Key Management in Wireless Sensor Networks

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*
Homepage: http://www.iiit.ac.in/people/faculty/ashokkdas
Personal Homepage: https://sites.google.com/view/iitkgpakdas/

Part I

Key Management in Wireless Sensor Networks

Key Distribution in Wireless Sensor Networks

The bootstrapping protocol

- Establishes cryptographically secure communication links among the communicating sensor nodes.
- Must not only enable a newly deployed sensor node to initiate a secure infrastructure, but it must also allow nodes deployed at a later time to join the network securely.
- A challenging area of sensor networks due to resource limitations of sensor nodes as well as vulnerable to physical capture of nodes by an adversary in a sensor network.
- Public key routines (such as RSA, Diffie-Hellman, ElGamal) are not so much viable options. However, recent research demonstrates that ECC is viable.
- Symmetric key ciphers (such as DES, AES, RC5) are viable options

Key Distribution in Wireless Sensor Networks

Different phases of the bootstrapping protocol

- **Key pre-distribution phase:** Done in offline by the key setup server (usually, the base station).
- **Direct key establishment phase:** Performed by each sensor node after its deployment in the network.
- **Path key establishment phase:** Required if nodes do not establish direct keys during the direct key establishment phase.

Requirements of the bootstrapping protocol

- *R1:* Deployed sensor nodes must be able to establish secure node-to-node communication.
- *R2:* Illegal sensor nodes should not be able to gain entry/access into the network, either through packet injection or masquerading as a legitimate sensor node.
- *R3:* One can always add new sensor nodes dynamically at any time after the initial deployment and these additional deployed nodes can form secure connections with the already deployed nodes in the sensor network. Thus, the bootstrapping information must always be present and can not be simply erased after deployment to prevent compromise in the event of capture.

Key Distribution in Wireless Sensor Networks

Evaluation metrics of the bootstrapping protocol

- ***Scalability:*** It should support a large-scale sensor network.
- ***Storage overhead:*** The amount of memory required to store security credentials must be minimum.
- ***Communication overhead:*** The number of messages exchanged during a key establishment procedure must be less.
- ***Computational overhead:*** The amount of processor cycles required to establish a secret key between two communicating sensor nodes should be minimum due to resource limitations of sensor nodes.
- ***Network connectivity:*** This is the probability that two sensor nodes can establish a secret key.

Key Distribution in Wireless Sensor Networks

Evaluation metrics of the bootstrapping protocol (Continued...)

- ***Resilience against node capture:*** For any two non-compromised sensor nodes u and v, we have to find out what is the probability that the adversary can decrypt the secret communications between u and v when c sensor nodes are already compromised ?
  Let $P_e(c)$ denote the fraction of total secure communications compromised after capturing c sensor nodes by an attacker in a sensor network.
  If $P_e(c) = 0$, we call a key establishment scheme as *unconditionally secure against node capture* or *perfectly resilience against node capture*.

Key distribution using a single network-wide key

Protocol

- The simplest solution is the use of a single network-wide master key for the entire network.
- Each node is given the same mission key before deployment in the network by the key setup server.
- After deployment, any two neighbor nodes can communicate securely with each other using this key.

Key distribution using a single network-wide Key

Properties

- Only a single network-wide cryptographic key is needed to be stored in each sensor node's memory.
- Works well without needing to perform the direct key establishment phase.
- Provides 100% network connectivity.
- NO computational overhead.
- NO communication overhead.
- Scalable.

Key distribution using a single network-wide Key

Drawbacks

- The compromise of even a single node in a network would reveal the secret key and thus allow decryption of all network traffic.
- Another solution is to use a single shared network-wide key to establish session keys between any two neighbor nodes, and then erase the network-wide key.
- The main difficulty of this variant of the key establishment procedure is that it does not allow addition of new nodes after initial deployment.

Random key distribution

(L. Eschenauer and V. D. Gligor, “A key management scheme for distributed sensor networks”, in *9th ACM CCS*, pp. 41-47, Nov. 2002.)

Key pre-distribution phase

- Done in offline by the key setup server (base station).
- Each node u is assigned a unique node identifier id_u.

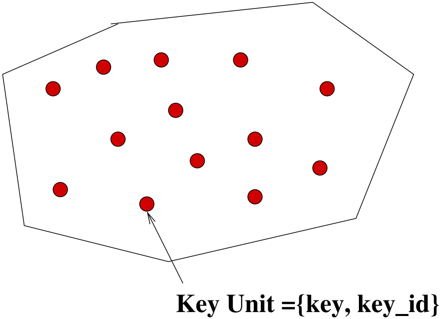


Figure: Key pool $\mathcal{M}$ of size M.

Random key distribution

Key pre-distribution phase (Continued...)

