On The Connectivity of Key-Distribution Strategies in Wireless Sensor Networks

H. Shafiei*, Ahmad Khonsari†*, Mohammad S. Talebi*, Mohamed Ould-Khaoua‡, and Nazanin Dehghani†
Emails: {shafiei, mstalebi, ak, dehghani}@ipm.ir, mohamed@dcs.gla.ac.uk
*School of Computer Science, IPM, Tehran, Iran
†Department of Electrical and Computer Engineering, University of Tehran, Tehran, Iran
‡Department of ECE, University of Soltan Qaboos, Oman

***Abstract*—Wireless sensor networks (WSNs) are usually missioned to gather critical information in hostile and adversarial environments, which make them susceptible to compromise and revelation. Therefore, establishing secure communication in such networks is of great importance necessitating utilization of efficient key distribution schemes. In order to address such methods, several works using probabilistic, deterministic and hybrid approaches have been introduced in past few years. In this paper, we study the connectivity of key-distribution mechanisms in secured topologies of wireless sensor networks. We explore the effect of the radio range on the connectivity of the network and provide a lower bound on the radio range under which the cover time of the underlying topology decreases significantly. We also deduce that any broadcasting algorithm in such a network is performing only by a factor $O(n^{\beta})$, where $\beta \in (0, 1)$, worse than broadcasting algorithms in unsecured topologies. Our numerical results and simulation experiments validates the correctness and efficiency of our analysis.**

I. Introduction

In recent years there has been a surge of interest in usage of wireless sensor networks (WSN). WSNs are expected to be exploited in a wide variety of applications, ranging from data collection to monitoring in different scenarios. Emergence of micro-sensors based on MEMS technology has made it possible to deploy a large networked system comprising of battery-operated sensor nodes. WSNs enable us to implement ubiquitous architectures to gather, process and transfer data from various environments ranging from urban sites to wide rural areas [1].

Security is an indispensable concern for sensor networks to work safely in real world circumstances, in particular over adverse or hostile environments. Establishing secure connectivity in WSNs proves quite challenging [2]–[4]. Implementing security primitives such as public-key and elliptic-curve cryptography demand high computational and storage requirements. It is believed that traditional Internet style key exchange and key distribution protocols based on infrastructures using trusted third parties are impractical for large scale WSNs due to lack of infrastructure and uncontrolled environment of such networks. Thus, symmetric key pre-distribution strategies are known to be a promising approach in attaining secure communications in WSNs.

In key pre-distribution strategy, each sensor node is assigned a list of keys (called *key-chain*), before the deployment phase. Thus, sensors having identical keys are able to communicate with each other directly. It is desirable to store the keys in sensor nodes in order to enable the neighboring nodes possess one or more common keys with each others. Nodes not having a key in common have to communicate through a path, called *key-path*, in which a key is shared between each pair of neighboring nodes (as shown in Figure 1). Due to the adversarial nature of deployment environment, sensor nodes are highly subject to compromise. An efficient key distribution strategy should impede information revelation or disclosure of keys being used in other parts of the WSN. In traditional strategies either a single mission key is being scattered in all sensor nodes, or a set of separate $n-1$ keys are being installed in every sensor node such that each key is used as to establish a secure connection between two neighboring nodes. The deficiency of single mission-key solution relies on the fact that capturing any sensor node may compromise the entire WSN. Moreover, selective key revocation is impossible upon sensor capture detection. An extreme solution would be the utilization of unique pair-wise keys for each of node pairs in the network. In other words, in a WSN of size n, each node would store a unique pair-wise key with each of the other $n-1$ nodes of the network, resulting in a key-chain of size $n-1$ in each sensor. Perceptibly, since pair-wise sharing of keys between every two sensor nodes facilitates selective key revocation, compromising any sensor node will not divulge the key-chain except the key of the compromised node avoiding wholesale WSN compromise, which results in a desirable yet resource demanding resilience.

