Location-Aware Key Distribution in WSNs

Dr. Ashok Kumar Das

IEEE Senior Member
Associate Professor
Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad

E-mail: *ashok.das@iiit.ac.in*
URL: `http://www.iiit.ac.in/people/faculty/ashokkdas`
`https://sites.google.com/view/iitkgpakdas/`

Location-Aware Key Distribution in WSNs

The closest pairwise keys scheme (CPKS)

- The closest pairwise keys scheme (CPKS) proposed by Liu and Ning is a key pre-distribution scheme of location-awareness in nature.
- In the key pre-distribution phase, for each sensor node u to be deployed in the target field, the key setup server first determines a set S of m nodes whose expected locations of deployment are closest to that of u.
- For every node $v \in S$, for which a pairwise key between u and v has not already been assigned by the setup server, a new random symmetric key k_{uv} is generated.
- The key-plus-id combination (k_{uv}, v) is loaded to u's key ring, whereas the pair (k_{uv}, u) is loaded to v's key ring.

The closest pairwise keys scheme (CPKS)

- In direct key establishment phase, two neighboring nodes, say, u and v can establish a secure communication link, if they have a pre-distributed pairwise key.
- To identify a common key is trivial, because each pairwise key in a particular node is accompanied by the id of the other nodes holding the key.
- A cryptographic handshake may be then performed by the nodes u and v for mutual verification of the common key shared between them.

Network connectivity of CPKS

- Assume that the deployment field is two dimensional. Let u be a sensor node whose expected location be (u_x, u_y), whereas its actual location be (u'_x, u'_y). This corresponds to a deployment error $e = (u'_x - u_x, u'_y - u_y)$.
- Liu and Ning showed that the network connectivity of CPKS depends upon the deployment error e. If the maximum deployment error e is small, CPKS provides significantly better connectivity than the random schemes.
- They have also shown that for sufficiently large errors, CPKS essentially degrades to the random pairwise keys scheme (EG scheme) which has very poor connectivity when the network size is larger.

Network connectivity derivation

- For the sake of simplicity, we assume that the target field is two-dimensional, so that every point in that region is expressed by two co-ordinates x and y.
- Assume that u is a sensor node whose expected location is (u_x, u_y) whereas its actual location is (u'_x, u'_y). This corresponds to a deployment error of $e_u = (u'_x - u_x, u'_y - u_y)$.
- The actual location (or equivalently the error e_u) can be modeled as a continuous random variable that can assume values in R^2.
- The probability density function $f_u(u'_x, u'_y)$ of (u'_x, u'_y) characterizes the pattern of deployment error.
- Let (u'_x, u'_y) is uniformly distributed within a circle with center at (u_x, u_y) and radius e called the *maximum deployment error*. We have:

$$f_u(u'_x, u'_y) = \begin{cases} \frac{1}{\pi e^2} & \text{if } (u'_x - u_x)^2 + (u'_y - u_y)^2 \leq e^2 \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

Network connectivity derivation

- Another strategy is to model (u'_x, u'_y) as a random variable following the two-dimensional normal (Gaussian) distribution with mean (u_x, u_y) and variance σ^2. The corresponding probability density function is:

$$f_u(u'_x, u'_y) = \frac{1}{2\pi\sigma^2} e^{-[(u'_x-u_x)^2+(u'_y-u_y)^2]/(2\sigma^2)}. \quad (2)$$

- However, for the sake of simplicity, we only consider the uniform distribution given in Equation (1).
- Two nodes are called *physical neighbors* if they lie in each other's communication range. They are called *key neighbors* if they possess shares of a common key. They are called *direct neighbors* if they are both physical and key neighbors.
- Let u and v be two deployed nodes. Assume that each node has a communication range ρ and that the different nodes are deployed independently i.e., (u'_x, u'_y) and (v'_x, v'_y) are independent random variables.

Network connectivity derivation

- The probability that u and v are in each other's communication range can be calculated by

$$p(u,v) = \int\int\int\int_C f_u(u'_x, u'_y)\, f_v(v'_x, v'_y)\, du'_x\, du'_y\, dv'_x\, dv'_y \qquad (3)$$

  where C is the region $(u'_x - v'_x)^2 + (u'_y - v'_y)^2 \leq \rho^2$.
- Since u can share pairwise keys with c nodes, the expected value of ρ' is given by $\rho' = \rho \times \sqrt{\frac{c}{d+1}}$.
- Let v be a key neighbor of u. Then, the probability that v lies in the physical neighborhood of u is given by

$$p(u) = \frac{1}{\pi \rho'^2} \int\int_C p(u,v)\, dx\, dy \qquad (4)$$

Network connectivity derivation

- Again, since u is expected to have $c \times p(u)$ direct neighbors, the probability that u can establish a pairwise key with one of its physical neighbor is given by

$$p = \frac{p(u) \times c}{d} \approx p(u) \times \lambda \tag{5}$$

  where $\lambda = \frac{c}{d+1}$.
- We take the communication range ρ as the basic unit of distance measurement, i.e., $\rho = 1$. One can compute the probability p for the density function given above and establish that $p \approx 1$ for small deployment errors.

Resilience against node capture attack of CPKS

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDERABAD

- We note that each predistributed pairwise key $k_{u,v}$ between two neighbor nodes u and v is randomly generated.
- Thus, no matter how many nodes are captured, the pairwise keys between non-compromised sensor nodes remain still secure.
- This means that no matter how many sensor nodes are captured, the non-compromised nodes can communicate with each other with 100% secrecy.
- In this way, CPKS provides unconditional security against node capture attacks.