Yet Another Bounded Broadcasting for Random Key Predistribution Schemes 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*—Wireless Sensor Networks (WSNs) have many promising applications involving unattended deployment in hostile territories. Random key predistribution schemes (RKPS) have been proposed to secure these networks. RKPS require broadcasting within the secured sensor network for key discovery and key revocation. Unbounded broadcasting in RKPS could incur large transmission and computational overheads and may not be sustainable on sensor node platforms, due to their limited power resources. Since the requests are triggered by unauthenticated nodes, this broadcasting can be exploited by a sabotaging adversary to deliberately exhaust the power on the sensor nodes and prevent them from performing their intended function. Enforcing the maximum value of the TTL (MAXTTL) on all nodes of the sensor networks can be an effective approach to mitigating this potential threat if it does not impede the function of the RKPS key discovery and revocation. In this paper, we model the RKPS sensor network as a Random Geometric Graph (RGG) and investigate the upper bounds on RGG diameter as guidance for MAXTTL on all RKPS key discovery and key revocation broadcasts. The simulation results show that our approach is practical and does not impede its function.**

Keywords- sensor networks, random key predistribution, graph diameter, random graph, theoretical bound.

I. INTRODUCTION

Wireless sensor networks (WSNs) comprise of a large population of inexpensive battery-powered sensor nodes that are deployed randomly in a large area. Each node communicates through a wireless radio interface with other neighboring nodes within its wireless transmission range. Consequently, communicating sensors form a wireless ad-hoc network transmitting real-time physical measurements in its deployment area. WSNs have promising applications that require unattended deployment such as environment monitoring and military operations in hostile territory. These applications motivate research in securing WSNs.

Among the proposed WSN security schemes, Random Key Pre-distribution Scheme (RKPS) [1], [2] has shown to be an effective approach that guarantees any pair of neighboring nodes in a WSN would be able to build a secure connection using symmetric cryptography. Modeling a sensor network as a random graph allows RKPS to apply Erdős-Rényi random graph theory to choose an optimal keyring size for a given keypool size. Keyring size is chosen such that each sensor node is able to authenticate at least a fraction of its neighboring nodes, and set up secure connections to these authenticated nodes to form a trust graph. Each sensor node can later authenticate the remaining untrusted neighboring nodes by flooding the trust graph with authentication requests. We term this mechanism as secured flooding since this flooding occurs along the edges of the trust graph only.

Unbounded broadcasting in RKPS may excessively consume computational and transmission power on each sensor node for authentication and retransmissions. An adversary can exploit this weakness to inject bogus authentication requests into a WSN incurring large performance hits on the network over time. These performance hits constitute a Denial-of-Service attack that can be used to sabotage a WSN by draining sensor power and preventing the network from carrying authentic traffic.

Flooding in ad-hoc networks is typically controlled by a TTL value to ensure that a packet will not be forwarded indefinitely within the networks. Prior research [1], [4], [6], [7], [9]–[12] has presented several studies reporting empirical observations and theoretical analysis on the diameter of a WSN. However, they either lack rigorous and repeatable results [1], [6], [7], or have to base upon different assumptions [4], [9]–[12] that may not be applicable for all WSNs.

In this paper, we study a more applicable modeling based on Random Geometric Graph (RGG) to identify the diameter of a WSN for bounding broadcasting in RKPS. We propose a MAXTTL value setting on each sensor node to ensure that packets with TTL values above MAXTTL cannot be injected into the network. The RGG based modeling can more accurately represent a WSN, and thus derive a more applicable MAXTTL value to mitigate excessive power consumption. The simulation results also show our approach is practical and accurate.

The rest of the paper is organized as the following. Section II discusses the related research work. Section III

 ISBN: 978-1-61208-245-5

describes how results on the upper bound of the diameter of Random Geometric Graph (RGG) can be used to derive the value of MAXTTL for a sensor network enabled with RKPS. Section IV describes RKPS in detail and reviews the application of both Erdős-Rényi graph theory and RGG theory relevant to RKPS modeling. Section V present our simulation design and results respectively. Finally, Section VI concludes the paper with future directions.

