Towards A Theoretically Bounded Path Key Establishment Mechanism in Wireless Sensor Networks

Aishwarya Mishra
School of Information Technology
Illinois State University
Normal IL 61790 USA
amishra@ilstu.edu

Tibor Gyires
School of Information Technology
Illinois State University
Normal IL 61790 USA
tbgyires@ilstu.edu

Yongning Tang
School of Information Technology
Illinois State University
Normal IL 61790 USA
ytang@ilstu.edu

***Abstract*—Random Key Pre-distribution Scheme (RKPS) guarantees any pair of neighboring nodes in a Wireless sensor network (WSN) can build a secure connection either directly or through a path key establishment mechanism (PKEM). For any pair of neighboring sensor nodes without a direct secure connection due to unfound common key, a node can resort to PKEM to flood a keyrequest in the connected graph to reach the neighboring node and build a secure connection thereafter. One remaining challenge in PKEM is to find an optimal transmission radius for flooding. Commonly used empirically or probabilistically bounded flooding mechanisms may cause high power consumption on sensor nodes and also easily be exploited to launch power exhaustion Denial of Service (DoS) attacks to sabotage a WSN. In this paper, we tackle this challenge by first theoretically analyzing the upper bound of diameter in Erdős-Rényi (ER) random graph theory, and then verifying the performance of theoretical bounded PKEM using simulations. The performance evaluation shows both the correctness and effectiveness of our proposed theoretically bounded path key establishment mechanism.**

***Keywords*- sensor networks, random key predistribution, graph diameter, random graph, theoretical bound, path key establishment mechanism.**

I. INTRODUCTION

With the growing prevalence of wireless sensor networks (WSNs), security becomes extremely important for WSN-based applications [1], [5], [17], [19], [20], [28], especially when they are deployed in hostile environment. One of proposed solutions for resource constraint WSNs is Random Key Pre-distribution Scheme (RKPS) [1], which guarantees any pair of neighboring nodes in a WSN would be able to build a secure connection either directly or through a path key establishment mechanism (PKEM).

The first Random Key Predistribution Scheme was proposed in [1] and emerged as a promising solution for WSNs. RKPS is fully distributed and allocates shared secret keys to each sensor node in such a manner that the adversarial compromise of a fraction of the nodes does not impact the security of the complete network. This scheme relies on allocating on each sensor before deployment a small random subset of keys (keyrings) from a large universal set of random keys (keypool), such that each keyring overlaps with any other keyrings with a small probability.

RKPS pre-distributes the keys in such a way that each sensor node in a deployed WSN can directly build secure wireless connections with at least a fraction of its neighboring nodes, where common keys can be found in their pre-distributed key pools. By properly selecting the RKPS parameters (e.g., keyring size), a connected graph among all sensor nodes in the WSN can be constructed, in which a network path composed of one or multiple wireless connections can be found for any two nodes according to Erdős-Rényi (ER) random graph theory. For any pair of neighboring sensor nodes without a direct secure connection due to unfound common key, a node can resort to PKEM to flood a keyrequest in the connected graph to reach the neighboring node and build a secure connection thereafter. It is worth noting that flooding is the required messaging mechanism at the initial phase of trust establishment among sensor nodes. More effective routing mechanisms [2] can be applied later among trusted sensor nodes.

One remaining challenge in PKEM is to find an optimal transmission radius for flooding. Commonly used empirically or probabilistically bounded flooding mechanisms may cause high power consumption on sensor nodes and also easily be exploited to launch power exhaustion Denial of Service (DoS) attacks [29] to sabotage a WSN.

In this paper, we tackle this challenge by first theoretically analyzing the upper bound of diameter in Erdős-Rényi (ER) random graph theory, and then verifying the performance of theoretical bounded PKEM using simulations. The performance evaluation shows both the correctness and effectiveness of our proposed theoretically bounded PKEM.

The rest of the paper is organized as the following. Section II discusses the related work. Section III provides the background of PKEM and derives the theoretical bound of flooding radius in PKEM. Section IV and Section V present our simulation design and results. Finally, Section VI concludes the paper.

