodes corresponding to vertices of the edge are assigned the same pairwise key along with their ids. Thus, an edge in E_X of Ramanujan expander graph means physical link between sensor nodes corresponding to vertices of the edge can be secured. Thus, secure graph which consists of secure links is $G(V, E_S) = G(V, E_R \cap E_X)$. Once this graph is established, each remaining unsecured physical link in $G(V, E_R)$ can be secured with a pairwise key negotiated through the shortest path (*key-path*) between its vertices in $G(V, E_S)$. Figures 3, 4

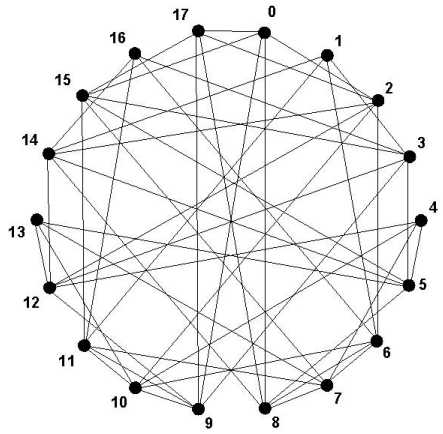

Fig. 4. Ramanujan expander graph $G(V, E_X) = X^{5,17}$ with 18 nodes where each node has 6 neighbors including self loops and multi-edges. Self loops and multi-edges are not shown in this figure.

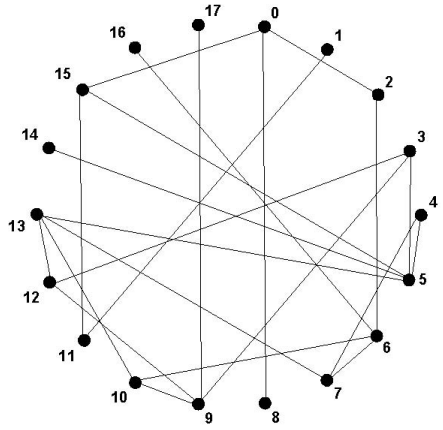

Fig. 5. Secure graph $G(V, E_S) = G(V, E_R \cap E_X)$ with 18 nodes. A link in Figure 3 is included in secure graph if nodes corresponding to its vertices share a pairwise key. Pairwise keys are distributed due to Ramanujan expander graph of Figure 4.

and 5 provide examples for graphs $G(V, E_R)$, $G(V, E_X)$ and $G(V, E_S)$ respectively.

B. Mapping

Consider a distributed wireless sensor network of size n. We would like to assign a list of pairwise keys, called key-chain, to each sensor node before the deployment. To decide which pairwise key to be pre-distributed to which sensor pair, we construct a Ramanujan expander graph $X^{s,t}$ which has $n = t+1$ nodes where each node has degree of $s+1$ including the self loops and multi-edges. Self loops and multi-edges are replaced with randomly selected edges so that each node stores same amount of pairwise keys. Table I defines the mapping between *Key Distribution* and *Expander Graphs*. Vertices of the Ramanujan expander graph correspond to sensor nodes. Two sensor nodes share a pairwise key if corresponding vertices have a link in Ramanujan expander graph. Average degree of the Ramanujan expander graph $G(V, E_X) = X^{s,t}$ defines key chain size for the sensor nodes. Diameter of the secure graph $G(V, E_S) = G(V, E_R \cap E_X)$ corresponds to maximum key-path length for two sensor nodes which have no link in Ramanujan expander graph.

IV. Analysis and Computational Results

Secure graph $G(V, E_S) = G(V, E_R \cap E_X)$ consists of the vertices and subset of the edges of random physical graph $G(r, n) = G(V, E_R)$. We would like secure graph $G(V, E_S)$ to be connected with link probability p_S. For $G(V, E_S) = G(V, E_R \cap E_X)$, $p_S = p_R\ p_X$ where p_R (p in Equation 1) is the link probability of physical network $G(r, n) = G(V, E_R)$, and p_X is the link probability of Ramanujan expander graph $G(V, E_X) = X^{s,t}$:

$$p_X = 1 - [(\frac{t}{t+1})(\frac{t-1}{t}) \dots (\frac{t-s}{t+s-1})] = \frac{s+1}{t+1} \qquad (5)$$

Due to the results of Xue and Kumar in [14], each node should be connected to $k = \Theta(\log n)$ nearest neighbors for the secure graph $G(V, E_S)$ to be asymptotically connected with probability one as $n \to +\infty$:

$$\begin{aligned} k = p_R\ p_X\ n &= C\ \log n \\ \frac{\pi r^2}{\pi}\ \frac{s+1}{n} &= \frac{C\ \log n}{n} \\ r &= \sqrt{\frac{C \log n}{s+1}}. \end{aligned} \qquad (6)$$

Equation 6 provides relation between parameters n which is the number of sensor nodes, degree s of the Ramanujan expander graph $X^{s,t}$, tunable radio transmission range parameter C, and radio range r of the sensor nodes. Given any three parameters, Equation 6 can be used to find required value of the fourth one for the secure graph $G(V, E_S)$ to be connected. Based on the results of Ellis *et al.* in [13, Theorem 7], diameter of such a secure graph $G(V, E_S)$ is at most $(4+o(1))/r$ when $C > 5.11$.

