Performance Analysis of Random key Pre-distribution Scheme for Multi-Phase Wireless Sensor Networks

Bhupendra Gupta and Ankur Gupta

***Abstract*—We consider a wireless sensor network where nodes are randomly distributed in a geographic region. These nodes are battery operated. We assume that these nodes can fail at any time after deployment. These failures may cause shortage of nodes and hence various disability in the network. To overcome this we consider a multiphase wireless sensor network. In such a network, nodes are periodically re-deployed to ensure the connectivity of the network. In this article, we give the analytical results for the number of nodes re-deploy at each generation and average age of a node picked at random from the network. We also gives the condition for that an active link is not compromised when a number of nodes has been compromised.**

***Index Terms*—Vertex degree, connectivity distance, wireless LAN, wired LAN.**

I. Introduction

A wireless ad-hoc network is characterized by a set of autonomous nodes that are distributed over a geographic region. These nodes are communicated with each other by forming a secure link between each other in a decentralized manner.

When these nodes are deploying in a hostile environment, the security of ongoing communication becomes extremely important. To ensure the security of such a network various schemes are proposed.

One of them is the public key cryptography that has been used for many years for wireless sensor networks. The cryptographic methods used in wireless sensor networks must satisfied some constraints like number of sensor node in the network, processing time, power consumption and sensing radius of the sensor nodes. The situation became complex as the network becomes extremely large and new security traits have been introduced, the public key cryptography becomes inefficient and can rarely be used. A complete survey on security issues in wireless sensor network has been given in [7]. Most of the existing schemes are based on the basic public key cryptography, like Diffie-Hellman key agreement [8] and RSA signature [9]. Both [8] and [9] do not have trust on the selection of the parameters like network size, sensing radius, low power techniques etc. [1, 2, 10, 11, 12] shows that it is feasible to apply public key cryptography to the wireless sensor networks by appropriate selection of the parameter. One of the most popular schemes used today for secure wireless network is the random key pre-distribution scheme (RKP). The scheme was first introduced by Eschenauer and Gligor[1] and later on extended by Chan, Perrig and Song [2]. Their result is based on the well known random graph model and the classical result on connectivity of the graph by Erdos and Renyi[5]. In RKP, each node is equipped with a set of key called key-ring of size K_n when deploy. These keys are randomly drawn from a common key-pool of size P_n maintained at a secure site. The key-ring is then used to form a secure link between a pair of node that shares at least one common key in their respective key-ring. In [4], authors raise a question under the assumption of full visibility that for a secure wireless network, what should be the size of key-ring and key-pool? Here full visibility means every node can communicate with every other node by using a pair wise secure communication link. In [6], author's finds out the survivor function i.e. the probability that the graph is k-connected and the expected connectivity for the same random key pre-distribution scheme. A lot of variations of basic RKP schemes are available in the literature. But each of them has their pros and cons.

One drawback of the basic RKP scheme is that when several nodes are compromised there key-ring is exposed to the adversary. So the security of the network is degraded. One possible solution is to periodically refresh the key-pool and reassign the keys to each node. Also the lifetime of a node is limited by their battery power. Also a node can fail or dead at any time after deployment. So the average lifetime of each node is much shorter than the overall operating time of the networks. Hence, it becomes necessary to periodically deploy new nodes as old nodes dead or fail due to some region to ensure the connectivity of the networks. Such a network is called a multi-phase wireless sensor network.

A robust key pre-distribution protocol (RoK) for multiphase wireless sensor networks has been proposed by Claude and Angelo [3]. They partition the key-pool (key-ring) into forward key-pool (key-ring) and backward key-pool (key-ring). They analytically show that the probability of an active link is compromised is constant.

II. Our Model

The lifetime of a node is limited by their battery power. So a node can destroy at any time after deployment. Here, we use a random key pre-distribution scheme for a multi-phase wireless sensor networks. A multiphase wireless sensor network is a network in which nodes that fails at any time are immediately replaced by new nodes to ensure the

Manuscript received May 13, 2012; revised June 20, 2012.

Authors are with the Indian Institute of Information Technology, Design and Manufacturing Jabalpur, MP, India (e-mail: gupta.bhupendra@gmail.com; ankurg@gmail.com).

connectivity of the wireless sensor networks.

