2012 International Conference on Information and Network Technology (ICINT 2012)
IPCSIT vol. 37 (2012) © (2012) IACSIT Press, Singapore

Revisiting Graph Theory with the Help of Probability in Establishment of Pair Wise Keys in Wireless Sensor Networks

Nayan [+], Swapnil Singh and Mahesh Kumar

ICFAI University, Department of Computer Science, Dehradun, India

Abstract. Besides key management techniques, one of the critical aspects of wireless sensor networks is it's effective utilization. The resources (i.e. sensor nodes, energy, key methods) must be properly utilized and channelized for optimum efficiency of Networks without damaging the basic infrastructure. This paper presents a novel way of forming clusters of six nodes and forming trees from connected graphs with the help of Graph Theory. The switching of network in Tree like graph from clusters of node enhances the effectively and will reduce traffic burden. We have calculated our respected probabilities with binomial theorem which makes quite easy to diagnosis, which part of network is more vulnerable, So that a network designer can put emphasis. And thus more robust sensor networks can be designed which is hard to be spoofed.

Keywords: probability, trees, communication radius.

1. Introduction

Wireless network play a crucial role in transferring of data from distant places. Since there updating of resources is not viable. So, it is always a better option to utilize the placed resources completely. These networks are nothing but a replica of graph theory in mathematics .which is best understood by treating each vertex as node and a direct edge as communication link. Besides Security and pair wise keys, seamless data transfer is also a critical issue. Because without the knowledge correct viable path or link. We will end up in huge energy loss and in adverse surrounding energy is very important.

Since connectivity depends upon the node density and communication radius. But to know the exact values of density nodes and communication radius is prime important .These things not only enhances the efficient use of network but also improves the application of security protocols. So, there is a need to deploy pair wise keys with certain probability so that all subunits functions well. The performance of the network much varies with the communication radius, if radius is large then node density will improve but at the same time the traffic and congestion will also increase, because of formation of direct edges between nodes. (i.e.) probability of connection will improve at the cost of high traffic ,high computational time and loss of energy in the form of heat .The main aim of this paper is to cut short the radius without minimizing the connection probability.

According to Leonard Kleinrock and John Silvestersix[3] is a magic number for optimum transmission (radius) for radio networks. In this paper we are using this magic number and applying probability concept we have calculated effective probability of connection between nodes. This paper presents a novel approach to evaluate node density with practical implication. The Switching technique which is used in dealing with clusters and Base station is usually unique of its type. We are assuming that in a wireless sensor networks there are equi- likely two events are possible, either a node is directly connected or will be indirectly connected between two nodes. Since a direct connection is always a better way of communication, until it can't increases traffic burden on networks.

[+] Corresponding author. Tel.: + 9739785912/9431221188.
E-mail address: nayan366@gmail.com.

The rest of the paper is organized as follows. Next section contains literature survey and motivation for our work. In Section 3, we start with different notations and definitions which are used in this paper. Section 4 provides general model of graphs with calculated probability. After that Proposed mechanism is there backed with different formulas to evaluate correct communication radius. Section 6, 7 ends the paper with conclusions and Acknowledgement.

2. Related Work

There are various key distribution schemes are available. Each one has its own merit and demerits. Time has come to look an additional support for wireless sensors. Besides public key cryptography and digital Signature methods which are not suitable for tiny wireless Sensors. We have to implement certain techniques which will enhance the effectively of networks. There are many methods proposed by [4] to have calculative communication radius between nodes. To increase the (node per density) without increasing traffic is asserted beautifully in [4].The dependency is keys in any wireless network is illustrated through Chan , Perrig and Sang [6].[3]In back 1978 Six is called as magic number and still it is suitable for our networks. Large number of keys and long transmission lines are impractical now a days because large development in intrusion systems.

3. Notations

The following notations will be used throughout this paper:-

– G:-Graph

–N:-number of nodes in the network

–E:-edges formed in the network

–R:-communication radius

–P:-Probability of formation of direct edges in the network

–P:-simple probability of edges

–N:-Size of the network

–A:-Area of the network

–Dg:-degree of vertex

–X:-number of nodes captured

–T:-Tree

–F:-Forest

4. Definitions

We start with a brief description of various concepts and definitions used in this paper.