II. Related Work

In this section, we review prior research that has either proposed guidance on the TTL values for authentication requests, or has some bearing on the derivation of MAXTTL. We also review research on modeling RKPS deployment using RGG theory and the work on upper bound of RGG diameter.

RKPS [1] and its variations have been widely used for securing WSNs, which has been reviewed in [5]. Since this paper is to address a fundamental problem for RKPS, we base our work on a generalized model of the basic RKPS detailed in the next section. This model includes all elements of the scheme that have remained invariant in the derived schemes.

Prior research in [1], [6], [7] had presented empirical observations that the keypath lengths do not exceed a constant number for their simulated WSNs with 1000 to 10000 nodes. However, there is no formal mathematical guidance that could characterize the relationship of the TTL values and the size of WSNs. For example, the first reference to use of a TTL for secured flooding [6] only provided the observation on the average lengths of the keypaths based on the simulation results on a limited node population.

Recent research in RKPS has applied RGG theory to model the highly clustered topology of a practical sensor network deployment. While RGG models the connectivity graph with high fidelity, the presence of edges in the trust graph depends upon the probability with which any two neighboring nodes share a common key. Consequently, RGG with unreliable links has been explored for modeling the trust graph. Di Peitro et al., defined the cryptographs in [8] that model the trust graph as an intersection of a Erdős-Rényi random graph with a RGG graph modeling the deployment. References [9]–[12] modeled the trust graph as a RGG graph, with the presence of edges governed by a Bernoulli function.

It is notable that the authors of [10] also proved connectivity of the RGG with edge probability modulated by a uniform random intersection graph, which shows a theoretical model of the random key predistribution under the full visibility assumption [11]. We discuss these results more formally in the next section.

The authors of this paper have introduced the problem of MAXTTL in [4] and applied theoretical upper bound on the diameter of Erdős-Rényi random graphs to solve it for the full visibility case. In this paper we tackle the practical limited visibility case where a sensor node can only communicate with nodes within their transmission range. This limits their visibility to a much smaller subset of nodes within the network. In our modeling, we applied results from several papers [13], [14] on the application of random graph theory to sensor networks, which discusses the application of Erdős-Rényi random graph theory to RKPS in the context of sensor networks and produces validating results for specific ranges of its parameters. We also used guidance from [14] that discusses the construction of a high performance simulation and allowed us to validate our simulation design.

III. MAXTTL For Secure Flooding

In Figure 1, we show a model of a sample sensor network deployment implementing RKPS, where each sensor node plotted as a node vertex in the graph is surrounded by a circle representing its transmission range. The two overlaid graphs on this model represent the transmission connectivity and secure connectivity respectively. The lighter edged graph among the node vertices represents the connectivity graph formed among a node within its transmission range. The darker edges form the trust graph representing secure connectivity among neighboring node vertices in the connectivity graph. Secure connectivity can be achieved if two neighboring nodes share a common key within their keyrings. Note that the trust graph is a subgraph of the connectivity graph.

While there are more economical broadcasting schemes for ad-hoc networks, flooding may be necessary to ensure speedy and fault tolerant communication of security information in RKPS. In particular, two important protocols in RKPS for authentication and key revocation rely upon secured flooding to accomplish their functions. Authentications typically occur immediately after deployment of a WSN and before the sensor nodes can securely communicate to initialize more optimized broadcasting protocols based on the dominant set in the topology. At this stage the secured sensor network may not be fully connected and a gossiping based broadcast may not reach an authentication node and return back within a bounded time. Key revocation in RKPS aims to remove keys of compromised sensors from the network and also requires speedy announcement of compromised nodes that can be executed by secured flooding in a secure and fault tolerant manner.