Here we assume that n nodes are deployed at bootstrap time (generation 0 , G_0). Nodes that die are fail during generation G_i are immediately replaced by new nodes at generation G_{i+1}. The time between two generations is called generation period.

We assume that a new generation starts after a fixed time period a. We also assume that the lifetime of a node follows the truncated exponential distribution with mean λ and the truncation parameter t. Let X_i denote the number of nodes deploy at generation G_i.

So we can formulate X_1, X_2, X_3, ... as uniformly and independently distributed random variables.

III. NOTATIONS

n	Total number of nodes;
r	Critical transmission radius;
K_n	Size of the Key-Ring;
P_n	Size of the Key-Pool;
K	Vertex Connectivity;
p_s	Probability that two nodes share at least one key;
q_s	$1 - p_s$;

IV. ANALYTICAL RESULTS

The wireless network is exposed to adversary. If a number of nodes are compromised, then all of its keys are expose to the adversary and all the link consist of at least one compromised nodes are also compromised. To ensure the correct operation of the network it is necessary that rest of the network is connected by secure link only. We compute analytically $L_{compromised}$, the fractions of active link compromised indirectly when x nodes are compromised. So, the probability that a given key has not been compromised is defined as:

$$P[A\ given\ key\ has\ not\ been\ compromised] = \left(1 - \frac{K_n}{P_n}\right)^x \quad (1)$$

$$P[A\ given\ key\ has\ been\ compromised] = 1 - \left(1 - \frac{K_n}{P_n}\right)^x \quad (2)$$

As explained in [2], the probability p(i) that two nodes share i common keys is defined as:

$$p(i) = \frac{\binom{P_n}{i}\binom{P_n - i}{2(K_n - i)}\binom{2(K_n - i)}{K_n - i}}{\binom{P_n}{K_n}^2} \quad (3)$$

The Probability p_s that there is a link between two nodes is equivalent to the probability that two nodes share at least one common key in their respective key-ring can be defined as:

$$p_s = 1 - \frac{\binom{P_n - K_n}{K_n}}{\binom{P_n}{K_n}} \quad (4)$$

So, the fraction of total communication compromised can be defined as:

$$L_{compromised} = \sum_{i=1}^{K_n} \left(1 - \left(1 - \frac{K_n}{P_n}\right)^x\right)^i \frac{p(i)}{p_s} \quad (5)$$

Now, we find out the condition on that a link picked at random from the network whose both end nodes are not compromised is not compromised when x nodes are compromised.

Define B_i be an event such that an arbitrary link l_i picked at random from the network uses the keyK_i. Let C_i be the event that the key K_i has been compromised. Then the probability that an arbitrary link has been compromised when x nodes have already been compromised can be defined as:

$$P[l_i\ is\ compromised \mid x] = \sum_{i=1}^{P_n} P[B_i]P[C_i|x]$$

$$= P_n \frac{1}{P_n} P[C_i|x]$$

$$= 1 - \left(1 - \frac{K_n}{P_n}\right)^x \quad (6)$$

Using, $(1 - x) \leq \exp(-x)$ we get,

$$P[l_i\ is\ compromised \mid x] \leq 1 - \exp(-K_n x/P_n) \quad (7)$$

Let $\frac{K_n}{P_n} = \frac{1}{n^c}$ and $n >> x$, also$c > 1$.

We have that the above probability converges to zero for sufficient large value of n, i.e,

$$P[l_i\ is\ compromised \mid x] \to 0 \quad (8)$$

Since nodes can fail or dead at any time after deployment. The fail nodes are re-deploying at the next generation. We are interested in finding out the number of new nodes deploys at each generation. We assume that at generation G_0 there are n nodes in the network i.e. $X_0 = n$. The nodes died or fails in time interval $(0, a)$, where a is some fixed constant, are replaced by new nodes at generation G_i . Since the lifetime of a node follows the truncated exponential distribution. So the probability that a node died in time interval $(0, a)$ can be written as:

$$P\ [A\ given\ Xi\ falls\ in\ time\ interval\ (0,a)] = \frac{1 - \exp(-a\lambda)}{1 - \exp(-\lambda t)} \quad (9)$$

