International Institute of Information Technology Hyderabad

System and Network Security (CS5470)

Assignment 2: Simulation of the key management protocol in WSNs: Laurent Eschenauer, Virgil D. Gligor: A key-management scheme for distributed sensor networks. ACM Conference on Computer and Communications Security (ACM CCS'02), 2002: 41-47

Deadline: February 25, 2014 (Thursday)

Total Marks: 100

Note:- *It is strongly recommended that no student is allowed to copy programs from others. Hence, if there is any duplicate in the assignment, simply both the parties will be given zero marks without any compromise. Rest of assignments will not be evaluated further and assignment marks will not be considered towards final grading in the course. No assignment will be taken after deadline. Upload your only rollno_assign_2_.c file along with a README file in a zip file (rollno_assign_2.zip) to course portal (moodle).* ***You are restricted to use only C programming language for implementation. No other programming language implementation will be accepted.***

Let ρ, d and A denote the communication range of each sensor node, average neighborhood size of each sensor node and area of the deployment field (target field). Then, the the maximum network size n is given by

$$n = \frac{A \times (d+1)}{\pi \rho^2}.$$

For example, if $n = 10,000$, $A = 500 \times 500\ m^2$ and $\rho = 25\ m$, we have $d = 78$.

You can use the following data structure for representing a sensor node in wireless sensor networks (WSNs):

```
#include <stdio.h>
#include <stdlib.h>
#include <math.h>
#include <time.h>

char DAT_FILE[100]; /* locations of sensor nodes in the target
                       field to be stored in a data file */
int KEYRING_SIZE;  /* key ring size m for each sensor node */
int KEYPOOL_SIZE;     /* key pool size M */
```

```
int n;             /* total number of sensor nodes to be deployed */
int d;             /* average number of neighbor nodes for each sensor node */
double RANGE;      /* communication range of sensor node */
double p;  /* network connectivity during direct key establishment phase */
double pi; /* network connectivity during path key establishment phase
              using i hops in the path */

/* a sensor node representation */
typedef struct {
   int x; /* x-coordinate of sensor node location in target field */
   int y; /* y-coordinate of sensor node location in target field */
   int *keyring; /* key ring */
   int phynbrsize; /* number of physical neighbors of a sensor node */
   int keynbrsize; /* number of key neighbors of a sensor node */
   int *phynbr; /* list of physical neighbors of a sensor node */
   int *keynbr; /* list of key neighbors of a sensor node */
} sensor;
```

The data file contains the following information:

- The first line contains the total number n of sensor nodes in the target field.
- Remaining lines contain the locations of n sensor nodes in the target field.

In this assignment, you require to do the following three tasks:

- **Task 1:** For the sake of simplicity, consider the deployment field (target field) is either square field of size $L \times L$ m^2 or rectangle field of size $L_1 \times L_2$ m^2. Assume that $n = 10,000$ sensor nodes to be deployed in the sensor network (deployment field). Generate different $10,000$ locations (x_i, y_i) randomly for all sensor nodes SN_i, $i = 1, 2, \ldots, n$. Then, display the deployment of all sensor nodes in a graph (for example, you can use "gnuplot" software **[https://www.cs.princeton.edu/courses/archive/fall07/cos323/precepts/plotting/gnuplot.html]**). An example is given in Figure 1 for a sensor network of $10,000$ randomly deployed sensor nodes in a target field of size 500×500 m^2, where the points represent sensor nodes' locations.

  [20 Marks]

- **Task 2:** Simulate the network connectivity for the direct key establishment phase.

  [40 Marks]

- **Task 3:** Simulate the network connectivity for the path key establishment phase (using the number of hops $h = 1, 2$).