In the abovementioned approach, the probability of key share success is equal to 1 and the average key-path length is identical to 1 as long as the two communicating parties lie in each other's radio range. Nevertheless, having this perfect resilience demands for storing $n-1$ keys in each node in a network of size n, which is potentially beyond the limits of a sensor node for both intrinsic and technological reasons. The shortcomings of such strategy can be categorized as follows: first, pair-wise key sharing between any two sensor nodes would be unusable since direct node-to-node communication is achievable only in small node neighborhoods delimited by radio range and node density, leading to waist of priceless resources such as dedicated memory and energy. Second, incremental addition and deletion as well as re-keying of sensor nodes would become both expensive and complex as

they would require multiple keying messages to be broadcast network-wide to all nodes during their active periods.

In order to utilize the WSNs limited yet priceless resources and preserving resilience, while achieving scalability, a random pair-wise key distribution scheme based on Erdös and Renyi's work on random graphs has been proposed in [8]. In a network of size n, each sensor node stores the key of the remaining nodes with probability p and thus stores a random set of np pair-wise keys. Each node identity (ID) is matched with np other randomly selected node IDs with probability p. A pair-wise key is generated for each ID-pair, and is stored in both nodes key-chain along with the ID of other party. Moreover, recently key-distribution schemes based-on expander graphs [9] have been proposed in [10], [11]. In these approaches, a expander graph is generated using various methods introduced in [12] and [13]. Intuitively, each sensor node is assigned to a node of the expander graph. The key-chain of each sensor node is built upon the neighborhood of such a graph resulting in a highly resilient key-distribution scheme.

Our focus in this paper is on the connectivity of key-distribution mechanisms in secured wireless sensor networks. We first explore the condition on the radio range of each sensor to ensure the entire network remains connected. We next establish a lower bound on the radio range under which the *cover time*[1] of the network decreases significantly. We also deduce that any broadcasting algorithm in such a network is performing only by a factor $O(n^{\beta})$, where $\beta \in (0,1)$, worse than broadcasting algorithms in unsecured topologies. The accuracy and efficiency of our analysis and formulas are validated by our numerical results and simulation experiments.

The rest of the paper is organized as follows. Section II provides some definitions, describes the notation that is used throughout the paper and provides the critical radio range for connectivity of underlying secure topology. Section III introduces the optimum bound for radio range. Section IV discusses the broadcasting in secured random geometric graphs, V presents numerical results and simulations. Finally, Section VI provides some concluding remarks and outlines directions of future research.

II. Secured Connectivity

In this section, we explore the condition on the *radio range* under which the two following holds:

- The underlying communication graph is connected with high probability[2].
- Each node has at least one neighbor which is in possession of a common key.

The first item and its generalizations have gained more attention by the research community in the last few years [14], [15]. However, the second one is restricted to the cases in which there is a compromise between reliability, in terms of security, and performance in terms of connectivity.

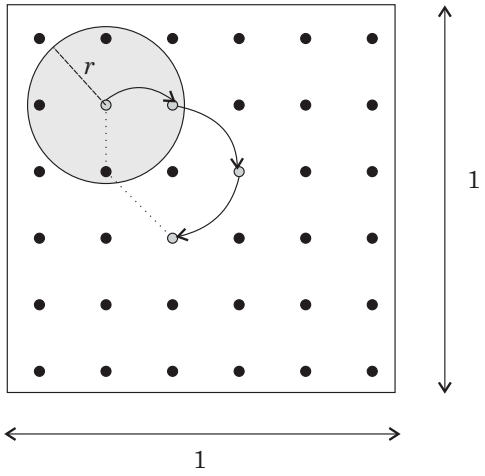


Fig. 1: An example of a two dimensional Random Geometric Grid. A node is connected to all other nodes that are within the distance r of itself and possess common key

In this section we explore the connectivity of key-distribution schemes deployed with a random geometric topology under large system asymptotic. For the sake of simplicity, we first state some fundamental results using recently proposed random graph theory, which is a comprehensive approach in modeling largely deployed WSNs. Then we proceed to prove an important condition for the connectivity of the underlying graph, considering security merits.

A d-dimensional random geometric graph is denoted by $\mathcal{G}^d(n,r)$, where n represents the number of nodes and r is the radio range. One simple way to construct such a random graph is to scatter n nodes uniformly on the $[0,1] \times [0,1]$ square and connect each two nodes whose Euclidean distance are less than r. A typical example of such a graph is depicted in Figure 1. One of the most issues of concern regarding random geometric graphs is its connectivity. We distinguish between two notions of connectivity.