So, the average number of nodes deploy at generation G_i is given as:

$$X_1 = Average\ number\ of\ nodes\ of G_0\ fails\ in\ (0, a)$$

$$= X_0 P[A\ given\ node\ X_i\ fails\ in\ (0, a)]$$

$$= n\ \frac{1 - \exp(-a\lambda)}{1 - \exp(-\lambda t)} \quad (10)$$

Let E_i be the event that a given node dies between

generation $G_i - 1$ and G_i, the probability of event E_i can be written as:

$$P[E_i] = \frac{1}{1-\exp(-\lambda t)} \int_{(i-1)a}^{ia} \lambda \exp(-\lambda x) dx$$

$$= \frac{(\exp(-a\lambda)-1)\exp(-ia\lambda)}{1-\exp(-\lambda t)}. \quad (11)$$

The number of node deploy at a generation i can be given as:

$$X_i = \sum_{j=0}^{i-1} X_j P[E_j]$$

$$= \sum_{j=0}^{i-1} X_j \frac{(\exp(-a\lambda)-1)\exp(-ja\lambda)}{1-\exp(-\lambda t)} \quad (12)$$

The lifetime of a node can vary from 0 to t. We want to find out the average age of a node picked at random from the network. Let the current generation is k. Then the number of active nodes deploy i generation ago, denoted as X(i) can be given as the difference of number of nodes deploy at generation $G_k - i$ and the number of nodes of generation G(k − i) fails in time interval ((k − i)a, ka). So X(i) can be written as:

$$X^{(i)} = X_{k-i} - \frac{X_{k-i}}{1-\exp(-\lambda t)} \int_{(k-i)a}^{ka} \lambda \exp(-\lambda x) dx$$

$$X^{(i)} = X_{k-i}$$

$$\left[1 - \frac{(\exp(-\lambda(k-i)a) - \exp(-ka\lambda))}{1-\exp(-\lambda t)}\right]$$

$$X^{(i)} = X_{k-i}\left[1 - \frac{\exp(-\lambda ka)(\exp(i\lambda a)-1)}{1-\exp(-\lambda t)}\right]. \quad (13)$$

The probability that a node picked at random has average age i can be given as:

$$p(i) = \frac{1}{n} X^{(i)}. \quad (14)$$

So, the average age E[α] of nodes is defined as:

$$E[\alpha] = \int_0^t x p(i) dx$$

$$= \int_0^t \frac{x}{n} X^{(i)} dx$$

$$= \int_0^t \frac{x X_{(k-i)}}{n}$$

$$\left[1 - \frac{\exp(-\lambda ka)(\exp(i\lambda a)-1)}{1-\exp(-\lambda t)}\right] dx$$

$$= \frac{t^2 X_{k-i}}{2n}\left[1 - \frac{\exp(-\lambda ka)(\exp(i\lambda a)-1)}{1-\exp(-\lambda t)}\right]. \quad (15)$$

V. Simulation Results

In this section we give simulated results for average number of nodes to redeploy every generation, and the average age of a node. We consider a network with 500 nodes, generation period $a = 2$, and $\lambda = 1$.