As mentioned in the introduction, RKPS secured flooding can have large computational and power overheads that can be exploited to launch DoS attacks. This can be mitigated by setting a maximum limit on the TTL (MAXTTL) on each sensor before deployment. A node receiving a flooded packet will ensure that the contained TTL less than MAXTTL before forwarding it. This will ensure that an adversary

 ISBN: 978-1-61208-245-5

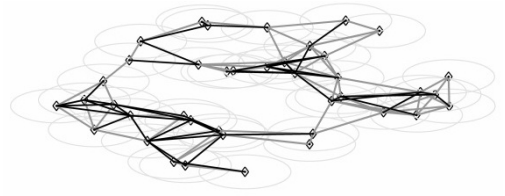

Figure 1: A sensor network secured with RKPS.

injecting packets with long TTL can only inflict limited damage to a RKPS sensor network.

Recent research in RKPS based schemes has utilized RGG for modeling the deployment of a sensor network. MAXTTL can be derived on the basis of the theory related to the upper bound on the diameter of RGG. Diameter of a random graph is the longest of all the shortest paths between every pair of vertices in the graph. Deriving MAXTTL from this value would allow a secured flooding request (SFR) to adequately cover all shortest paths of a connected RGG, without impeding their function.

MAXTTL would also ensure the economy of the RKPS scheme since it would prevent SFRs from traveling on longer redundant paths and cycles within the network. To establish that the paths longer than the diameter are present in a RGG, we observe that longer paths exist between two nodes connected to the nodes between which the diameter exists. By induction, it can be deduced that the diameter can be included in the path between any two pair of nodes accessible by the nodes between which the diameter exists.

Delinquent packets with large TTLs may also get forwarded indefinitely in cycles. The only other solution to prevent forwarding of packets in cycles is to enforce duplicate checking of each packet on every sensor node. Typical secure duplicate checking would require that each sensor spend a prohibitive amount of computational resources for calculating the hashcode for each packet it receives. To prevent cycles of a length l each sensor will need to store a comparable (l) number of hashcodes. There is evidence to suggest that the length of the longest cycles on large random graphs is $O(n)$ [3]. The memory, if it were available could be better used to increase the number of keys in sensor keyrings. We can therefore safely assume its absence.

IV. RKPS Model And Theoretical Analysis

In this section, we first analyze RKPS to show how Erdős-Rényi random graph theory is applicable to choose the size of the keyring for a keypool based on the network size and deployment density. Subsequently, we introduce theory related to RGG connectivity and the analytical results on the upper bound of its diameter that can be directly used to calculate an optimal MAXTTL.

A. Generalized RKPS Model

RKPS predistributes random subsets of keys (keyring) from a large pool of keys (keypool) on each sensor node. Any two keyrings share a common key with a small probability and after deployment each sensor attempts to establish trust with its neighbors by discovering common key(s) through keyrequests. A keyrequest contains a list of key identifiers which uniquely identify each key in a requesting node's keyring. A neighboring node receiving the keyrequest will attempt to find a key in its own keyring. If successful the node will respond back by encrypting a random number with the identified common key (challenge), which must be decrypted by the requesting node and sent back as plain text (response) to complete the authentication. Subsequently, the identified common key can be used to negotiate a shared session encryption key.

Due to the limited memory available on each sensor, the keyring are only large enough to allow a fraction of neighbors to successfully identify common keys in a keyrequest. If a receiving sensor is unable to identify common keys in a keyrequest, it resorts to a path key establishment mechanism (PKEM), where it forwards the keyrequest to the neighbors it is securely connected to. These secure neighboring sensors will in turn either authenticate the keyrequest or forward it to their secure neighbors which will repeat the process until some sensor able to authenticate the keyrequest responds back. RKPS choice for keypool and keyring sizes also ensures that every sensor is securely connected to the rest of the sensor network and the keyrequests sent by it will propagate throughout the network.

A repeatedly forwarded keyrequest constitutes a path through the network, where each node within the path trusts the next node in the path, termed as a keypath [1]. For a single PKEM execution multiple keypaths emanate from the node requesting PKEM authentication of a single keyrequest. Consequently, a large number of the connected sensor nodes within the network will spend power in computation and communication to authenticate a single keyrequest.

