The Impact of Incomplete Secure Connectivity on the Lifetime of Wireless Sensor Networks

Huseyin Ugur Yildiz, Bekir Sait Ciftler, Bulent Tavli, Kemal Bicakci, and Davut Incebacak

***Abstract*—Key pre-distribution schemes accommodate secure connectivity by establishing pairwise keys between nodes. However, ensuring security for all communication links of a wireless sensor network is non-trivial due to the memory limitations of the nodes. If some of the links are not available due to the lack of a primary security association between the transmitter and the receiver, nodes can still send their data to the base station but probably not via the best route which maximizes the network lifetime. In this study, we propose a linear programming framework to explore the incomplete secure connectivity problem with respect to its impact on network lifetime, path length, queue size, and energy dissipation. The numerical results show that if any two nodes share a key with a probability of at least 0.3, then we should expect only a marginal drop (*i.e.*, less than 3.0%) in lifetime as compared to a fully-connected network.**

***Index Terms*—wireless sensor networks, linear programming, energy efficiency, network lifetime, key distribution.**

I. Introduction

Cryptographic key management - a fundamental part of any cryptosystem - is a costly and complex process [1]. Pre-configuring the devices with cryptographic keying material is a prerequisite for securing the communication links if indirect key establishment is not available or otherwise undesirable. If there is a pairwise secret key or public key of the communication partner is known a priori for two parties, then a primary security association between them could be established [2].

For a wireless sensor network (WSN) composed of hundreds or even thousands of nodes, it is not a viable approach to apply the aforementioned pre-configuration for all communication links due to limited memory available on sensor nodes. As a result, usually, only a subset of node pairs could establish a secure link for communication using primary security associations. This incomplete secure connectivity problem has been investigated by considering various aspects of the system design in earlier work. For instance, the associated cost in terms of throughput was rigorously analyzed [2]. There are a vast volume of published studies (*e.g.*, [3]–[5]) that have attempted to examine connectivity issues and suggest several types of pairwise key distribution. On the other hand, a topic largely untouched in the literature is the cost with respect to network lifetime. There is definitely an energy cost if a node cannot send its data via the optimal route to the base station due to an insecure link on that route, but the exact cost is yet to be determined.

We consider a WSN where sensor nodes communicate only if they share a pairwise key used for symmetric key encryption. Network lifetime is a crucial performance metric in WSNs and hence it is the focus of our work while studying the problem of not having a fully connected secure network. To obtain accurate energy expenditure figures in WSNs, we use log normal shadowing propagation model since realistic assumptions on radio propagation models have dramatic effects on system lifetime when compared to the results obtained under ideal conditions [6].

This paper seeks to remedy the following research problem: What is the minimum requirement for the primary security association probability (which is assumed to be same for all links in the WSN) for a corresponding lifetime sacrifice? In our work, we present a novel linear programming (LP) framework which quantifies network lifetime values when the aforementioned probability changes between zero and one. Furthermore, we investigate the effects of key sharing probability on queue size, path length, and energy dissipation when minimum cost routing is utilized.

II. The System Model

A. Key Sharing Probability and Secure Connectivity

The probability that a node shares a primary security association with another node is a good abstraction for many key management schemes. As an example, consider the Eschenauer and Gligor's seminal work on Key Pool Scheme [3]. In this scheme, an offline trust authority provides a large key pool of size P where each node is randomly given k different keys from this key pool before deploying the WSN. Key pools usually consist of $2^{17} - 2^{20}$ keys. The probability of key sharing (KSP) between two nodes (*i.e.*, at least one shared key between two nodes) is given as in Equation 1.

$$P_{sharing} = 1 - \frac{k!(P-k)!(P-k)!}{P!k!(P-2k)!}. \quad (1)$$

In fact, this value gives us the primary security association probability. If there is at least one shared key between two nodes, then a direct connection could be established for conveying the sensed data to the base station. For example, to obtain $P_{sharing} = 0.5$ with $P = 2^{20}$ the key ring size should be at least $k = 853$. When AES-128 is used as the encryption algorithm, 16B of memory is required for every cryptographic key. Therefore, the corresponding storage

H. U. Yildiz, B. Tavli, and K. Bicakci are with TOBB University of Economics and Technology, 06520, Ankara, Turkey (e-mail: {huyildiz, btavli, bicakci}@etu.edu.tr).