II. Related Work

Research on RKPS was first introduced in [1]. A variety of schemes have been proposed [16], [17], [19]–[21], [28] built upon the basic RKPS by combining with other key predistribution schemes for improving sensor network security [18], [26]. These schemes have been reviewed in [5], which also covered an extensive survey on the state-of-the-art in sensor network security. Since our problem is tangential to the RKPS that is assumed in our work, we focus on reviewing PKEM related research work in the past [2], [7]–[9].

Further results pertinent to our work are found in [11], which discussed the application of graph theory to RKPS in the context of sensor networks, and produces validating results for specific ranges of its parameters. The work in [1] presented empirical observations that the length of any keypath does not exceed an estimated constant number for their simulation cases with $1000 \sim 10000$ nodes, but did not provide formal mathematical guidance which could characterize how PKEM will behave for much larger node populations. Another contribution in [1] was the explicit statement of the assumptions related to the minimum degree of the underlying connectivity graph, which had been assumed to be higher than the maximum number of neighboring nodes supported by modern wireless MAC layer protocols.

The first attempt of using a TTL limited path key establishment appears in [11], which aimed at limiting the overhead of the RKPS scheme. However, they were mainly interested in observing the average lengths of various keypaths by repeating the same experiments as in [1]. The result from [11] also noted that most of the actual keypath lengths were much smaller than the observed maximum length. However, they did not characterize the asymptotic behavior of the PKEM and how the length of a keypath was affected by the node population, and deployment density.

The work in [12] followed the same directions as [6] and proposed a theoretic graph framework for parametric decision making for RKPS, optimal keyring size, and network transmission energy consumed in PKEM. Some simulation guidance can be found in [12] showing the approach to the construction of a high performance simulation, which is also adopted in our simulation design. However, impractical full-visibility was assumed in [12]. Moreover, only the average length of keypaths was investigated other than the nature of the longest keypaths.

In contrast to the previous research discussed above, our work focuses on finding the maximum required length of keypath under the practical sensor network model with limited visibility and the consideration of expected node populations, node connectivity, and the power resources of a sensor node.

III. Theoretical Bound Analysis

For a given network with node population n, RKPS applies Erdős-Rényi random graph theory to choose the sizes of keyring k and keypool K, such that the secure network formed resembles a connected Erdős-Rényi random graph. In this paper, an Erdős-Rényi random graph is represented by $G_{(n,p)}$, where n is the number of vertices and p represents the probability that a vertex is connected to any others within the graph. A graph where all the nodes are connected into a single giant component is denoted as a connected graph.

A. Trust Graph

Secure connectivity between neighboring nodes in a sensor network can be represented by a trust graph [3], in which each sensor node is represented by a vertex and a secure connection between any two nodes is represented by an edge. Similarly, the underlying wireless connectivity in the sensor network can also be represented in the form of a connectivity graph, where each sensor represented by a vertex is connected to all other sensors within its transmission range. It is worth noting that the trust graph is contained within the connectivity graph and by definition is a sub-graph of the connectivity graph. Figure 1 shows a trust graph example built on the top of a deployed WSN.

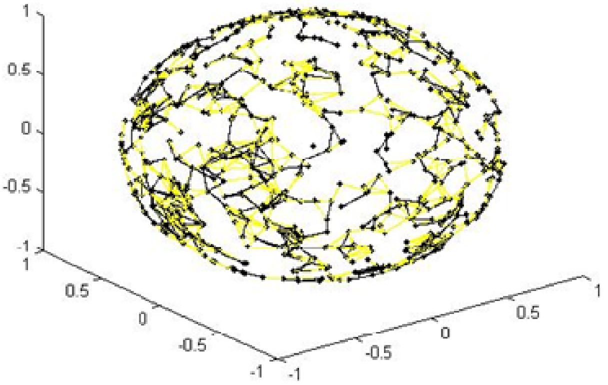

Figure 1: An example of trust graph: lighter edges represent wireless connectivity and darker edges represent secure connectivity.