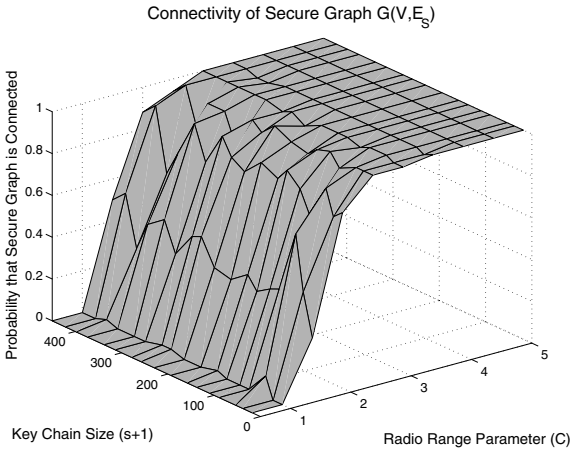

Fig. 6. Connectivity of secure graph $G(V, E_S) = G(V, E_R \cap E_X)$. Figure plots probability that a secure graph with 1000 nodes is connected for each value of key chain size $(s+1)$ and tunable radio transmission range parameter C. Simulation results support findings of Xue and Kumar which is described in Section I-B. The critical value for C is $C > 2$ when the probability of connectedness is close to one.

A. Computational Results

We have implemented our key distribution algorithm. Our implementation consists of tree parts. First, we generate a random graph $G(r, n)$ for an arbitrary network size n and radio range r (Equation 6) to simulate the underlying physical network. This graph is generated as described in Section I-B. Next, we generate Ramanujan expander graph $X^{s,t}$ where $n = t + 1$ is the network size, and $s + 1$ is the required key chain size for the sensor nodes. Finally, we distribute pairwise keys to nodes based on the Ramanujan expander graph. We generate secure graph only including physical links which have associated pairwise keys. Pairs of sensor nodes which have physical link but do not have a pairwise key to secure it need to secure their communication through a path. For those pairs we find the key path lengths and the maximum of the key-path lengths corresponds to the diameter of the secure graph $G(V, E_S)$. We plot connectivity of secure graph in Fig. 6 for each each value of key chain size $(s + 1)$ and tunable radio transmission range parameter C. Our simulation results support findings of Xue and Kumar which is described in Section I-B. When sensor nodes have radio range r due to Equation 6, for the critical value of $C > 2$, the probability of connectedness for secure graph is close to one.

Next, we compare Ramanujan expander graph based key distribution scheme with random pairwise key scheme [1] in Fig. 7. We show that our deterministic approach yields shorter average key-path length while preserving perfect resilience.

V. Discussions and Conclusion

This work provides a novel deterministic approach to distribute pairwise keys to sensor nodes. We model underlying physical network as a random graph and use asymptotically optimum Ramanujan expander graphs to distribute pairwise keys to sensor nodes. For the analysis, we use results in [21],

Expander Graphs $X^{s,t}$		Key Distribution
$\|V\| = t+1$ vertices	$\rightarrow$	$n = t+1$ sensor nodes
Number of edges excluding self loops and multi-edges	$\rightarrow$	Number of distinct pairwise keys
Vertex degree $s+1$	$\rightarrow$	Key-chain size $s+1$
Edge (i,j)	$\rightarrow$	Pairwise key $k_{i,j}$ stored on nodes i and j
Edge probability in $G(V,E_X) = X^{s,t}$	$\rightarrow$	Probability of key share between any pair of nodes
Diameter of $G(V,E_S) = G(V,E_R \cap E_X)$	$\rightarrow$	Maximum key-path length