B. S. Ciftler is with the Department of Electrical and Computer Engineering at Florida International University, Miami, FL, 33174 (e-mail: bcift001@fiu.edu)

D. Incebacak is with Kocaeli University, Kocaeli, Turkey, E-mail: davut.incebacak@kocaeli.edu.tr.

requirement is computed approximately as 14 KB. In a typical WSN platform (*e.g.*, Mica2 motes) 512 KB of storage is not uncommon, hence, allocating less than %3 of storage space for security purposes is feasible in most circumstances. We assume the same $P_{sharing}$ value applies for all the links.

B. Radio Propagation Model

We use the discrete HCB-LNS (Heinzelman-Chandrakasan-Balakrishnan – Log-Normal-Shadowing) energy model [7] which is a revised version of an energy model proposed by Heinzelman *et. al.* [8]. In discrete HCB-LNS model, energy dissipation for transmitting M_P Bytes of data from node-*i* to node-*j* is denoted as

$$E_{tx,ij} = 8 \times M_P \left(\rho + \eta \left\lceil \frac{\varepsilon T_b P_{t,ij}}{\eta} \right\rceil \right), \tag{2}$$

where ρ (50 nJ) denotes the energy dissipation on electronic circuitry, ε (4 μJ) shows the transmitter efficiency. T_b is the duration of a bit (26.04 μs) corresponding to the network bandwidth of $\kappa = 1/T_b = 38.4$ Kbps. The minimum energy quantum value (η – transmitter's discrete energy levels are multiples of η) is taken as $10 \times \rho$ [7]. Energy dissipation for receiving M_P Bytes of data can be expressed as $E_{rx} = 8 \times M_P \times \rho$.

The probabilistic nature of radio propagation is incorporated into our model as follows. First, we obtain the path loss values ($\overline{\Upsilon_{ij}}$) (overbar is used to indicate that the quantity is in dB) between all node pairs in network as in Equation 3.

$$\overline{\Upsilon_{ij}} = \overline{\Upsilon_0} + 10nlog_{10}(d_{ij}/d_0) + \overline{X_\sigma}, \tag{3}$$

The distance between transmitter and receiver is denoted by d_{ij} where $d_0 = 1$ m is a reference distance. $\overline{\Upsilon_0} = 55$ dB is the path loss at the reference distance, $n = 4$ is the path loss exponent, and $\overline{X_\sigma}$ is a zero-mean Gaussian random variable with standard deviation of $\sigma = 4$ [9].

Then, we calculate SNR values (ψ_{ij}) for a given target PRR (Packet Reception Rate) value (χ_{ij}) [9] as

$$\chi_{ij} = \left(1 - \frac{1}{2} \exp(\frac{-\psi_{ij}}{2} \frac{1}{0.64}) \right)^{8 \times M_P}. \tag{4}$$

Note that PRR represents the probability of a successful packet reception at a distance d_{ij}.

Finally, we calculate the antenna output power, $\overline{P_{t,ij}}$ using 5, which is used to calculate $E_{tx,ij}$ with Equation 2 as

$$\overline{\psi_{ij}} = \overline{P_{t,ij}} - \overline{\Upsilon_{ij}} - \overline{P_n}, \tag{5}$$

where $\overline{P_n}$ is the noise floor which is -145 dB at the temperature of 300 Kelvin for Mica motes [9]. Note that $E_{tx,ij}$ is the total energy dissipated at the transmitter, while $T_b P_{t,ij}$ is the energy radiated from the antenna only [7]. We use the targeted PRR value on the link from node-i to node-j as $\chi_{ij} = 0.94$ and have the same target PRR throughout the network.

To compensate for packet losses, retransmissions are required. The energy cost of transmitting and receiving data packets on a failed transmission attempt (*i.e.*, a packet should be received completely to determine whether the packet is corrupted or not) over link (i, j) should be scaled by λ_{ij} to account for retransmissions [9]. The relation between χ_{ij} and λ_{ij} can be expressed as $\lambda_{ij} = \frac{1}{\chi_{ij}}$.