B. Generalized RKPS Model

Random subsets of keys (keyrings) are chosen from a large pool of keys (keypool), such that any two keyrings may share at least a common key with certain probability. After being deployed, each sensor attempts to establish trust with its neighbors by discovering common key(s) through keyrequests. For any given node u, the small size of keyrings only allows a fraction of u's neighbors directly authenticate the received keyrequest from u. For any u's neighbor node, for instance, v that are unable to directly authenticate u's keyrequest, a path key establishment mechanism (PKEM) can coordinate the trust establishment between u and v.

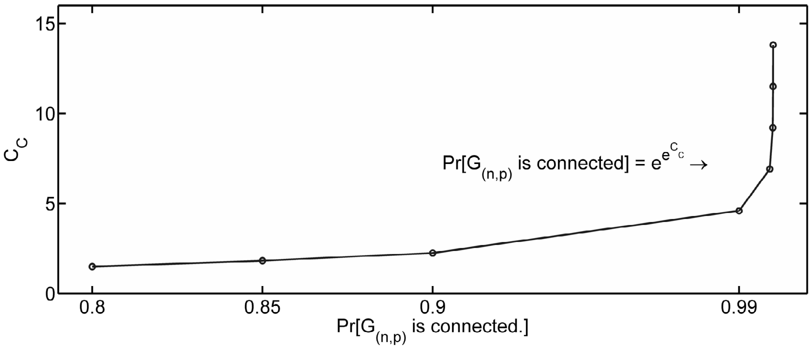

Figure 2: The impact of C.

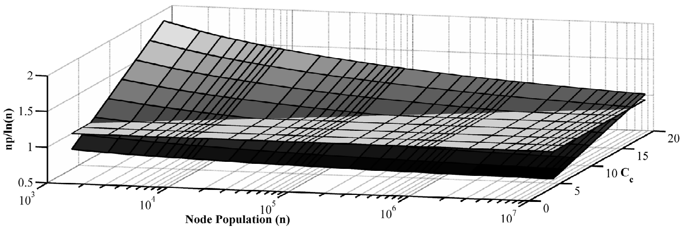

Figure 3: Plot of $np/\log(n)$ showing the value of C for various ranges of n and C.

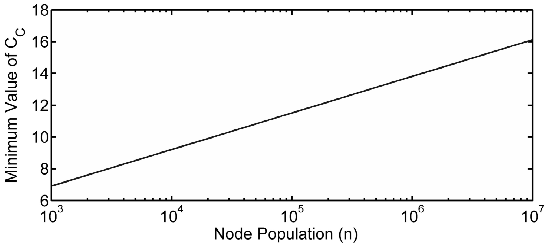

Figure 4: Plot showing $C = \log(n)$, values of C where $np/\log(n) = 2$.

With the support of PKEM, v forwards the indirectly authenticated keyrequest from u to its trusted neighbors which either authenticate or forward it to their trusted neighbors until a transitively trusted node authenticates the targeted neighboring node u. RKPS chooses the keyring and keypool sizes such that the secure network formed by the deployed sensors can be modeled as a connected ER graph, and the keyrequest would potentially be forwarded to all nodes connected securely to each other.

A repeatedly forwarded keyrequest describes a path through the network, where each node within the path trusts the next node in the path, termed as a keypath [1]. As a consequence of PKEM, multiple keypaths emanate from the node requesting PKEM authentication of a particular keyrequest, and a large number of the connected sensor nodes within the network consume power in computation and communication to authenticate a single keyrequest. Initial research on RKPS [1] investigated the varying length of keypath to propose an empirical mechanism to limit the length of keypath using Time-To-Live (TTL) parameter on the process of keyrequest. However, the recommended TTL depended upon empirical observations, which may not be applicable to different sizes of WSNs using different deployment schemes.

The deployment model of a sensor network is generally assumed to be uniformly random and the neighboring nodes of any particular sensor after deployment cannot be predicted.