TABLE I
EXPANDER GRAPHS TO KEY DISTRIBUTION

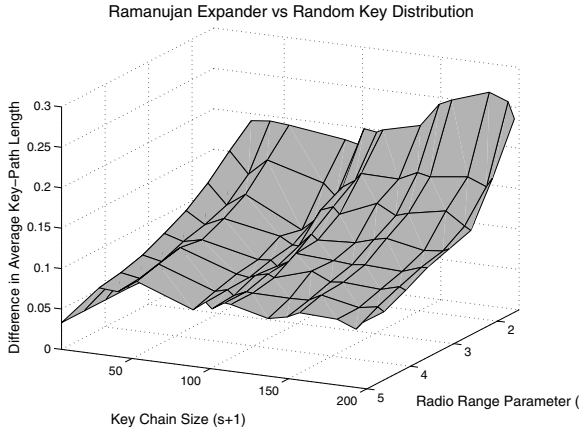

Fig. 7. Ramanujan expander graph based key distribution is compared with Random pairwise key scheme for a network of size 1000. Figure plots difference in average key-path lengths (Random - Ramanujan) of secure graphs $G(V,E_S)$ for each value of key chain size $(s+1)$ and tunable radio transmission range parameter C. Deterministic nature of Ramanujan expander based key distribution yields shorter average key-path length.

[22] and [14]. We derive the Equation 6 which can be used to fine tune the parameters of underlying physical network or expander key distribution graph to reach a connected secure graph.

Chan *et al.* in [1] uses random graphs to distribute pairwise keys which can not perform better than asymptotically optimum Ramanujan expander graphs with the same size and degree. Unlike other solutions detailed in [12], we preserve perfect resilience and show ways of fine tuning network parameters to reach a desired security. Nevertheless, probability of key share and resilience subject to storage limitations are conflicting factors and one cannot be improved without sacrificing the other.

ACKNOWLEDGMENT

We would like to thank to Mukkai Krishnamoorthy for valuable discussions on Ramanujan expander graph constructions.

REFERENCES

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

[2] S. Camtepe and B. Yener, "Combinatorial design of key distribution mechanisms for wireless sensor networks," in *9th European Symposium on Research Computer Security*, September 2004.

[3] R. Blom, "An optimal class of symmetric key generation systems," in *Eurocrypt 84*, 1985.

[4] W. Du, J. Deng, Y. 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 CCS'03*, October 2003.

[5] J. Lee and D. Stinson, "Deterministic key pre-distribution schemes for distributed sensor networks," in *11th Annual Workshop on Selected Areas in Cryptography*, August 2004.

[6] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," in *Crypto 92*, 1992.

[7] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *10th ACM conference on Computer and communications security CCS'03*, October 2003.

[8] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *IEEE Infocom'04*, March 2004.

[9] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *9th ACM conference on Computer and Communications Security*, November 2002.

[10] D. Hwang, B. Lai, and I. Verbauwhede, "Energy-memory-security tradeoffs in distributed sensor networks," in *3rd International Conference on Ad-Hoc Networks and Wireless (ADHOC-NOW 2004)*, July 2004.

[11] J. Lee and D. Stinson, "A combinatorial approach to key predistribution for distributed sensor networks," in *IEEE Wireless Communications and Networking Conference*, March 2005.

[12] S. A. Camtepe and B. Yener, "Key distribution mechanisms for wireless sensor networks: a survey," Rensselaer Polytechnic Institute, Computer Science Department, Tech. Rep. 05-07, March 2005.

[13] R. B. Ellis, X. Jia, and C. Yan, "On random points in the unit disk," *Random structures and algorithms*, 2005.

[14] F. Xue and P. R. Kumar, "The number of neighbors needed for connectivity of wireless networks," *Wireless Networks*, vol. 10, pp. 169–181, 2004.

[15] M. Jakobsson, S. Wetzel, and B. Yener, "Stealth attacks on ad-hoc wireless networks," in *Vehicular Technology Conference*, 2003.

[16] N. Linial and A. Wigderson, "Expander graphs and their applications," Lecture Notes, Hebrew University, Israel, January 2003.

[17] N. Linial, "Expanders, eigenvalues and all that," NIPS 2004 Talk, 2004.

[18] R. Govindaraju, "Design of scalable expander interconnection networks," Ph.D. dissertation, Rensselaer Polytechnic Institute, Troy, New York 12180, USA, 1994.

[19] M. Blum, R. Karp, O. Vornberger, C. Papadimitriou, and M. Yannakakis, "The complexity of testing whether a graph is a superconcentrator," *Information Processing Letters*, vol. 13, no. 4,5, pp. 164–167, 1981.

[20] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica*, vol. 8, no. 3.

[21] B. Bollobas, *Random Graphs*, 2nd ed. Cambridge University Press, 2001.

[22] P. Gupta and P. R. Kumar, "Critical power for asymptotic connectivity in wireless networks," *Stochastic Analysis, Control, Optimization and Applications, A Volume in Honor of W.H. Fleming*, vol. 10, pp. 547–566, 1998.