C. LP Model for Lifetime Maximization

The network topology is represented as a directed graph $G = (V, A)$ where we define V as the set of all nodes including the base station (node-1). We also define set W which includes all nodes except the base station $W = V \setminus \{1\}$. $A = \{(i, j) : i \in W,\ j \in V - i\}$ is the set of arcs. Traffic generated at each node terminates at the base station either by direct transfer or through other sensors acting as relay nodes.

We adopt the network lifetime definition given in [10] and used widely in earlier work which is the time when the first sensor node exhausts all its battery energy. However, this definition should not be misinterpreted – when we examine the LP framework carefully it can be seen that to maximize the minimum lifetime, all nodes are forced to dissipate their energies in a balanced fashion, hence, sensor nodes in the network deplete their battery energies simultaneously. Note that WSN lifetime also depends on the traffic patterns between the nodes (*i.e.*, when some of the critical nodes are out of power, the entire network may be disconnected). Hence, the network lifetime definition we adopted is also useful in capturing such behavior (*i.e.*, the whole network determines the lifetime not a subset of the nodes).

We presume that time is organized into rounds of duration 100 s ($T_{rnd} = 100$ s). At each round every node dissipates a certain amount of energy for data acquisition ($E_{DA} = 600$ μJ) and generates $M_D = 230$ Bytes of processed data. Packet processing energy is also considered ($E_{PROC} = 120$ μJ). Each data packet has $M_H = 25$ Bytes of overhead, thus, the data packet length is $M_P = M_H + M_D = 255$ Bytes.

The amount of data packets that flows from node-i to node-j is represented by f_{ij}. Each sensor node-*i* creates the same amount of traffic ($s_i = M_P$ Bytes) at each round to be conveyed to the base station (*i.e.*, Constant Bit Rate traffic).

The LP model, formulated with the objective of maximizing t (the minimum lifetime of sensor nodes), is given in Figure 1. Equation 6 states that all flows are non-negative. Equation 7 is the flow balancing constraint which states that for all nodes except the base station, the difference between the amount of data flowing out of node-i and the amount of data flowing into node-i is equal to the amount of total data generated by node-i. Furthermore, all generated data by the sensor nodes terminate at the base station (*i.e.*, node-1). Equation 8 is the energy constraint. Total energy dissipation in a sensor node is comprised of reception energy, transmission energy, extra energy dissipation due to the retransmissions caused by packet losses, and data acquisition (E_{DA}) with processing energy (E_{PROC}) throughout the network lifetime. This equation states that no sensor node can spend more than its initial battery energy (e_i). Equation 9 states that each sensor node is assigned equal initial energy ($\xi = 25$ KJ) at the beginning of the network operation.

Equation 10 is used to ensure that the data can flow from node-i to node-j with a probability of $P_{sharing}$. The value of γ_{ij} is taken from a uniformly distributed random variable ($\gamma_{ij} \sim U(0, 1)$). We assume that $\gamma_{ij} = \gamma_{ji}$ (*i.e.*, the link between any node pair is symmetric). Equation 11 is used to guarantee that the bandwidth utilization of node-i is bounded

Maximize t
subject to:

$$f_{ij} \geq 0 \ \forall (i,j) \in A \tag{6}$$

$$\sum_{j \in V} f_{ij} - \sum_{j \in W} f_{ji} = \begin{cases} s_i t & \forall i \in W \\ -\sum_{j \in W} s_j t & i = 1 \end{cases} \tag{7}$$

$$\sum_{j \in V} E_{tx,ij} \lambda_{ij} f_{ij} + E_{rx} \sum_{j \in W} \lambda_{ji} f_{ji} + t(E_{DA} + E_{PROC}) \leq e_i \ \forall i \in W \tag{8}$$

$$e_i = \xi \ \forall i \in W \tag{9}$$

$$f_{ij} = \begin{cases} f_{ij} & \text{if } \gamma_{ij} \leq P_{sharing} \\ 0 & \text{o.w.} \end{cases} \quad \forall (i,j) \in A. \tag{10}$$

$$\sum_{j \in V} \lambda_{ij} f_{ij} + \sum_{j \in W} \lambda_{ji} f_{ji} + \sum_{k \in W} \sum_{l \in V} \lambda_{kl} f_{kl} I^i_{kl} \leq \kappa \times t \ \forall i \in W \tag{11}$$

$$I^i_{jk} = \begin{cases} 1 \text{ if } \zeta d_{jk} \geq d_{ji} \text{ and } i \neq j \neq k \\ 0 \text{ else} \end{cases} \tag{12}$$