- Definition 1: Graph:-It is a pair of G = (V, E) where V is number of vertices (nodes or points) of the Graph and the elements of E are its edges.
- Definition 2 : Degree of vertex:-if G = (V, E) is a non-empty graph, then set of neighbors of a vertex (V) in G is denoted as d_{ig}
- Definition 3: Connected Graph: - A Graph is called connected if any two of its vertexes are linked by a path in G.
- Definition 4: Forest: - An acyclic graph, one not containing any cycles is called a forest.
- Definition 5: Tree: - A connected forest is called a Tree T .If T is a tree then any two vertices of T are linked by a unique path.

5. Graph Connectivity

In any Wireless sensor network, effectiveness depends upon the connectivity of the G .Between any two nodes there is directed or in directed edge called direct connection or indirect connection. Since we are considering a large area and G is an undirected Graph with n vertices and e edges and applying following constraints:-

- If G is connected, then $e \geq n - 1$
- If G is a tree, $e = n - 1$

We can represent a communication channel by a Graph G, in each vertex n is a user. Each node can collect information from a part of environments. And all the data must be transferred to sink node for further processing. Every cluster of nodes has a Sink node. Which collects all the gathered data. These Sink nodes also transfers data to more potent nodes which has more advance processor .here the use of tree comes in picture, traffic around trees will be less but this traffic are very important from security point of view.

6. General Model

The efficiency of a network depends upon two most important features:-

- The number of direct edges between two nodes.
- radius of a particular area where the number of nodes are placed

Since each node can transmit with same radius, it is very important to know how many nodes are needed for seamless transfer of data in particular radius.

6.1. Probability of direct edge

Consider a case when two nodes want to communicate. Then there are two possibilities either there will be a link between them or there will be no direct edge. We can find the probability of direct edges by applying binominal theorem. n be the total nodes and e is the successful direct edges. Then (n – e) will be Undirected or unsuccessful links between two nodes.

If p will be probability of successful direct edges and q will be probability of not direct edges.

According to law of probability (p + q) = 1

$$^{n}C_{e}(p)^{e}(q)^{(n-e)} \quad (1)$$

In the expansion $(p + q)^n$ gives the probability that when n such experiments are conducted e events are favorable and (n – e) events are unfavorable.

Since probability of both events are same. The above formula can be modified into**:-**

$$^{n}C_{e}(1/2)^{e}(1/2)^{(n-e)} \quad (2)$$

For example: suppose there are n=10, e=5

Then $P_{directedges} = {}^{10}C_5 (1/2)^5 (1/2)^5 = 0.2460$, n=12, e=8 then $P_{directedges} = 0.12$

As the number of nodes will increase the probability will decrease this can be recapitulated with the help of radius of environment of that graph.

6.2. Calculation of direct connectivity between two nodes

Case: 1 According to Eschenauer and Gilgor[2] the probability that two nodes share at least one key (or have a direct edge connection) is P_{actual}= 1-p (two nodes do not share a key)

According to new calculation = 1-p (not a direct edge or indirect edge) = $1-p\ (1- (n_{Ce})\ (1/2)^{e}(1/2)^{(n-e))}$

$$=P_{actual}=(n_{Ce})(1/2)^{e}(1/2)^{(n-e))} \quad (3)$$

Case: 2 According to Chang, Perrig and Song[6] P_{actual} is the actual probability of any two neighboring nodes sharing a pair wise key. If a node can store (m) keys in the network size (n)

$$P_{actual}=m(keys)/n$$

$$(n_{Ce})(1/2)^{e}(1/2)^{(n-e)} * nodes = m(keys)$$

If for a connectivity probability of P=0.99 on n=1000, M=1000*0.99=990

This high number of keys in any network is not feasible

For P=.12, n=12 m=1.44 approximately only two keys are needed to communicate between two nodes.

6.3. Communication radius between two nodes

For a communication radius $d_G \geq 1$.then [4] provides a radius range of all the nodes will be:-

$$r_0 >_{-} \sqrt{-\ln\left(\frac{1-(p)\text{^}1/n}{\lambda\pi}\right)} \quad (4)$$

Example: - let n=500 A=1000*1000 m^2 $\lambda = 5 * 10^{-4}$ for p=0.99 r_o = 83 m

