Markov-Chain Model for Unbounded Key Propagation

March 7, 2013

1 Three Children Model

In this case we let the number of children $m = 3$. Following the approach for the $m = 2$ case, we now define the following sets S_1, S_2, S_3, S_4, and S_5.

$$\begin{aligned}
S_1 &= \text{The number of nodes with 3 children} \\
S_2 &= \text{The number of nodes with 2 children} \\
S_3 &= \text{The number of nodes with 1 children} \\
S_4 &= \text{The number of nodes with 0 children} \\
S_5 &= \text{The number of nodes that are not connected}
\end{aligned}$$

In a network with n nodes, we can see that $\sum_{i=1}^{5} S_i = n$.

Now we examine the change of the network state at each epoch, where a node is assumed to only obtain one new child node connection in an epoch. To capture this behavior, we define the following variables D_2, D_3, and D_4 to be the number of new nodes connected from nodes in sets S_2, S_3, and S_4, respectively. Using this information, the transfer equations clearly generalize to:

$$\begin{aligned}
S_1 &\to S_1 + D_2 \\
S_2 &\to S_2 - D_2 + D_3 \\
S_3 &\to S_3 - D_3 + D_4 \\
S_4 &\to S_4 + D_2 + D_3 \\
S_5 &\to S_5 - D_2 - D_3 - D_4
\end{aligned}$$

Clearly, the initial state of the network is $S* = (S_1, S_2, S_3, S_4, S_5) = (0, 0, 0, 1, n-1)$. Using the aforementioned transfer equations we can represent this state as $S* = (D_2, D_3 - D_2, D_4 - D_3, 1 + D_2 + D_3, n - 1 - D_2 - D_3 - D_4)$. Therefore, we can represent the state of the network using a three-dimensional vector $D_k = (D_2, D_3, D_4)$.

If we now consider transitions in the state of the network by some vector $\bar{h} = (i, j, k)$, where the transition is defined as $D + \bar{h} = (D_2 + i, D_3 + j, D_4 + k)$, as well as the transfer equations used to define the network state evolution, we come up with the following constraints for $\bar{h}$

Based on the transfer equations, we can also define the following constraints for the network state.

$$0 \le i \le D_3 - D_2 \tag{1}$$
$$0 \le j \le D_4 - D_3 \tag{2}$$
$$0 \le k \le 1 + D_2 + D_3 \tag{3}$$
$$i + j + k \le n - 1 - D_2 - D_3 - D_4 \tag{4}$$

With these constraints, we conclude that the network can evolve along any vector path bounded by these constraints and the line $D_2 + D_3 + D_4 = n - 1$, which is the point where all nodes have the key. A visual depiction of the unconstrained and partly constrained network state space is shown in Figures 1 and 1.

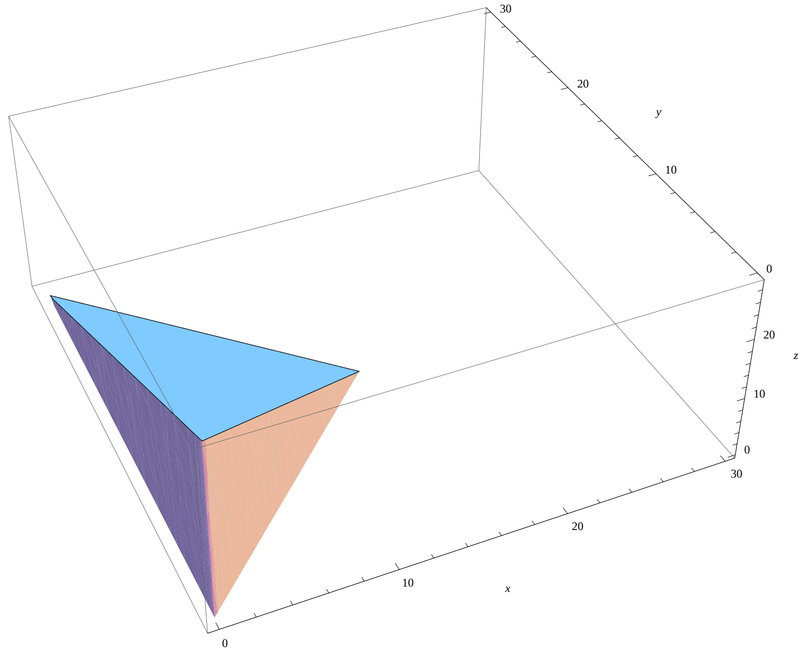

Figure 1: Plot of the network space under constraint 1, where x, y, and z are D_2, D_3, and D_4, respectively.