Fig. 1: LP model for Lifetime Maximization

by the available channel bandwidth. Interference function (I^i_{jk}) is defined in Equation 12 which states that the flow from node-*j* to node-*k* interferes with node-*i* if the distance between node-*j* and node-*k* times ζ is greater than or equal to the distance between node-*j* and node-*i*. ζ represents the interference factor ($\zeta = 1.7$) [11].

D. LP Model for Energy Minimization

Although maximizing lifetime is the ultimate objective in WSNs, analyzing average path length, average queue size, and average energy dissipation are also important. Therefore, we modify the LP model presented in subsection by changing the objective function from lifetime maximization to energy minimization. Hence, we analyze the network for a predetermined amount of time (*i.e.*, $t = 1000$ rounds). The objective function is the minimization the total energy dissipation in the network (E_{TOT}) which is

$$\sum_{(i,j) \in A} E_{tx,ij} \lambda_{ij} f_{ij} + E_{rx} \sum_{(i,j) \in A} \lambda_{ji} f_{ji} + t(E_{DA} + E_{PROC}) \tag{13}$$

The constraints of this model are the Equations 6, 7, 10, 11, and 12. Variables of the model are the flows (*i.e.*, f_{ij}). Since the duration is constant (*i.e.*, 1000 rounds), only transmit and receive energy terms can be minimized, therefore, this LP model minimizes the path costs and we choose energy dissipation as our cost function. Performance evaluation metrics for this model are *average queue size per node per round*, *average path length per node per packet*, and *average energy dissipation per node per round* which are obtained by using $\frac{\sum_{(i,j) \in A} f_{ij}}{t \times |W|}$, $\frac{\sum_{(i,j) \in A} f_{ij} \times d_{ij}}{\sum_{(i,j) \in A} f_{ij}}$, and $\frac{E_{TOT}}{t \times |W|}$, respectively.