RKPS chooses the keyring and keypool sizes such that the secure network formed by direct authentications of the neighboring sensor nodes forms a connected Erdős-Rényi graph, and a keyrequest sent by any node would be forwarded to all nodes within the network. The deployment model of the sensor network is generally assumed to be uniformly random and the neighboring nodes of any particular sensor node after deployment cannot be predicted beforehand. This requires that any sensor node within the network should be able to connect with any other node if they happen to be deployed in each other's neighborhood.

RKPS models the a sensor network in the form of a connected Erdős-Rényi random graph represented by $G(n,p)$, where n is the number of vertices and p represents the probability with which a vertex is connected to any other

 ISBN: 978-1-61208-245-5

vertex in the graph. Erdős-Rényi graph theory introduced in [15] proves that $G(n,p)$ where the value of p is derived according to Eq. 1 will be connected with the probability $P[G(n,p)\ is\ connected]$ shown in Eq. 2. Authors in [1], suggested choice of the common parameter C_C such that $P[G(n,p)\ is\ connected]$ is close to 1.0 in Eq. 2. Figure 2 indicates the value of CC, for the desired values of $P[G_{(n,p)}\ is\ connected]$.

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

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

where C_C is a constant.

Formally, to design a connected $G_{(n,p)}$, we choose value of CC in Eq. 1, such that $P[G_{(n,p)}\ is\ connected]$ in Eq. 2 is close to 1.0.

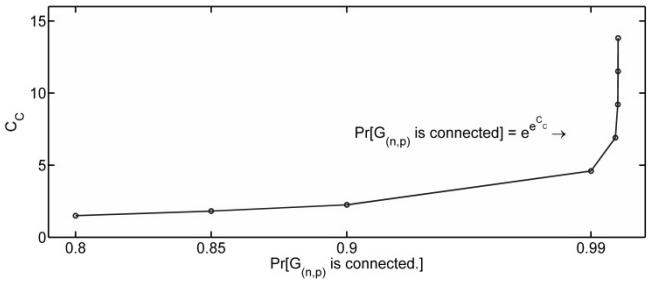

Figure 2: Values of C_C for desired probability of connectivity in Eq. 2.

Prior research in [1] on RKPS identified the desired range for CC is between 8 and 16, as shown in Figure 2. The value obtained for p can be used subsequently to calculate the keyring size (k) for a given keypool size (K) to ensure that the RKPS sensor network is connected with high probability.

B. Full Visibility vs Limited Visibility

It is essential to note, however, that the Erdős-Rényi random graph theory assumes that any node within the graph can be connected to another one, i.e., every node can see any others within the network (full visibility model). However, in practical sensor networks, a sensor node is only connected to a subset of the n vertices, $n_a \ll n$, that represents the expected number of neighboring nodes of a sensor within its communication range (limited visibility model). In order to overcome this practical limitation, the work in [1] proposed scaling p to the effective probability p_a, such that the average degree d_{avg} of the deployed sensors in the network remain equal to the expected degrees of a vertex in the equivalent $G_{(n,p)}$ as indicated in Eq. 3. Note that the p_a represents the probability with which a sensor network will be connected to any node within its neighborhood and this is the probability that will be used to calculate k and K subsequently.

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

The value of p_a, calculated from Eq. 3 is used to derive the keyring size k, from Eq. 4 for a given keypool size K.

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

C. Deployment Modeling of RKPS with RGG

While the original scheme only models the average degree of the connectivity graph, more recent research in key predistribution schemes has formally modeled the connectivity graph as a Random Geometric Graph. Study of Random Geometric Graph (RGG) theory began with [16] and has been adopted generally to study the practical deployment of ad-hoc networks on a planner surface. We borrow the definition from [17] to define the generalized form of RGG, quoted as follows. Let $X_1, \cdots, X_n$ be independent, uniformly distributed random points in the unit cube $[0,1]_d$, where d represents the number of dimensions. The set of vertices of the graph $G_n(r_n)$ is $V = 1, \cdots, n$ while two points i and j are connected by and edge if and only if the Euclidian distance between X_i and X_j does not exceed a positive parameter r_n, i.e., $E = \{(i,j) \parallel X_i - X_j \parallel < r_n\}$ where $\parallel . \parallel$ denotes the Euclidean norm.