For a random graph $G_{(n,p)}$ [4], [13], [25], we have:

$$if \quad p = \frac{\ln(n)}{n} + \frac{C}{n} \tag{1}$$

$$then \lim_{n\to\inf} P(G_{(n,p)}\ is\ connected) = e^{e^{-C}} \tag{2}$$

where C is a constant and should be chosen such that the chance of having a connected graph $P(G_{(n,p)}\ is\ connected)$ is close to 1.

Prior research [1] on RKPS has recommended choosing the value of C between 8 and 16, as shown in Figure 2. which can yield the desired value of p, and further derive the keyring size (k) for a given keypool size (K).

It is worth noting that the ER graph theory assumes that any node within a given graph can be connected to any others, i.e., every node can see any others within the network (full visibility model). However, in sensor networks a sensor node is only connected to a small subset of n_a ($n_a \ll n$) randomly deployed nodes, which are within its communication range (limited visibility model). In order to overcome this practical limitation, the work in [1] proposed adjusting p to the effective probability (p_a).

By introducing the concept of effective probability, a node can connect to any of its neighboring nodes, such that the average degree d of the nodes in the graph remains constant as shown below:

$$d = (n_a - 1)p_a = np \tag{3}$$

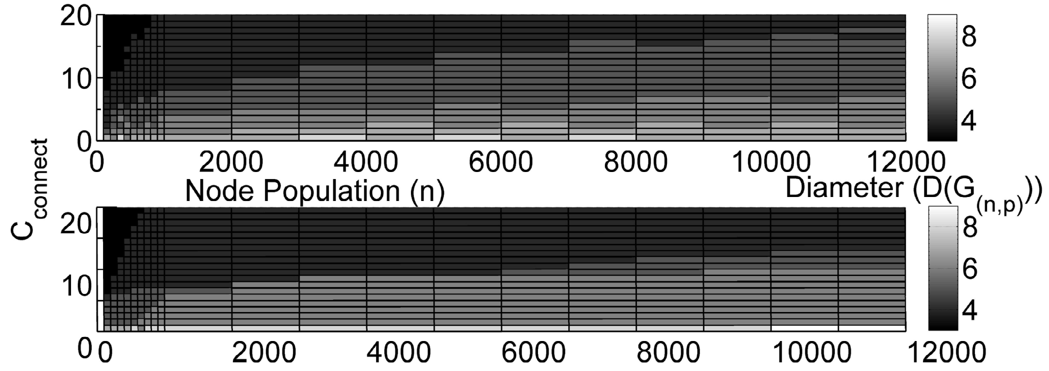

Figure 5: The comparison of practical and theoretical graph diameters considering the impact of C.

With this calculated value of p_a, the work in [1] derived k according to the following equation:

$$p_a = 1 - \frac{(K-k)!^2}{K!(K-2k)!} \tag{4}$$

The results identifying the upper bound on a random graph diameter for the parameter ranges assumed in the discussion above have also been proposed in Theorem 4 in [13], where $p \geq c\log(n)/n$.

C. Diameter of a Sparse Random Graph

Theorem 4 in [13] states that given Eq. 5, the diameter of the graph is concentrated.

$$\frac{np}{\log n} = c \geq 2 \tag{5}$$

$$diam(G_{(n,p)}) \leq \lceil \frac{\log n}{\log np} \rceil \tag{6}$$

This formula gives the theoretical upper bound on the diameter of a sparse random graph. Please note that we are assuming $c \geq 2$ because the value of the constant C typically chosen sufficiently high.

We utilized the Matgraph [14] library in MATLAB to verify by simulating the above theoretical results on several instances of random graph for various values of n when $c = 1$. Figure 3 confirms the theoretical results above. It is worth noting that the diameter values remain relatively stable for large increments of n, which should allow the future extension of a sensor network, even with the current limited diameter. We also notice that the observed diameter value is far below the one predicted by the theoretic analysis, which would make it robust against transmission failures in the shortest path.