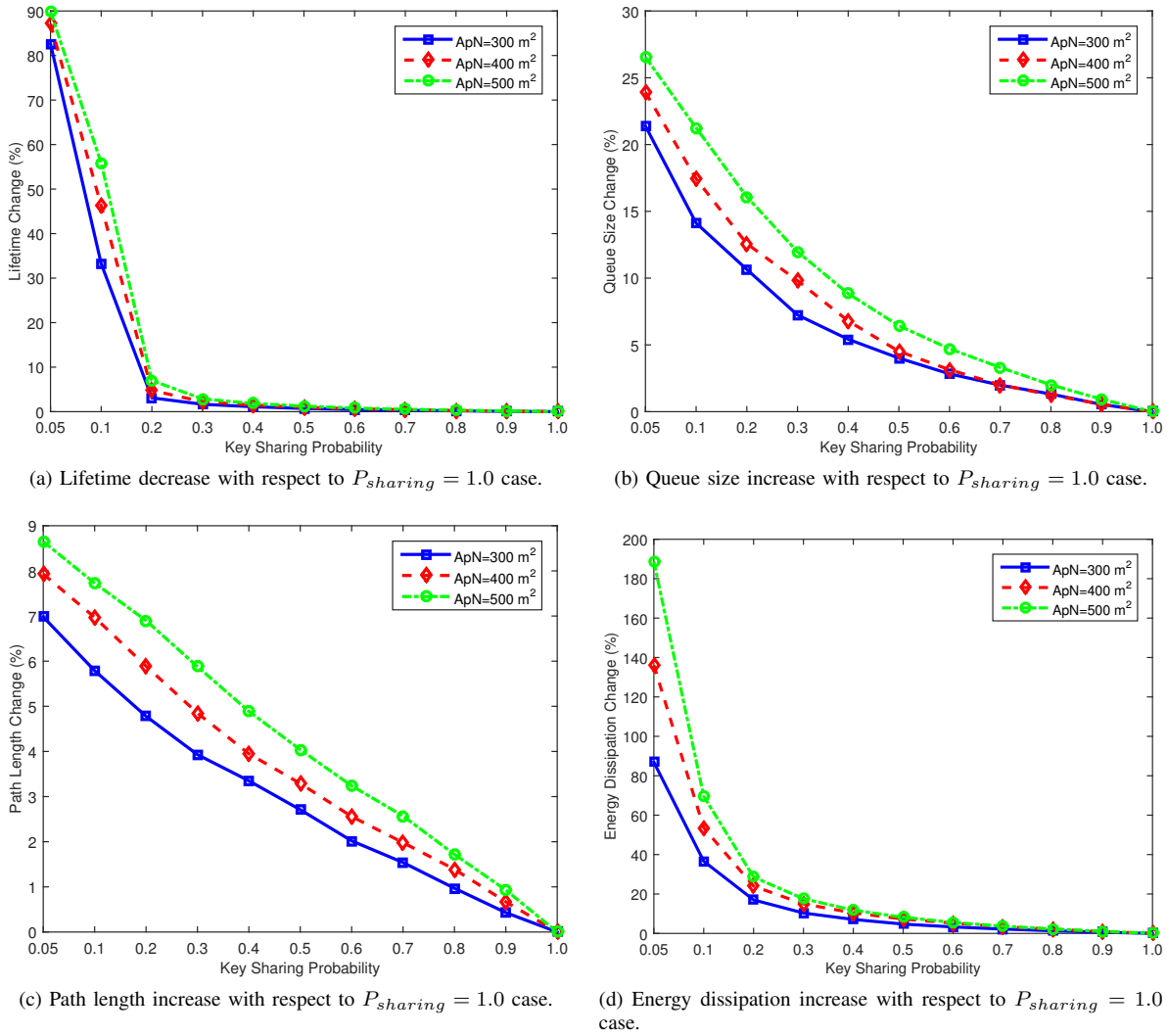
III. Analysis

We use MATLAB to construct the network topology and General Algebraic Modeling System (GAMS) with XPRESS solver for the numerical analysis of the developed LP models. The network topology is a disc shaped area with a base station located at the center. Sensor nodes are uniformly distributed by using the best known disk packing geometries [12]. The results are averaged over 100 randomly generated KSP distributions.

The results of our analysis are presented in Figure 2 as functions of KSP with 300 nodes (*i.e.*, $|W| = 300$). We used three network densities at each subgraph. Network density metric we utilized is ApN (Area per node) which is obtained by dividing the total network area to the number of nodes (*i.e.*, a higher ApN means a sparser network). We utilized only the topologies where no disjoint subsets are created by the flow restrictions.

Figure 2a is obtained by solving the LP model given in Section II-C where the objective is to maximize t (network lifetime). The maximum lifetime is achieved when there is no flow restriction due to KSP (*i.e.*, $P_{sharing} = 1$). Therefore, lifetimes obtained for all $P_{sharing} < 1$ are lower than or equal to the lifetime obtained with $P_{sharing} = 1$ case. For example, lifetime values obtained with $P_{sharing} = 0.1$ for $ApN = 300\ m^2$, $ApN = 400\ m^2$, and $ApN = 500\ m^2$ are %33.2, %46.2, and %55.9 lower than the corresponding lifetime values with $P_{sharing} = 1.0$, respectively. As the key sharing probability increase drop in network lifetime also decreases. This is because there are more route alternatives in a network with a larger number of links (*i.e.*, the number of usable links increases as the key sharing probability increases) and among these alternatives it is more likely to have a route which is close to the optimal route in terms of energy dissipation characteristics. An interesting result is the sharpness of this decrease (*i.e.*, to achieve maximal network lifetime it is not necessary to secure all physically viable links). For example, the decrease in network lifetimes with $P_{sharing} = 0.5$ are %0.7, %1.0, and %1.2 for $ApN = 300\ m^2$, $ApN = 400\ m^2$, and $ApN = 500\ m^2$, respectively. The effects of key sharing probability decrease is more severe in sparser networks. This is because there are more energy efficient route alternatives in a denser network and among these alternatives it is more likely to have a route which is closer to the optimal route in terms of energy dissipation characteristics.