Note that by definition the $G_n(r_n)$ is generalized over multiple dimensions d, however the two dimensional case is of specific interest to modeling the spatial deployment of sensor nodes on planner field. The Euclidean norm in this case becomes the distance between any two nodes and r_n corresponds to the transmission range of each node. The points described in RGG correspond to the location of each sensor node uniformly distributed on a unit area $(d = 2)$ that can be modeled as a unit square or unit circle without loss of generality. In the context of modeling the practical sensor network deployment the results obtained from RGG theory can be trivially scaled to the actual deployment area.

D. Connectivity of RGG

While RGG models the graph connectivity with high fidelity, the links of the trust graph are also modulated by the probability with which two neighboring nodes share a common key. As a result, RGG with unreliable links has been explored for modeling the trust graph [10] established the following result for the connectivity of RGG, where p_l and p_n represent the probability of the link and node presence respectively.

$$r = \sqrt{\frac{\ln n + C}{n p_l p_n \pi}} \,|\, n, C \to \infty, p_l, p_n \in [0,1] \tag{5}$$

More recently, research in [11] has investigated routing in a practical sensor network deployment using Random Geometric Graph with randomly deleted edges. They formally

 ISBN: 978-1-61208-245-5

proved results for the following conditions.

$$if \quad \pi p_l r^2 \geq C\frac{\ln n}{n} | C > 8, p_l \in [0,1], r \in (0, 1/\sqrt{\pi}) \tag{6}$$

$$r \geq c\sqrt{\frac{\ln n}{n}} | c > 1.598, p_l \in [0,1], r \in (0, 1/\sqrt{\pi}) \tag{7}$$

Then RGG $G_n(r, p_l)$ is connected with probability tending to 1 as $n \to \infty$, p_l is again the probability of link presence.

E. Network Connectivity Requirement in RGG

Xue et al., in [18] showed that in a two-dimensional RGG where the nodes are distributed uniformly, the number of neighbors of each node need to grow like $\Theta(\log n)$ if the network is connected. Further they also showed analytically that for a RGG where each node is connected to less than $0.074 \log n$ (lower bound) nodes the network is asymptotically disconnected. However, if the nodes are connected to greater than $5.1774 \log n$ (upper bound) nearest neighbors, then the network will be asymptotically connected. Finally, Balister et al., in [19] improved the lower bound to $0.3043 \log n$ and the upper bound to $0.5139 \log n$.

We note [18] and [19] rely upon a Poisson distribution of nodes on a unit disk. Low or rare events [20] allow the approximation of the binomial distribution with a Poisson distribution.

F. RGG Diameter

Ellis et al., [17] have shown two important asymptotic results on the diameters of RGG. Let $\phi(n) \to \infty$ be non-negative. There exists an absolute constant $K > 0$ such that if

$$r \geq \sqrt{\frac{\ln n + \phi(n)}{n}} | n, \phi(n) \to \infty \tag{8}$$

then the unit disk random graph $G(n,r)$ is connected with diameter denoted by $D(G_{(n,r)}) < K(2/r)$. They also derived the value of K analytically to 129.27. In Theorem 7 [17] they prove a still lower bound for the following conditions.

Let

$$r = c\sqrt{\frac{\ln n}{n}} | c \geq 2.26164 \tag{9}$$

Then the unit disk random graph $G_{(r,n)}$ is connected with diameter

$$D(G_{(n,r)}) \leq (4 + o(1))/r \tag{10}$$

V. Simulation Results

We constructed a simulation model to verify the diameter of the trust graph generated in RKPS scheme using direct authentication. The simulation generates random topologies for sensor networks with limited visibility by varying the number of nodes from 1000 to 12000, and calculated the corresponding keyring sizes from a keypool of 100000. The visibility range of each sensor is calculated on the basis of Eq. 9 since it provides an elegant result which can be used to directly calculate the diameter of the random graph.