- *Physical Connectivity:* The random geometric graph $\mathcal{G}^d(n,r)$ is said to be *physically connected* if there exists at least one path between every two nodes. In other words, every node can communicate with any other node, possibly using other nodes as relays.
- *Secured Connectivity*: The random geometric graph $\mathcal{G}^d(n,r)$ is said to be *securely connected* if there exists at least one *secured path* between every two nodes. Precisely speaking, every node can communicate with any other node, possibly using relays which are in possession of a key in common with each other.

Clearly, the first notion defined above, is necessary for the connectivity of the underlying graph. However, as the second notion implies, we are interested in connectivity of such a graph so that only nodes with keys in common can communicate with each other.

[1]The cover time of a graph is the expected time taken for random walk to visit every node of the graph .

[2]In the rest of this paper, unless the otherwise stated, by *with high probability*, also abbreviated as *w.h.p*, we mean the probability at least $1-\frac{1}{n^2}$.

In what follows, first we state some underlying results for the physical connectivity of $\mathcal{G}^2(n,r)$.

A. Physical Connectivity

In this subsection, we state some useful underlying lemmas regarding the physical connectivity of the $\mathcal{G}^2(n,r)$.

Lemma 1: For all $\epsilon > 0$ if $\pi r^2(n) = (1-\epsilon)\frac{\log n}{n}$, then $\mathcal{G}^2(n,r)$ is disconnected *w.h.p.*, while if $\pi r^2(n) = (1+\epsilon)\frac{\log n}{n}$, then $\mathcal{G}^2(n,r)$ is connected *w.h.p.*

Proof. For proof see [15].

Physical connectivity is essential for secured connectivity; hence, we require each node to set its radio range $r(n)$ greater than $\frac{\log n}{\pi n}$. In this respect, no node can be allowed to be an isolated node.

B. Secured Connectivity

In this subsection, we explore the secured connectivity, which is of much more interest to us.

In order to come up with a tractable analysis of the secured connectivity, we model the event of possession of a common key as a random variable whose success probability is denoted by $p(n)$.

In the sequel, we state the condition for $r(n)$ and $p(n)$ in order to guarantee the secured connectivity.

Lemma 2: For $\mathcal{G}^2(n,r)$, and for sufficiently large n,

$$\Pr(\text{network is connected}) \geq 1 - np(n)e^{-\frac{\pi p(n) r^2(n) n}{2}} \tag{1}$$

Thus, the network is connected if $p(n)$ and $r(n)$ satisfy

$$\lim_{n\to\infty} np(n)e^{-\frac{\pi p(n) r^2(n) n}{2}} = 0 \tag{2}$$

Proof. For proof see [14].

As mentioned in the previous section, most key-distribution strategies construction lead to regular graphs; i.e. the degree of each node is equal and denoted by $\Delta(n)$. Therefore, it is clear that the success probability is given by:

$$p(n) = \frac{\Delta(n)}{n} \tag{3}$$

Using the above results, we now discuss the requirements for the secured connectivity for random geometric topologies.

Theorem 1: For any fixed $\beta \in (0,1)$, if

$$\Delta(n) = \Theta(n^\beta) \tag{4}$$

then the network is connected if $r^2(n)$ satisfies

$$r^2(n) \geq c\frac{\log n}{\Delta(n)} \tag{5}$$

where c satisfies

$$c \geq \frac{2\beta}{\pi} \tag{6}$$

Proof: Substituting (4) and (5) in (2), yields the following condition for connectivity

$$\lim_{n\to\infty} n\frac{n^\beta}{n} e^{-\frac{\pi \frac{n^\beta}{n} r^2(n) n}{2}} = 0 \tag{7}$$

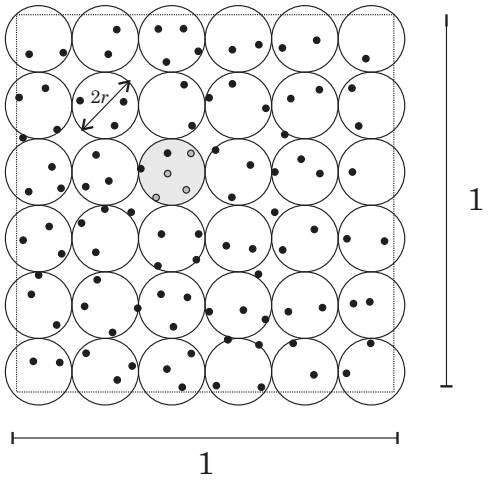


Fig. 2: An example of a two dimensional Secured Random Geometric Graph with radio range $r^2(n)$. At most k (in this case $k = 4$) nodes in their radio range possess a common key