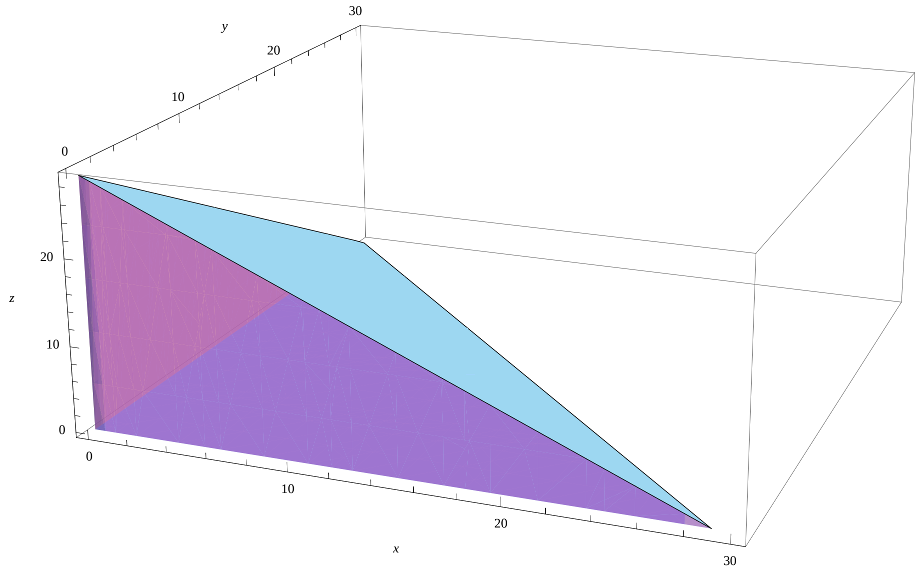

Figure 2: Plot of the network space without constraints, where x, y, and z are D_2, D_3, and D_4, respectively.

With a constrained network state space, we can now define the expected time for a key to be distributed, $E(T_D)$, by assigning a probability $P_D(\bar{h})$ to each possible network state transition. In particular, we have the following.

$$P_D(\bar{h}) = \Pr[D_{s+1} = D + \bar{h} | D_s = D]$$

In this context, D_s is the state of the network at state s (i.e. after s epochs). We can now define $E(T_D)$ as follows,

$$E(T_D) = \frac{1}{1 - P_D(\bar{h*})}[1 + \sum_{\bar{h} \in A_{D_s}} P_D(\bar{h}) \times E(T_{D+\bar{h}})],$$

where $A_{D_s} = \{(i, j, k) | 0 < i + j + k \leq n - 1 - D_2 - D_3 - D_4, 0 \leq i \leq D_3 - D_2, 0 \leq j \leq D_4 - D_3, 0 \leq k \leq 1 + D_2 + D_3\}$.

From this point, we refer to the original proof of the correctness of this equation. No further work must be done

2 Generalized Model

Following the approach for the $m = 3$ case, we can generalize the this model to $m \geq 4$ as follows.

1. Define network state sets S_1, S_2, $\ldots$, S_{m+1}, S_{m+2}, and also define network state variables D_2, $\ldots$, D_m, D_{m+1}.

2. Generalize the transfer equations to the following.

$$\begin{aligned}
S_1 &\to S_1 + D_2 \\
S_2 &\to S_2 - D_2 + D_3 \\
S_i &\to S_i - D_i + D_{i+1} \\
S_{m+1} &\to S_{m+1} + \sum_{k=2}^{m} D_k \\
S_{m+2} &\to S_{m+1} - (\sum_{k=2}^{m+1} D_k)
\end{aligned}$$

3. Represent the network state space in terms of all D_i variables, thus resulting in a m-dimensional network state space.