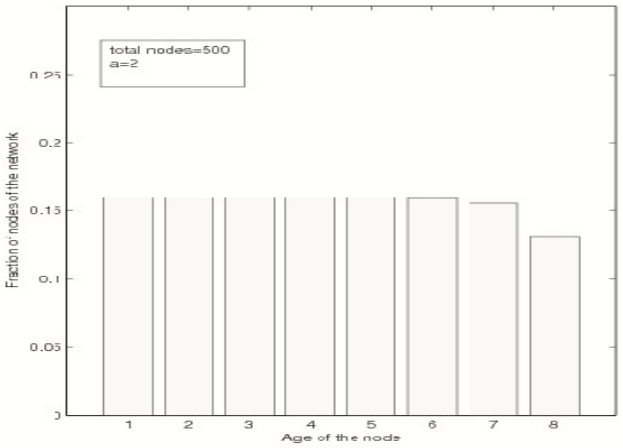

Fig. 1. Average age of the nodes against fraction of the total number of nodes

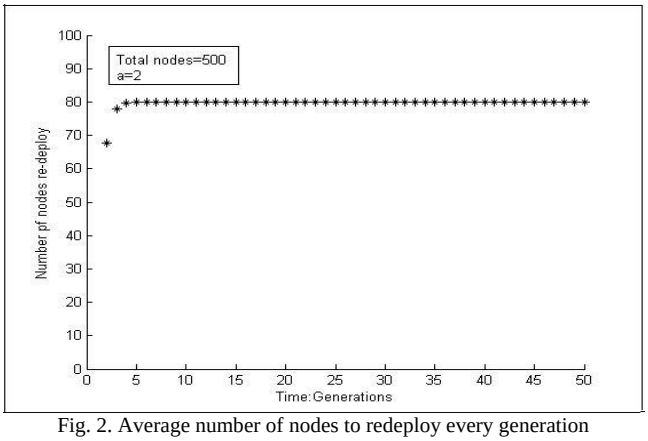

Fig. 2. Average number of nodes to redeploy every generation

From the Fig. 1 and Fig. 2, it is clear that average number of nodes deployed increases in initial few generations and after that became constant, while the fraction of small age of nodes remains almost constant and de-creases of the node of higher ages.

References

[1] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks," *Proceedings of the 9th ACM Conference on Computer and Communication security*, November 2002, pp. 41-47.

[2] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," *Proceedings of the 2003 IEEE Symposium on Security and Privacy*, May 2003, pp. 197-213.

[3] C. Castelluccia and A. Spognardi, "ROK: A robust key pre-distribution protocol for multi-phase wireless sensor networks," *SecureComm 2007-3rd International Conference on Security and Privacy in Communications Networks*, 2007.

[4] Pietro, R. Di and Mancini, L.V., "How to design a connected sensor networks that are provably secure," *Proceedings of the SecureComm 2006, the 2nd IEEE/CreatNet International conference on security and privacy in communications networks*, Baltimore, 2006, pp. 89-100.

[5] P. Erdos and A. Renyi, "On the evalution of Random Graph," *Publ. Math. Inst. Hunger. Acad. Sci.*, 5, pp.17-61, 1960.

[6] R. Palaniswami, M., "Secure k-connectivity properties of wireless sensor networks in mobile Adhoc and sensor systems," *MASS 2007. IEEE International Conference on Digital Object Identifier: 10.1109/*

Yee Wei Law; Li-hsing Yen; Di Pietro, OBHOC.2007.4428764, pp. 1-6.
[7] Y. Wang, G. Attebury and B. Ramamurthy, "A Survey of Security Issue in Wireless Sensor Networks," *IEEE Communication* Surveys,Vol 8, issue 2, 2006.
[8] W. Diffie and M. E.Hellman, "New Directions in Cryptography," *IEEE Trans. Info. Theory*, Vol 22, No. 6, pp 644-654, 1976.
[9] R. L. Rivest, A. Shamir and L.Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Commun. ACM*, Vol. 26, No. 1, pp. 96-99, 1983.
[10] N. Gura, A. Patel, A. Wander, H. Eberle and S.C.Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," CHES'04*: Proc. Wksp. Cryptographic Hardware and Embedded System*, 2004.
[11] A. S.Wander, "Energy Analysis of Public-Key Cryptography for Wireless Sensor Network," *PreCom'05: Proc. 3rd IEEE Int. Conf. Pervasive Computing and Communication*, 2005.
[12] G. Gaubatz, J. P. Kaps and B. Sunar, " Publc Key Cryptograhy in Sensor Networks-Revisted," *ESAS'04: 1st European Wksp. Sequrity in Ad-Hoc and Sensor Networks*, 2004.

Bhupendra Gupta was born in Meerut, U.P., India on 28th Nov. 1976. He is PhD Statistics from Department of Mathematics and Statistics, IIT Kanpur in 2008. He is working as assistant professor in Indian Institute of Information Technology, Design & Manufacturing Jabalpur. MP, India.

Dr. Gupta's area of interest is random networks and their application in various areas like sensor networks etc. His main research interests include communication networks and performance analysis. His current research has concentrated on random networks with application in network security, wireless and sensor networks.

Ankur Gupta M.Tech in CSE from Indian Institute of Information Technology Design & Manufacturing Jabalpur, MP, India in 2011. Presently he is working as a research engineer in Siemens Information System Ltd. His current research is concentrated on random networks, communication networks, and medical image processing and computer vision.