From the right hand side of (7), we get

$$\begin{aligned} \text{(R.H.S of (7))} &= \lim_{n\to\infty} n^\beta e^{-\frac{\pi n^\beta r^2(n)}{2}} \\ &= \lim_{n\to\infty} e^{\beta\log n - \frac{\pi n^\beta r^2(n)}{2}} \\ &= \lim_{n\to\infty} e^{\beta\log n - \frac{\pi c \log n}{2}} \end{aligned} \tag{8}$$

where (8) is obtained from (5) and (4). Clearly, for (8) to vanish, the coefficient of $\log n$ must be negative, leading us to the following condition

$$\begin{aligned} \beta - \frac{\pi c}{2} &\leq 0 \\ c &\geq \frac{2\beta}{\pi} \end{aligned} \tag{9}$$

which completes the proof.

III. Optimum Secure Connectivity

So far, we have provided a critical radio range[3] (for each node) guaranteeing asymptotic connectivity of the secured random geometric graph. Although this bound is essential for the network to remain connected, it may lead to bottlenecks in the network and consequently alleviates its performance. This is due to the lack of alternative secured routing choices as a result of utilizing the tight bound of the critical radius. However, in specific applications of WSNs such radio range may not guarantee the performance constraint of that applications; This motivated us to provide an optimum radio range for secured random geometric graph which ensures that at least k alternative routing paths exist for each node of the graph. In what follows we investigate such optimum radio range.

Lemma 3: For $\mathcal{G}^2(n,r)$, and sufficiently large n, let $P_k(n)$ be the probability that every node in $\mathcal{G}^2(n,r)$, say v, has at

[3]Here, the terms *radio range* and *radius* are exactly the same and used interchangeably.

least k secured neighbors within its radio range $r^2(n)$. Then the following bound holds:

$$P_k(n) \leq \exp\left(-\frac{e^{-\frac{(n\pi r^2(n)p-k+1)^2}{2n\pi r^2(n)p}}}{4r^2(n)}\right) \tag{10}$$

Proof: We first divide our unit area into $R(n)$ disjoint regions, each of which has radius $r(n)$ as depicted in Figure 2. According to the figure, it is not hard to prove that there are $R(n) = 4r^2(n)$ regions, each has at most $n\pi r^2(n)$ nodes. Let $X(i)$ be a random variable whose value is equal to the maximum number of secured neighbors residing in region i of $\mathcal{G}^2(n,r)$. Remind that the probability of a node has a common key with every other nodes is $p(n)$. Thus, it follows that:

$$\begin{aligned}
P_k(n) &= \Pr(\bigcap_{i=1}^{R(n)} X(i) \geq k) \\
&= [\Pr(X(1) \geq k)]^{R(n)} \\
&= \left[1 - \sum_{i=0}^{k-1} \binom{n\pi r^2(n)}{i} p^i (1-p)^{n\pi r^2(n)-i}\right]^{(4r^2(n))^{-1}} \\
&\leq \left[1 - e^{-\frac{(n\pi r^2(n)p-k+1)^2}{2n\pi r^2(n)p}}\right]^{(4r^2(n))^{-1}} \\
&\leq \exp\left(-\frac{e^{-\frac{(n\pi r^2(n)p-k+1)^2}{2n\pi r^2(n)p}}}{4r^2(n)}\right)
\end{aligned}$$

■

In the following theorem, we provide a bound for the above mentioned optimum radius to ensure the existence of at least k alternative routing paths for each node of the secured random geometric graph.

Theorem 2: For a $\mathcal{G}^2(n,r)$ assume that $k = \alpha n^\beta$ where $\alpha, \beta \in (0,1)$ and $p(n)$ be the probability of possession of a common key for two arbitrary nodes with $r^2(n) \geq \frac{1}{4\pi - 2\alpha}\frac{\log(n)}{n^\beta}$, then $P_k(n)$ almost surely tends to 1.