As discussed earlier, most empirical studies of RKPS have assumed a value of C in the range of 8 to 16. Figure 3 and Figure 4 plot the value of C in Eq. 5 and Eq. 6 showing C can be safely assumed higher than 2 for lower ranges of n and higher ranges of C in Eq. 1. These values are coincident with the range assumed in prior research on RKPS schemes.

The value of C in Eq. 1 has significant impact upon whether c in Eq. 5 is in a range where the diameter of the random graph remains $O(\log(n)/\log(np))$. Figure 5 implies that lower values of C in Eq.1 will not allow the diameter of the graph to remain small.

IV. Simulation Design

Our simulations are designed to verify the characteristics of trust graph using RKPS scheme with various ranges of n, p and C to validate whether the obtained trust graph from simulations follows the theoretical results. We generated random topologies for sensor networks by varying the number of nodes from 1000 to 5000, and calculate the corresponding keyring sizes from a keypool of 100000. While pursuing the construction of our simulations, we also identified an important implicit assumption that the minimum degree of the underlying connectivity graph of a sensor network should be higher than the maximum expected degree of the trust graph as the results from [15].

In order to investigate the effective diameter of a trust graph in a WSN, we created a sensor network simulator along the directions discussed in [22]. Our simulator model derives the keying size based on [1], and allows for variations in the sensor network deployment densities through node range variation.

Most of the simulation studies in recent studies [1], [6], [15] have used a unit square as the deployment area with varying transmission ranges to simulate different node densities. More recently, the work in [22] identified the boundary effect that occurs at the borders of any sensor network, where the boundary sensors do not enjoy the average neighborhood connectivity available to nodes away from the boundary. To eliminate this effect, the work in [22] proposed the deployment of the sensor network on a spherical surface to eliminate the boundary effect and produce a sensor network model, which can be used to test the hypothesis assuming homogeneous node connectivity. Boundary effect can significantly influence the degree distribution of a trust graph in simulations but its impact in practical deployments

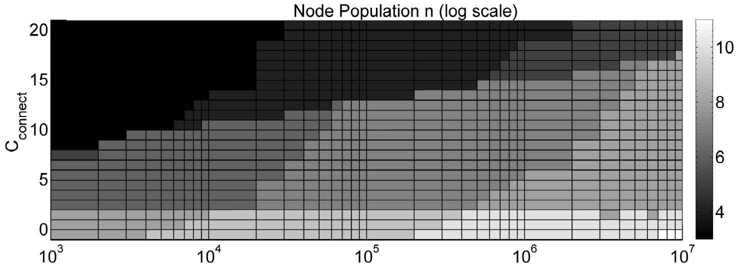

Figure 6: Log range plot of diameter for various ranges of n and C.

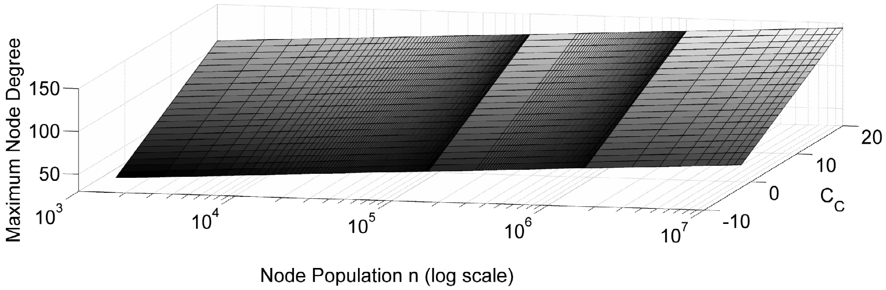

Figure 7: Asymptotic plot of required maximum node degree for large sensor networks.

is considerably less and further mitigated if the nodes on the boundary resort to dynamic range extension as suggested by [23]. Following the directions from the work in [22], we model our node deployment using Ziggurat method due to Marsaglia [24] to generate uniformly distributed points on a spherical surface. We calculate the node distances using the greatest circle arc length. But we also assume that the node range is a disk shaped area on the surface of the sphere equivalent to the one formed on a plane, which allows us to model practical planner deployment, while eliminating the boundary effect.