Our simulation model closely follows the guidance from [14]. The keying size are derived based on the guidance from [1], and allows for variations in the sensor network deployment densities through node range variation according to Eq. 9. We have also taken into account the boundary effect identified in [14] and eliminated it from our final results.

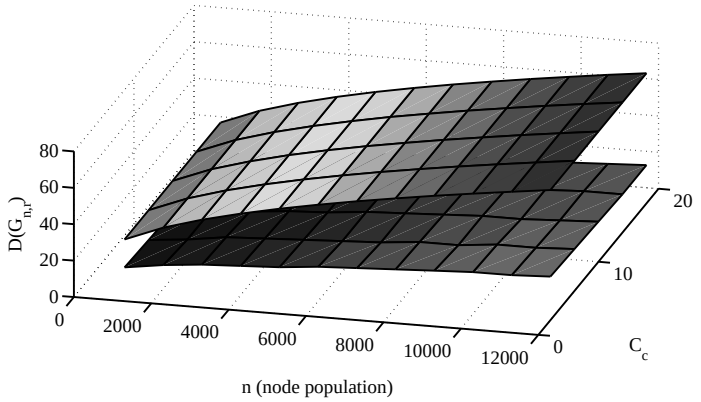

Figure 3: Simulation results and asymptotic predictions for a 12000 node sensor network.

Figure 3 shows a plot of our simulations on MATLAB and Java. The upper surface represents the calculated upper bound. The lower surface represents the actual diameter of the simulated sensor network. The actual diameter of the network is consistently smaller than the prediction for the diameter by a wide margin. However, it is notable that the upper bound on the diameter is much higher than the actual diameter of the network. This indicates that tighter theoretical bounds on the diameter of the Random Geometric Graphs, and consequently the MAXTTL are possible.

However, we recommend keeping a wide margin between the actual MAXTTL and predicted MAXTTL value. The actual value used in practical deployments should be set higher than the predicted value. This is to accommodate the fact that the trust graph is not a perfect Random Geometric Graph. It may have many absent edges between neighboring nodes at the beginning of the deployment, when secure trust relationships have not been established. Theory on faulty Random Geometric Graphs [**?**] is still nascent and upper bound on its diameter may provide a more accurate prediction for the MAXTTL.

Figure 4 shows the prediction of the diameter for sensor networks for large node populations $O(10^6)$. We observe that the diameter is relatively small and grows slowly with the node population $O(log(n)/n)$.

Diameter of the network increases very slowly with network size and remains constant for large ranges of node populations. This shows promise in the extensibility and graceful degradation of a sensor network deployment,

 ISBN: 978-1-61208-245-5

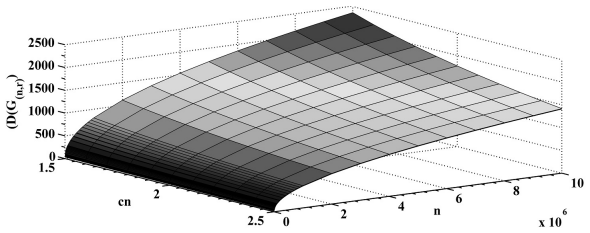

Figure 4: Long range predictions for the sensor network diameters.

even if the MAXTTL value is locked as a constant before deployment. 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 therefore MAXTTL alone may not be well suited for precise control of power consumption for SFRs. The consequent power consumption of PKEM is not precise and the number of transmissions increase rapidly with each increment in TTL value.