Proof: According to Lemma 3, $P_k(n) \to 1$ if and only if:

$$\lim_{n\to\infty} \frac{e^{-\frac{(n\pi r^2(n)p-k+1)^2}{2n\pi r^2(n)p}}}{4r^2(n)} \to 0 \tag{11}$$

which follows that:

$$\lim_{n\to\infty} 4r^2(n)e^{npr^2(n)(\pi/2-\alpha)} \to \infty \tag{12}$$

Now, assume that

$$c(n) = \frac{npr^2(n)}{\log(n)} \tag{13}$$

substituting it in the last equation yields:

$$\lim_{n\to\infty} 4\log(n)c(n)n^{(\pi/2-\alpha)c(n)-1} \to \infty \tag{14}$$

The following condition must be held in order to equation (14) tends to infinity:

$$(\pi/2 - \alpha)c(n) \geq 1 \tag{15}$$

thus, a tight bound for radio range of each node can be obtained by:

$$r^2(n) \geq c\frac{\log(n)}{n^\beta} \tag{16}$$

$$\tag{17}$$

where c satisfies the following condition:

$$c \geq \frac{2\beta}{2\pi - \alpha} \tag{18}$$

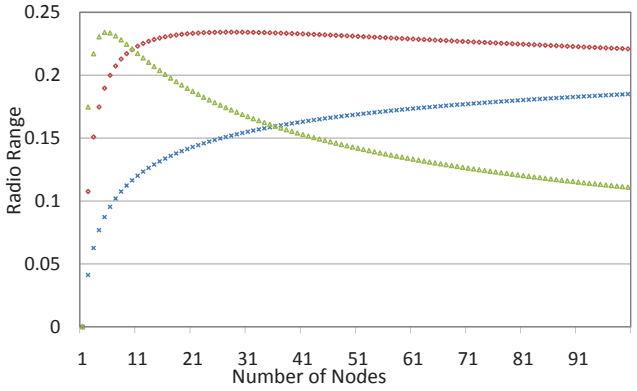
■

IV. Broadcasting in secured geometric graphs

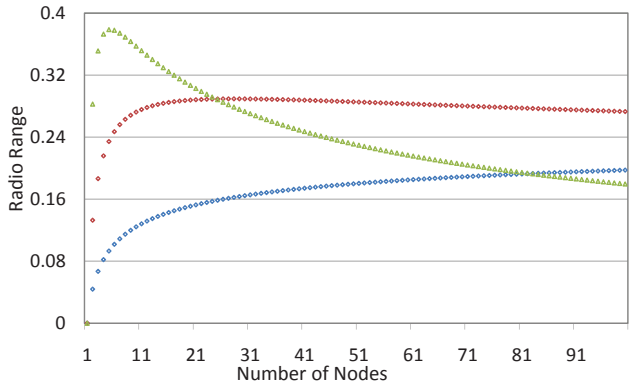
In this section we will elaborate on a performance characteristic of broadcasting algorithms in secured random geometric graphs. We prove that any broadcasting algorithm in such networks is performing only by a factor $O(n^\beta)$, where $\beta \in (0,1)$, worse than broadcasting algorithms in unsecured random geometric networks which is tolerable in most practical cases.

Due to the severe energy restrictions of wireless sensor networks utilizing energy-efficient broadcasting algorithms have became a significant issue in the course of last years. In fact, broadcasting is a very energy-expensive protocol which is widely used as a building block for a variety of other network layer protocols. Thus, exploiting performance characteristic of broadcasting in this type of network is of a paramount value. Many researchers have been carried out in order to either reduce the energy consumption of sensor networks by optimizing broadcasting [16] or study the performance of a proposed broadcasting algorithm [17]. In this section, we pursue on a major performance characteristic of such algorithms introduced in [18]. As stated in Chandra et al. [18], intuitively, the cover time of the graph is an appropriate metric for the performance of randomized broadcast algorithms. This intuition is further verified by [19]. Moreover, cover time is tightly coupled with the performance of applications and techniques such as gossiping in random geometric graphs [20], information collection and query answering [21] and routing [22]. This metric is defined as follows:

Let $G = (V, E)$ be a connected graph, for $u \in V$ let C_u be the expected time taken for a *random walk* W_u to visit every vertex of G. The cover time C_G of G is defined as $C_G = \max_{u\in V} C_u$. The cover time of many types of connected graphs has been extensively studied in [23]. Avin et. al. in [23] show that there exists a critical radius r_{opt} such that for any $r \geq r_{opt}$, $\mathcal{G}^2(n,r)$ has optimal cover time of $\Theta(n\log n)$ with high probability. However, despite the similarities between random geometric graphs and theirs secured variants, the result obtained in [23] is not applicable in such graphs. One remarkable difference is the existence of many small cliques uniformly distributed over the unit square like bins in random geometric graphs (which is essential in their analysis) that not holds in secured version of such graphs. Therefore, we believe that random regular graphs are appropriate models for our purpose. In what follows we



(a) 3 various cases: $\beta = 0.1$(Blue), $\beta = 0.2$(Red), $\beta = 0.3$(Green)



(b) 3 various cases: $\alpha, \beta = 0.1$(Blue), $\alpha, \beta = 0.2$(Red), $\alpha, \beta = 0.3$(Green)

Fig. 3: Numerical Results: show the radio range vs. number of nodes

provide an important lemma introduced in [24] for the cover time of random regular graphs.

Lemma 4: Let $k \geq 3$ be constant. Let $\mathcal{G}_k$ denote the set of k-regular graphs with vertex set $V = \{1, 2, \ldots, n\}$. If G is chosen randomly from $\mathcal{G}_k$, then *w.h.p.*

$$C_G \sim \frac{k-1}{k-2} n \log n \tag{19}$$

Proof: See [24]. ■

According to this lemma the cover time of the random regular graphs are nearly optimal. The reasoning that leads us to utilize random regular graphs as a model for secured random geometric graphs is that in the latter, every node with high probability has k neighbors in its radio range which are in possession of a common key if Theorem 2 holds. This is obviously equal to a random graph in which every node has k neighbors and as Theorem 2 holds, the geometric nature of these graphs dose not play significant role. In what follows we investigate asymptotic cover time of the secured random geometric graphs.

Theorem 3: Assume that $\mathcal{G}^2(n, r)$ be a secured random geometric graph with $r^2(n)$ satisfying $r^2(n) \geq \frac{1}{4\pi - 2\alpha} \frac{\log(n)}{n^\beta}$ where $\alpha, \beta \in (0, 1)$. Then the cover time is $O((1+\gamma) n \log(n))$ where $\gamma = 1/(\alpha n^\beta - 2)$.

Proof: By substituting αn^β with k in (19) the desired result is obtained. ■

Recall that according to [24] the asymptotic cover time of random geometric graph is $\Theta(n \log n)$. Thus, asymptotic cover time of secured version of such graphs is only by a factor $O(n^\beta)$ worse than random geometric graph, which proves our aforementioned claim.

V. Numerical Results and Simulations

The obtained formulas and analysis have been validated by means of both simulation and numerical results. We implemented a secured WSN using OMNET++ [25] simulator. We also implemented our formulas in MATLAB [26] in order to present numerical results for such a network with various parameters. Numerous validation experiments have been established, however, for the sake of specific illustration, validation results are presented for two scenarios in nodes are scattered in a unit square $[0, 1] \times [0, 1]$ with $n = 100$ and $n = 10000$ nodes.

The numerical results depicted in Figures 3, illustrate the radio range $r^2(n)$ versus the number of nodes n in the network. In both figures, X-axis and Y-axis show the number of nodes and the radio range of each node, respectively. Three different parameters have been examined for n ranging from 1 to 100. In Figure 3.(a), the parameter β has been varied in each of the curves. This figure reveals that for sufficiently large n, as β increases the radio range decreases, accordingly. This is due to the fact that increment in β increases the probability of common key possession leading to expanding the neighborhood of each node which effectively reduces $r^2(n)$. In Figure 3.(b), in addition to the parameter β, α also has been changed in each of the curves. This figure as well as the previous one, shows that for sufficiently large n, as β and α increases the radio range decreases significantly. Comparing these two figures also reveals that for the same n, the radio range in Figure 3.(a) is smaller than that of the other figure which confirms that to achieve better cover time we must sacrifice more energy (by rising the radio range). It is also worth mentioning that the radio range in both cases diminishes as the number of nodes becomes larger and larger.