V. Simulation Result

Figure 6 and Figure 7 plot the log range theoretical predictions from the theoretical analysis results, shown by Eq. 1 to Eq. 5. Several observations and conclusions can be drawn on the basis of these simulations.

The diameter of a deployed sensor network increases very slowly with the increase of network size, and remains constant for large ranges of node populations. This observation shows the promise in the extensibility and graceful degradation of a sensor network deployment, even if the TTL value is controlled as a constant. On the other hand, this shows that controlling the TTL would only provide limited control over the number of nodes visited by a keyrequest and the consequent power consumption of PKEM. The number of nodes which may receive a PKEM request rises rapidly with each increment of TTL in a large network.

Further, Figure 7 also shows that node degrees may rise as high as 140, which is prohibitively high for current sensor node platforms. We note that several methods have been proposed to mitigate this problem including range extension. Another method to allow higher node degrees could be to allow neighboring sensors to transparently repeat a keyrequest broadcast so as to allow a larger number of nodes to respond to authentication. Recent research in the power consumption of available sensor node platforms shows that each wireless transmission can cause very high power consumption.

VI. Discussion and Conclusion

This paper formally studies the communication overhead in path key establishment mechanism (PKEM) and the possible improvement through state-of-the-art research combining sensor network deployment schemes and communication mechanisms with the theoretical results from ER random graph study. PKEM is a variant of flooding broadcasting and specifically an instance of probabilistic broadcasting. While we have focused on PKEM specifically, our results are also extendable to the sensor node revocation protocol for RKPS, which also relies on broadcasting.

We have presented and tested an analytical model which provides simplified guidance on the TTL configuration of PKEM for large sensor network deployments. We have shown that certain assumptions regarding the modeling of the trust graph are necessary to preserve its properties as embodied in an ER random graph model. Lastly, we studied the predictions of our analytical model for large scale deployment and identified their impact on the feasibility of large scale sensor networks. Our simulations have demonstrated that the theory on random graph approximates the practical observations and can prove to be highly effective especially in the design of large scale sensor networks.

Our work also shows that the secure connectivity and diameter of the corresponding trust graph is intimately related to its deployment density and node connectivity. A graph with poor connectivity would significantly weaken the trust graph and may result in undesirable partitioning of the corresponding sensor network.

Through this work, we hope to trigger a discussion of the problem existed in keyrequest broadcasting methods. In order to securely limit the overhead of randomized broadcasting, generally reducing transmission complexity may be more suitable for wireless sensor networks, especially when they are deployed in large scale. This paper serves to provide a skeleton of theoretical assumptions, which may facilitate the application of ER graph theoretic results to the problem of broadcasting at large.

REFERENCES

[1] 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, Washington, DC, USA, 2002.

[2] C. Karlof, D. Wagner, Secure routing in sensor networks: attacks and countermeasures, First IEEE International Workshop on Sensor Network Protocols and Applications (2003).

[3] P. Roberto Di, V. M. Luigi, M. Alessandro, P. Alessandro, and R. Jaikumar, ”Redoubtable Sensor Networks,” ACM Trans. Inf. Syst. Secur., vol. 11, pp. 1-22, 2008.

[4] P. Erdos and A. Renyi, ”On the evolution of random graph.,” Institute of Mathematics Hungarian Academy Of Science, 1959.

[5] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, ”A survey of key management schemes in wireless sensor networks,” Comput. Commun., vol. 30, pp. 2314-2341, 2007.

[6] J. Hwang and Y. Kim, ”Revisiting random key pre-distribution schemes for wireless sensor networks,” in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004.

[7] S. Zhu, S. Setia, S. Jajodia, LEAP: efficient security mechanisms for large-scale distributed sensor networks, in: Proceedings of The 10th ACM Conference on Computer and Communications Security (CCS 03), Washington D.C., October, 2003.