VI. Discussion and Conclusion

While we have utilized asymptotic results on RGG graph theory, formal proofs for asymptotic diameters on faulty RGGs is still an open problem. Our simulation results indicate that either the upper bound on RGG diameters holds well for faulty RGGs as well and there is further scope for a tighter upper bound on the RGG diameter. Future theoretical results for tighter bounds on the diameter of RGGs and specifically for faulty RGGs would provide precise bounds applicable to the problem of MAXTTL.

Some form of fault tolerant gossiping may eventually be considered to reduce the transmission overhead and the power consumption of PKEM, however the latency would increase in this case. This would also make the network more vulnerable to worm hole attacks where an adversary is able to exploit the latency between two different parts of the network to launch various attacks.

Finally we hope to trigger a discussion of the problem of secure broadcasting as applied to RKPS, and the analytical modelling of its overhead. We believe that this overhead is unique to RKPS based schemes and may prove to be prohibitive in large networks. Competing public key cryptography like Elliptic Curve do not require a broadcast for key discovery with lower overhead than RSA and that may eventually be more feasible with development in technology.

References

[1] L. Eschenauer and V. D. Gligor, ”A key-management scheme for distributed sensor networks”, in the Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, 2002.

[2] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, ”Perfectly-Secure Key Distribution for Dynamic Conferences”, in the Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, 1993.

[3] B. Bollobs, Random graphs: Cambridge University Press, 2001.

[4] A. Mishra, T. Gyires, and Y. Tang, ”Towards A Theoretically Bounded Path Key Establishment Mechanism in Wireless Sensor Networks”, in the Proceedings of the Eleventh International Conference on Networks, Saint Gilles, Reunion, 2012.

[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 the Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, Washington DC, USA, 2004.

[7] C. F. C. Aldar, ”A graph theoretic approach for optimizing key pre-distribution in wireless sensor networks”, in the Proceedings of the 7th international conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks, Seoul, Korea, 2009.

[8] R. D. Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, ”Redoubtable Sensor Networks”, ACM Trans. Inf. Syst. Secur., vol. 11, pp. 1-22, 2008.

[9] O. Ya?an, ”Performance of the Eschenauer-Gligor key distribution scheme under an ON-OFF channel”, IEEE Transactions on Information Theory, vol. November, 2011.

[10] Y. Chih-Wei, W. Peng-Jun, L. Xiang-Yang, and O. Frieder, ”Asymptotic distribution of the number of isolated nodes in wireless ad hoc networks with Bernoulli nodes”, Communications, IEEE Transactions on, vol. 54, pp. 510-517, 2006.

[11] K. K. a. K. Rybarczyk, ”Geometric Graphs with Randomly Deleted Edges - Connectivity and Routing Protocols”, 2011.

[12] B. Y. Seyit Ahmet Camtepe, Moti Yung, ”Expander graph based key distribution mechanisms in wireless sensor networks”, IEEE International Conference on Communications (2006), vol. June 2006, pp. 2262-2267, 2006.

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

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

[15] P. Erdős and A. Rényi, ”On the evolution of random graph”, Publications of the Mathematical Institute of the Hungarian Academy of Sciences 5: 17-61, 1960.

[16] M. Penrose, Random geometric graphs: Oxford University Press, 2003.

[17] R. B. Ellis, X. Jia, and C. Yan, ”On random points in the unit disk”, Random Struct. Algorithms, vol. 29, pp. 14-25, 2006.

[18] F. Xue and P. R. Kumar, ”The number of neighbors needed for connectivity of wireless networks”, Wirel. Netw., vol. 10, pp. 169-181, 2004.

[19] P. Balister, B. Bollobs, A. Sarkar, and M. Walters, ”Connectivity of random k-nearest-neighbour graphs”, Adv. in Appl. Probab., vol. 37, pp. 1-24, 2005.

[20] A. Papoulis and S. U. Pillai, Probability, Random Variables, and Stochastic Processes: McGraw-Hill, 2002.

[21] J. Diaz, J. Petit, and M. Serna, ”Faulty random geometric networks,” Parallel Processing Letters, vol. 10, pp. 343-357, 2000.

 ISBN: 978-1-61208-245-5