The simulation results are depicted in Figures 4 and 5. Figure 4 is a log-log plot which shows the tradeoff between connectivity, i.e. the fraction of nodes that are connected to each other, and the radio range of each node in two different cases: $n = 100$ and $n = 10000$. As shown in the figure, the connectivity of the network increases as the radio range rises in both cases. However, the connectivity of the case in which n is greater, grows faster than the other case. These results are not surprising since we distribute sensor nodes in the unit square in either case. In order to validate Theorem 2, we consider a WSN with $n = 10000$, where $\alpha = \beta = 0.2$ and vary the radio range from 0 to 0.14 where step size was 0.02. For each radio range the average degree ratio (i.e. average degree nodes divided by k) of the network is calculated. Figure 5 plots the average degree ratio for various radio ranges. The figure confirms that at a specific step i.e. radio range equal to

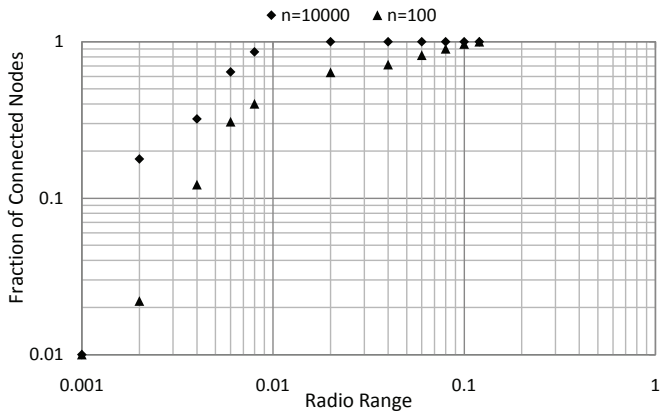


Fig. 4: log-log plot : shows tradeoff between connectivity and radio range

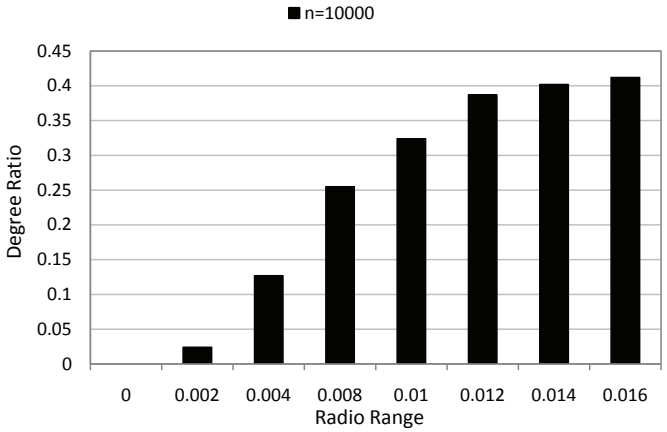


Fig. 5: The Average Degree Ratio for Various Radio Ranges

0.12, the average degree ratio reaches to its saturation point. Exactly the same result can be obtained using Theorem 2.

VI. Conclusion

In this paper, a secured wireless sensor network with n nodes is considered. Each node was supposed to extent its radio range to a circle with radius $r(n)$ and possesses a finite set of keys (called key-chain). Sensors having identical keys communicate with each other directly and the probability that a node have at least one such identical key with every other node is defined as $p(n)$. We provided a lower bound for the radio range under which the underlying network remains connected. We also investigated an optimum lower bound which leads to a lower cover time of the network. It is also shown that asymptotic cover time of secured random geometric graphs is only by a factor $O(n^{\beta})$ worse than non-secured version of such graphs. Our next steps target to elaborate on the problem of base-station positioning in such networks.

References

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", *Computer Networks*, vol. 38, no. 4, pp. 393-422, March 2002.

[2] L. Zhou and Z. J. Haas, "Securing Ad Hoc Networks", *IEEE Network Magazine*, vol. 13, no.6, 1999.

[3] S. Zhu et.al, "Leap: Efficient security mechanisms for large scale distributed sensor networks". *In Proc. of 10th ACM Conference on Computer and Communications Security (CCS03)*, pp. 62-72, 2003.