  [40 Marks]

A sample output for the simulating the network connectivity during the direct key establishment phase is given below:

```
$ ./a.out DATA-FILE KEYRING-SIZE KEYPOOL-SIZE
For example,
$ ./a.out sensor3.dat 100 40000

Reading data file...
```

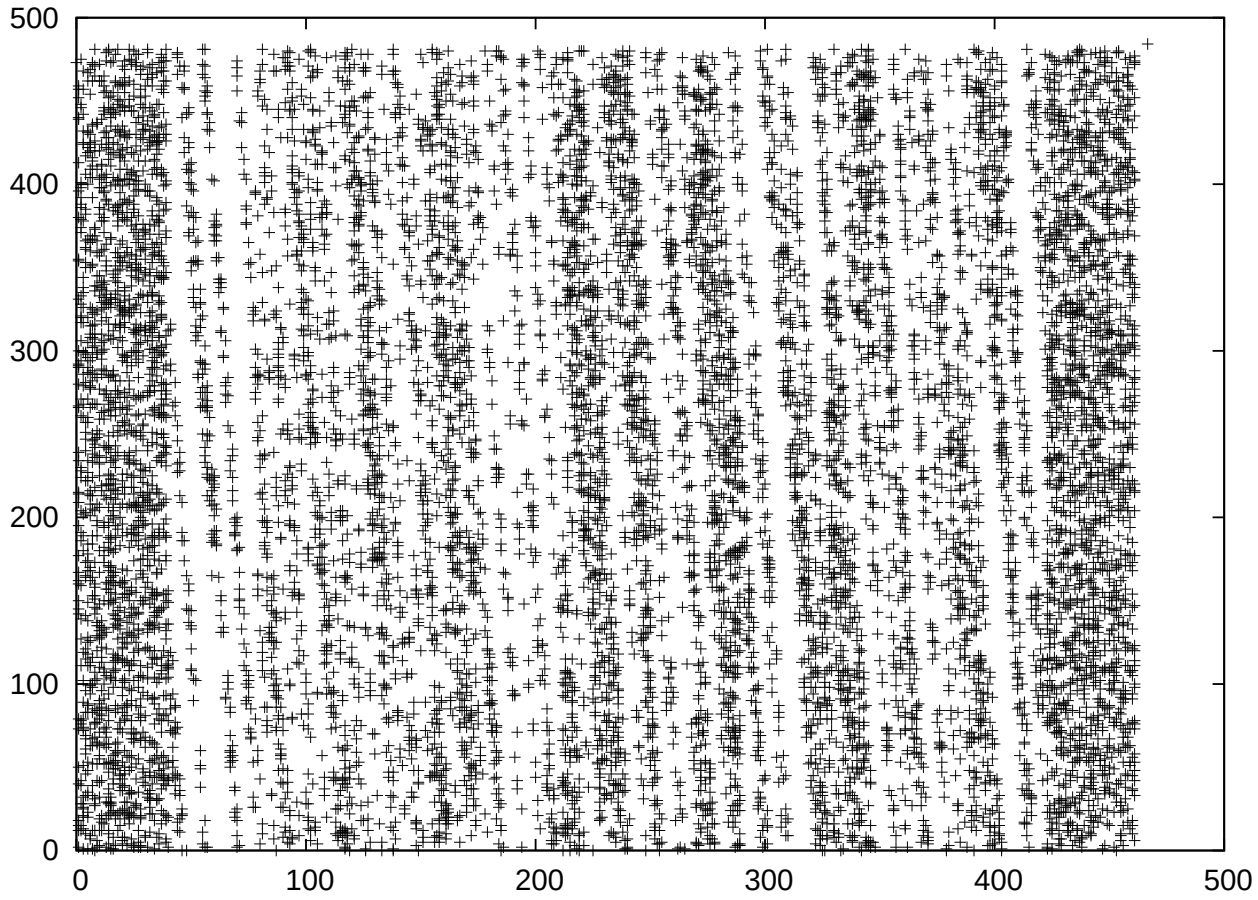

Figure 1: Target field having $10,000$ randomly deployed sensor nodes.

```
Scaling communication range...
Average distance = 258.24 m
Communication range of sensor nodes = 25.82 m

Computing physical neighbors...
Average neighborhood size = 98

EG scheme
Distributing keys...

Computing key neighborhood in direct key establishment phase...
Simulated average network connectivity =   0.2213
Theoretical connectivity     =   0.2217
```