In Figure 2b, Figure 2c, and Figure 2d, we present percentage difference of queue size, path length, and energy dissipation with respect to the $P_{sharing} = 1$ case, respectively, as functions of KSP. These results are obtained by solving the LP model presented in subsection II-D. The lower values of all these metrics are desired for better network performance. Indeed, the lowest values for all these metrics are obtained with $P_{sharing} = 1$. For example, average queue size per node per round, average path length per node per packet, and average energy dissipation per node per round with $P_{sharing} = 0.2$ and $ApN = 400\ m^2$ are %12.6, %5.9, and %24.0 higher than the $P_{sharing} = 1.0$ case, respectively. For lower KSP values path lengths are longer, energy efficiency of the paths are lower, and higher number of packets must be relayed due to the elongated paths with higher number of hops.



(a) Lifetime decrease with respect to $P_{sharing} = 1.0$ case.

(b) Queue size increase with respect to $P_{sharing} = 1.0$ case.

(c) Path length increase with respect to $P_{sharing} = 1.0$ case.

(d) Energy dissipation increase with respect to $P_{sharing} = 1.0$ case.

Fig. 2: Percentage change with respect to $P_{sharing} = 1.0$ case in a 300-node topology.

IV. Conclusion

This paper investigates the impact of incomplete connectivity on the WSN lifetime by introducing an LP framework. The results of our numerical analysis show that having a low (below 0.1) primary security association probability has a major impact on network lifetime, however, the drop in network lifetime sharply curves down as this probability increases. In all of the topologies we examine, the lifetime drop converges to insignificant levels if only half of the links in the network is secured.

References

[1] P. Argyroudis, R. Verma, H. Tewari, and D. O'Mahony, "Performance analysis of cryptographic protocols on handheld devices," in *Proc. IEEE International Symposium on Network Computing and Applications (NCA)*, 2004, pp. 169–174.

[2] O. Koyluoglu, C. Koksal, and H. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Transactions on Information Theory*, vol. 58, pp. 3000–3015, 2012.

[3] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. ACM Conference on Computer and Communications Security (CCS)*, 2002, pp. 41–47.

[4] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. IEEE Symposium on Security and Privacy (SP)*, 2003, pp. 197–213.

[5] W. Du, J. Deng, Y. Han, S. Chen, and P. Varshney, "A key management scheme for wireless sensor networks using deployment knowledge," in *Proc. IEEE International Conference on Computer Communications (INFOCOM)*, 2004, pp. 586–597.

[6] N. Aslam, W. Robertson, and W. Phillips, "Clustering with discrete power control in wireless sensor networks," in *Proc. International Conference on Sensor Technologies and Applications (SENSORCOMM)*, 2009, pp. 43–48.

[7] H. Cotuk, K. Bicakci, B. Tavli, and E. Uzun, "The impact of transmission power control strategies on lifetime of wireless sensor networks," *IEEE Transactions on Computers*, vol. 99, 2013.

[8] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, pp. 660–670, 2002.

[9] M. Zuniga and B. Krishnamachari, "Analyzing the transitional region in low power wireless links," in *Proc. Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, 2004, pp. 517–526.

[10] Z. Cheng, M. Perillo, and W. Heinzelman, "General network lifetime and cost models for evaluating sensor network deployment strategies," *IEEE Transactions on Mobile Computing*, vol. 7, pp. 484–497, 2008.

[11] M. Cheng, X. Gong, and L. Cai, "Joint routing and link rate allocation under bandwidth and energy constraints in sensor networks," *IEEE Transactions on Wireless Communications*, vol. 8, pp. 3770–3779, 2009.

[12] E. Specht. The best known packings of equal circles in the unit circle. [Online]. Available: http://hydra.nat.uni-magdeburg.de/packing/