[4] F. Stajano, and R. Anderson, "The resurrecting duckling: security issues for ad-hoc wireless networks", *LNCS*, vol. 1796, pp. 172-182, Dec 2006.

[5] G. Elias, A. Miri and T.H. Yeap, "High-Performance FPGA Based Hyperelliptic Curve Cryptosystem", *In Proc. of 22th Biennial Symposium on Communication*, vol. 33, pp. 349-366, Sep 2004.

[6] D. Malan, M. Welsh and M. Smith, "A public-key infrastructure for key distribution in tiny os based on elliptic curve cryptography", *In Proc. of 1st IEEE International Conference on Sensor and Ad Hoc Communications and Networks (SECON04)*, pp. 71-80, Oct 2004.

[7] G. Gaubatz, J. P. Kaps, and B. Sunar, "Public key cryptography in sensor networks". *In Proc. of 1st European Workshop on Security in Ad-Hoc and Sensor Networks (ESAS04)*, 2004.

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

[9] N. Linial and A. Wigderson, "Expander graphs and their applications", Lecture Notes, Hebrew University, Jan 2003.

[10] S. A. Camtepe, B. Yener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", *In IEEE/ACM Transactions on Networking*, vol. 15, no. 2, 2007.

[11] H. Shafiei, A. Khonsari, A. Mehdizadeh and M. Ould-Khaoua, "A Combinatorial Approach for Key-Distribution in Wireless Sensor Networks", *in Proc. of GLOBECOM'08*, pp. 138-142, 2008.

[12] M. R. Murty, "Ramanujan Graphs", *J. Ramanujan Math. Soc.*, Vol. 18, No.1, pp. 1-20, 2003.

[13] A. Ben-Aroya, A. Ta-Shma, "A combinatorial construction of almost-ramanujan graphs using the zig-zag product", *In Proc. STOC'08*, pp. 325-334, 2008.

[14] S. Shakkottai, R. Srikant and N. Shroff, "Unreliable sensor grids: Coverage, connectivity and diameter," *Ad Hoc Networks*, 2005.

[15] F. Xue and P. R. Kumar, *Scaling Laws for Ad Hoc Wireless Networks: An Information Theoretic Approach*, NOW Publishers, 2006.

[16] A. Durresi, V. K. Paruchuri, S. Sitharama Iyengar, R. Kannan, "Optimized Broadcast Protocol for Sensor Networks," *IEEE Transaction on Computers*, Vol 54, no. 8, 2005.

[17] H. Guo, F. Ingelrest, D. Simplot-Ryl and I. Stojmenovic, "Performance Evaluation of Broadcasting Protocols for Ad Hoc and Sensor Networks," in *Challenges in Ad Hoc Networking*, Springer Boston, 2006.

[18] A.K. Chandra, P. Raghavan, W.L. Ruzzo, R. Smolensky, and P. Tiwari, "The Electrical Resistance of a Graph Captures its Commute and Cover Times," *Journal of Computational Complexity*, pp. 312-340, 1997.

[19] R. Elsässer, T. Sauerwald, "Cover Time and Broadcast Time," *in Proc. of Symposium on Theoretical Aspects of Computer Science*, pp. 373-384, 2009.

[20] D. Kempe, A. Dobra, J. Gehrke, "Gossip-based computation of aggregate information", *in Proc. of IEEE Symposium on Foundations of Computer Science*, pp. 482-491, 2003.

[21] N. Sadagopan, B. Krishnamachari, A. Helmy, "Active query forwarding in sensor networks", *Ad Hoc Networks*, 2003.

[22] D. Braginsky, D. Estrin, "Rumor routing algorithm for sensor networks", *in Proc. of the 1st ACM Int. workshop on Wireless sensor networks and applications*, pp. 22-31, 2002.

[23] C. Avin, G. Ercal, "On The Cover Time of Random Geometric Graphs," *in Proc. of ICALP*, pp. 667-689, 2005.

[24] C. Cooper, A. Frieze, "The Cover Time of Random Regular Graphs," *SIAM J. Discrete Math.*, Vol. 18, no. 4, pp. 728-840, 2005.

[25] OMNET++ Simulator. [Online]. Available: http://www.omnetpp.org

[26] MATLAB version 7. The MathWorks Inc., 2009.