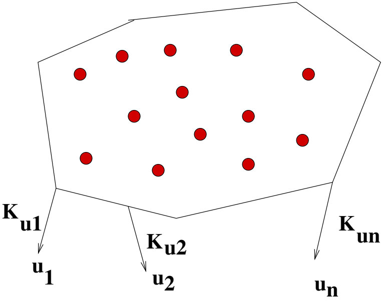


Figure: Key ring K_{u_i} selection of a sensor node u_i.

- For each node u_i, a small subset K_{u_i} of size m is selected randomly without replacement from the key pool $\mathcal{K}$.
- Each node u_i is pre-loaded with (i) id_{u_i}, and (ii) K_{u_i}.

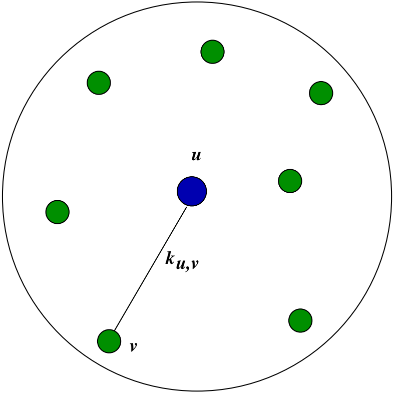
Random key distribution

Direct key establishment phase

- Executed by each sensor node after deployment in the network.
- Each node broadcasts a HELLO message (containing its own identifier).
  $u \rightarrow * : HELLO$
- Each node prepares a list of physical neighbors in its communication range.
  $NL_u = \{v_1, v_2, \ldots, v_d\}$ is the list of d neighbors of a node u.
- Key neighbors
- Direct neighbors

Random key distribution

Direct key establishment phase (Continued...)



- $u \rightarrow v : id_u || \{$ list of key ids $\}$
- $v \rightarrow u : id_v || \{$ list of key ids $\}$

Random key distribution

Direct key establishment phase (Continued...)

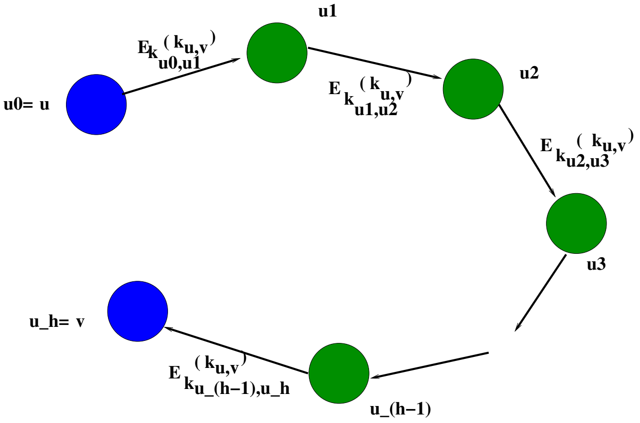
Another procedure of key discovery which is more secure, but slower, could utilize client puzzles such as a Merkle puzzle (R. Merkle, “Secure communication over insecure channels”, *Communications of the ACM*, 21(4):294-299, 1978).

- Assume u and v be two neighbor nodes.
- u generates m client puzzles, say, $P_1, \ldots, P_m$, one for each of the m keys in its key ring.
- $u \rightarrow v : \{E_{k_i}(P_i), MAC_{k_i}(P_i)\}$, $i = 1, 2, \ldots, m$.
- v decrypts an encrypted puzzle, say, $E_{k_i}(P_i)$ with one of the keys residing in its key ring and computes the corresponding MAC. If the computed MAC and the received MAC are equal, then u and v use this key for future communication.
- Though this method is secure one, but it introduces a lot of communication and computational overheads to establish pairwise keys among neighbor nodes.

Random key distribution

Path key establishment phase

- Executed after direct key establishment phase by a sensor node in the network, if required.



Random key distribution

Dynamic node addition phase

- Assume a node u needs to be deployed in the existing sensor network.
- The key setup server assigns a unique identifier id_u and selects a key ring K_u of size m from the key pool $\mathcal{K}$. These information are loaded in its memory before deployment.
- After deployment, u establishes keys with its neighbor nodes.
- Path key establishment could be executed by the node u, if necessary.

Random key distribution

Analysis

- **Storage overhead:** m keys.
- **Communication overhead:** list of m key ids (clear-text broadcasting) or list of m challenge messages (private shared-key discovery).
- **Computational overhead:** $\frac{2m+p_{EG}-p_{EG}\cdot m}{2}$ $\log m$ comparisons, where p_{EG} is the probability that two neighbor nodes can establish a secret key during the direct key establishment phase (network connectivity probability)[clear text broadcasting]. Required additional cost due to $2m$ encryptions and decryptions and $2m$ MACs for MAC verifying the puzzles [private shared-key discovery].