7. Proposed Mechanism to Increase Probability

Let λ (nodes per area) of nodes as λ = n/A Where A is area or having a communication radius r where A = π * r^2.To increase the λ we have to decrease the r because n is constant .We can induce the effective area by modifying A as A = p_{eff} πr^2 where p_{eff} is effective probability for connection between two nodes

$$So, \lambda = n/p_{eff}\pi r^2 \quad (5)$$

For a connected graph $d_G \geq 1$.if $d_G = 0$ then that node is isolated and for that p_{eff} =0.For $d_G = 1$ p_{eff} is maximum According to probability

$$^2C_1 (1/2)^1 (1/2)^1 = 0.50$$

This value is implemented in tree concept.[3] Six is a magic number .so, we are forming cluster of 6 nodes with having maximum p_{eff} when e = 3. it's because maximum probability is achieved when we have n = 2 e = 1 (i.e. p = 0.5) and n = 3 e = 1 (i.e. = 0.375) but this a costly affair. So, we are concentrating on magic number for our calculations. According to binominal theorem:-

$$n_{Ce}(1/2)^e(1/2)^{(n-e)} = n_{C(n-e)}(1/2)^e(1/2)^{(n-e)} \quad (6)$$

For n=6 and e=3 p_{eff} = .3125

We will take this p_{eff} in our radius calculation .so λ_{new} = nodes/p_{eff} πr^2. For magic number n=6with maximum probability =0.3125 A= $5*10^{-4}$

$$r_o \geq \sqrt{-\ln\left(\frac{1-(.3125)^{\wedge}1/6}{(5*10^{-4})\pi}\right)} = 58.8 \text{ m}$$

In the area of A= 1000*1000 m^2 we can form many clusters having a communication radius 56.16 m for effective utilization of nodes ,without disturbing the basic infrastructure. Once the data is gathered from all 6 nodes then it is transferred to sink node that sink node transfers these processed data to base stations. During connection between A Sink node and Base station they have d_G =1.which gave us a maximum probability of connection between two nodes. By applying same formula we can calculate exact optimum radius so that that seamless transfer of data will be possible. Here we are taking number of sink nodes=6.having p_{eff} =.5 which we have calculated earlier.

$$r_o \geq \sqrt{-\ln\left(\frac{1-(.50)^1/6}{(5*10^{-4})\pi}\right)} = 62 \text{ m}$$

7.1. Advantages of calculated probability

- One of the basic advantage of this calculation is that a network designer can predict the sensitivity of different stages in wireless sensor .we have diversified the nodes as simple nodes ,sink and base station nodes .P_{eff} at each stage will give a hint to which protocol to be used so that maximum utilization can be done.
- Another advantage is switching technique so that a tree formation can be achieved by applying simple graph theory concept:-
  If G is a tree, e = n − 1
  Since e = 1 and d_G=1. n=2 sink node and Base station. This technique will reduce the traffic
  Because only Six direct lines will be formed to process the information from 6 clusters.

8. Conclusions

The presented analysis depicts a clear connection between the direct connectivity of nodes in sensor networks .Our Calculations are simple and direct, which is based on binomial theorem. It gives us clear perception that how we can manage and reduce traffic and congestions in networks. By simply applying new protocols and security techniques without knowing probable possibilities, will ultimately results in huge energy loss, which is scarce in regions where these nodes are installed. The correct probability and the use of clusters with formation of trees are practical as well as effective and an efficient technique to carry data from far and distant places.

9. Acknowledgment

The author wants to thank Mr. Gaurav Srivastava, Mr. Nishi Mani and Mr. Nakes Mani for their motivational support throughout this paper.

10. References

[1] (Whitfield Diffie and Martin E. Hellman**)**, *New Directions in Cryptography***,**year 1976 **.**

[2] Laurent Eschenauer and Virgil D. Gligor,A *key-management scheme for distributed sensor networks* **,**ACM Conference on Computer and Communications Security, (year 2002, pages 41-47), {http://doi.acm.org/10.1145/586110.586117},DBLP,http: //dblp.uni-trier.de

[3] Leonard Kleinrock and John Silvester **,***Optimum Transmission radii for packet radio Networks or Why Six is a Magic Number (1978) ieee.*

[4] Christian Bettstetter**,** *On the Minimum Node Degree and Connectivity of a Wireless Multihop Network* (2002 ACM 1-58113-501-7/02/0006)

[5] Joengmin Hwang and Yongdae Kim**,**Revisiting *Random Key Pre-distribution Schemes for Wireless Sensor Networks* (2004 ACM 1-58113-972-1/04/0010)

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

[7] Eric Ke Wang, Lucas C.K.Hui and S.M.Yiu, *A New Key Establishment scheme for wireless sensor networks,(IJNSA)*, Vol 1, No 2, July 2009