[8] W. Du, J. Deng, Y.S. Han, P.K. Varshney, A pairwise key predistribution scheme for wireless sensor networks, Proceedings of the 10th ACM Conference on Computer and Communications (SecurityCCS 03) (2003) 4251.

[9] D. Liu, P. Ning, Establishing pairwise keys in distributed sensor networks, Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS 03) (2003) 5261.

[10] H. Chan, A. Perrig, D. Song, Random key predistribution schemes for sensor networks, in: Proceedings of the 2003 IEEE Symposium on Security and Privacy, May 1114, pp. 197 213.

[11] T. M. Vu, R. Safavi-Naini, and C. Williamson, ”On applicability of random graphs for modeling random key predistribution for wireless sensor networks,” in Proceedings of the 12th international conference on Stabilization, safety, and security of distributed systems, NewYork, NY, USA, 2010.

[12] V. Tuan Manh, W. Carey, and S.-N. Reihaneh, ”Simulation modeling of secure wireless sensor networks,” in Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools, Pisa, Italy, 2009.

[13] F. Chung and L. Lu, ”The Diameter of Sparse Random Graphs,” Advances in Applied Mathematics, vol. 26, pp. 257-279, 2001.

[14] Beno, t. Otjacques, F. Feltz, G. Halin, and J.-C. Bignon, ”Mat’Graph: transformation matricielle de graphe pour visualiser des changes lectroniques,” in Proceedings of the 17th international conference on Francophone sur l’Interaction Homme-Machine, Toulouse, France, 2005.

[15] R. Durrett, Random Graph Dynamics. New York, NY: Cambridge University Press 2006.

[16] A.S. Wander, N. Gura, H. Eberle et al., Energy analysis of public-key cryptography for wireless sensor networks, in: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications (PERCOM), 2005.

[17] D. Malan, M. Welsh, M.D. Smith, A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography, in: Proceedings of 1st IEEE International Conference Communications and Networks (SECON), Santa Clara, CA, October 2004.

[18] P. Ning, R. Li, D. Liu, establishing pairwise keys in distributed sensor networks, ACM Transactions on Information and System Security 8(1) (2005) 4177.

[19] M. Eltoweissy, M. Moharrum, R. Mukkamala, Dynamic key management in sensor networks, IEEE Communications Magazine 44 (4) (2006) 122130.

[20] X. Du, Y. Xiao, M. Guizani, H.H. Chen, An Effective Key Management Scheme for Heterogeneous Sensor Networks, Ad Hoc Networks, Elsevier, vol. 5, issue 1, January 2007, pp. 2434.

[21] J. Lee, D.R. Stinson, Deterministic key pre-distribution schemes for distributed sensor networks, To appear in Lecture Notes in Computer Science (SAC 2004 Proceedings) (2004).

[22] T. M. Vu, C. Williamson, and R. Safavi-Naini, ”Simulation modeling of secure wireless sensor networks,” in Proceedings of the Fourth International ICST Conference on Performance Evaluation Methodologies and Tools, Pisa, Italy, 2009.

[23] H. Joengmin and K. Yongdae, ”Revisiting random key predistribution schemes for wireless sensor networks,” in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004.

[24] G. Marsaglia and W. Tsang, The Ziggurat method for generating random variables, 2000.

[25] B. Bollobs, Random Graphs: Academic Press, London, 1985.

[26] M.F. Younis, K. Ghumman, M. Eltoweissy, Location-aware combinatorial key management scheme for clustered sensor networks, IEEE Transactions on Parallel and Distributed Systems 17 (8) (2006) 865882.

[27] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung, ”Perfectly-Secure Key Distribution for Dynamic Conferences,” in Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, 1993.

[28] P. Traynor, H. Choi, G. Cao, S. Zhu, T. Porta, Establishing pair-wise keys in heterogeneous sensor networks, in: Proceedings of IEEE INFOCOM 06.

[29] A.D. Wood, J.A. Stankovic, Denial of service in sensor networks, Computer 35 (10) (2002) 5462.