Random key distribution

Analysis (Continued...)

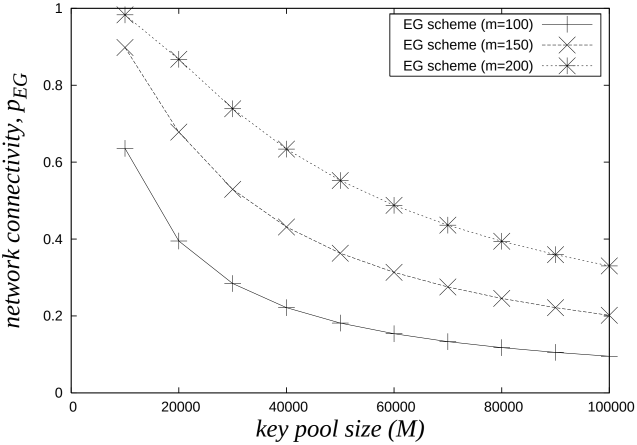
- **Network connectivity for direct key establishment phase:** The probability of establishing a direct pairwise key between two sensor nodes u and v is

$$\begin{aligned} p_{EG} &= 1 - \frac{\binom{M-m}{m}}{\binom{M}{m}} \\ &= 1 - \prod_{i=0}^{m-1} \frac{M-m-i}{M-i}, \end{aligned} \qquad (1)$$

where M is the key pool size and m the key ring size of a sensor node.

Random key distribution

Network connectivity of the EG scheme for different combinations of *M* and *m*.



Random key distribution

Network connectivity for path key establishment phase:

- Let d be the average number of neighbor nodes that each sensor node can contact.
- The probability of two sensor nodes establishing a pairwise key (directly or indirectly) is

$$p_1 = 1 - (1 - p)(1 - p^2)^d. \tag{2}$$

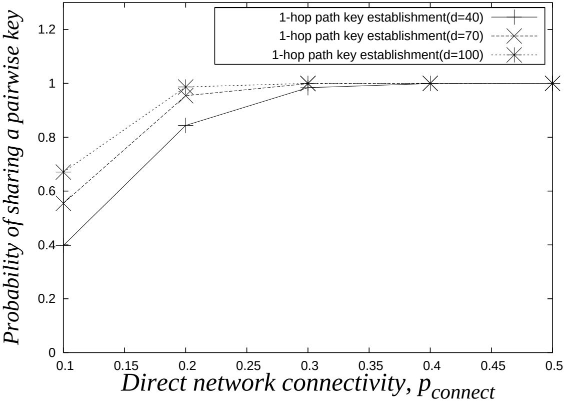
- If p_h is the probability that two neighbor sensor nodes can establish a key using a h-hop path key establishment phase, it is easy to deduce that

$$p_h = 1 - (1 - p_{h-1})(1 - p.p_{h-1})^d \text{ for all } h \geq 1, \tag{3}$$

where $p_0 = p$.

Random key distribution

The probability p_1 of establishing a pairwise key v.s. the probability p that two sensor nodes establish a direct pairwise key, with $d = 40, 70, 100$.



Random key distribution

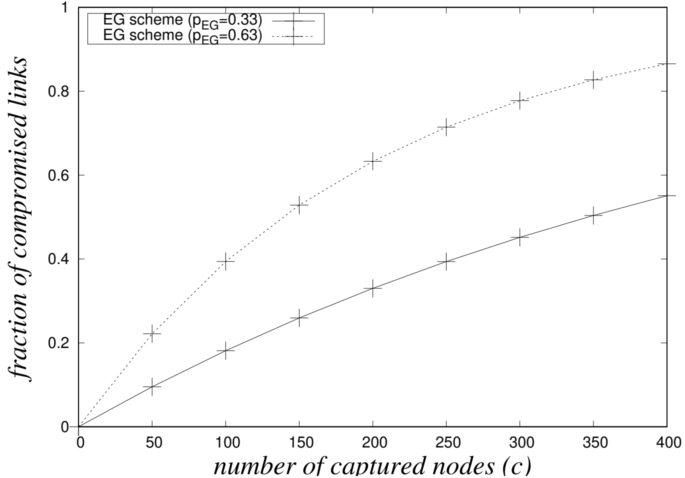
Resilience against node capture attacks during direct key establishment phase

- Node capture model: Random / Selective.
- For any two non-compromised sensor nodes *u* and *v*, we have to find out what is the probability that the adversary can decrypt the secret communications between *u* and *v* when *c* sensor nodes are already compromised ?
- When *c* nodes are already captured, the resilience against node capture is given by

$$P_e(c) = 1 - \left(1 - \frac{m}{M}\right)^c. \tag{4}$$

Random key distribution

Resilience against node capture attacks during direct key establishment phase (Continued...)



Random key distribution

Resilience against node capture attacks during path key establishment phase

- Consider a secure h-hop path $\langle u = u_0, u_1, u_2, \ldots, u_{h-1}, u_h = v \rangle$ between two neighbor nodes u and v through which u and v can establish a pairwise direct secret key between them.
- The secure link (u, v) is compromised by an attacker if either of its end points u and v are compromised, or any one of the intermediate nodes $u_1, u_2, \ldots, u_{h-1}$ is compromised.
- If a fraction f of sensor nodes are captured by an attacker in the network during the path key establishment phase, the probability that the secure link (u, v) is compromised is $1-$ (probability that the link (u, v) is not compromised) = $1 - (1 - f)^{h+1}$.
- p and p_h be the probabilities that two neighbors can establish a secure link during the direct key establishment phase and h-hop path key establishment phase, respectively.

Random key distribution

Resilience against node capture attacks during path key establishment phase (Continued...)

- Let there be n sensor nodes deployed in the network and each node have in average d physical neighbors in its communication range.
- The total number of secure links in the network is $\frac{nd}{2} \times p + \frac{nd}{2} \times (1-p) \times p_h$.
- The resilience against node capture during the h-hop path key establishment phase due to capture of a fraction $f (= \frac{c}{n})$ of sensor nodes in the network can be estimated as

$$\begin{aligned} P_e(c)_{pathkey} &= \frac{\frac{nd}{2} \times P_e(c) + \frac{nd}{2} \times (1-p) \times p_h \times (1-(1-f)^{h+1})}{\frac{nd}{2} \times p + \frac{nd}{2} \times (1-p) \times p_h} \\ &= \frac{P_e(c)}{p + (1-p) \times p_h} + (1 - \frac{p}{p+(1-p) \times p_h}) \\ &\quad \times (1-(1-f)^{h+1}). \end{aligned} \tag{5}$$

Random key distribution

Important observations

- Network connectivity p depends on size M of key pool with a fixed key ring size m. Smaller M leads to higher network connectivity.
- Resilience against node capture $P_e(c)$ depends on key pool size M and number of captured nodes c. Smaller key pool size leads to have low resilience against node capture. Further, as c increases, resilience also decreases.
- Needs to make a better trade-off between network connectivity and resilience against node capture.

Random key distribution

Important References

- L. Eschenauer and V. D. Gligor. A Key Management Scheme for Distributed Sensor Net- works. In 9th ACM Conference on Computer and Communication Security, pages 41-47, November 2002.
- H. Chan, A. Perrig, and D. Song. Random Key Predistribution Schemes for Sensor Networks. In IEEE Symposium on Security and Privacy, pages 197-213, Berkeley, California, 2003.
- W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney. A key management scheme for wireless sensor networks using deployment knowledge. In 23rd Conference of the IEEE Communications Society (Infocom'04), volume 1, pages 586-597, Hong Kong, China, March 21-25 2004.
- W. Du, J. Deng, Y. S. Han, and P. K. Varshney. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In ACM Conference on Computer and Communications Security (CCS'03), pages 42-51, Washington DC, USA, October 27-31 2003.

Random key distribution

Important References

- D. Liu and P. Ning. "Establishing Pairwise Keys in Distributed Sensor Networks," in Proceedings of 10th ACM Conference on Computer and Communications Security (CCS), pages 52-61, Washington DC, Oct 27-31 2003.
- Ashok Kumar Das. "A random key establishment scheme for multi-phase deployment in large-scale distributed sensor networks," in International Journal of Information Security (Springer), Vol. 11, No. 3, pp. 189-211, 2012, doi: 10.1007/ s10207-012 -0162-9.
- Ashok Kumar Das. "Improving Identity-Based Random Key Establishment Scheme for Large-Scale Hierarchical Wireless Sensor Networks," in International Journal of Network Security, Vol. 14, No. 1, pp. 1 - 21, 2012.

Important References

- Ashok Kumar Das. “An Efficient Random Key Distribution Scheme for Large-Scale Distributed Sensor Networks,” in Security and Communication Networks (Wiley), Vol. 4, No. 2, pp. 162 - 180, 2011.
- Ashok Kumar Das. “A Survey on Analytic Studies of Key Distribution Mechanisms in Wireless Sensor Networks,” in Journal of Information Assurance and Security, Vol. 5, No. 5, pp. 526-553, 2010, Dynamic Publishers Inc., USA.
- Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A survey of key management schemes in wireless sensor networks,” *Computer Communications*, vol. 30, no. 11-12, pp. 2314-2341, 2007.
- Y. Wang, G. Attebuty, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, *IEEE Communications Surveys & Tutorials*, vol. 8, no. 2, pp. 2-23, 2006.

Thank you