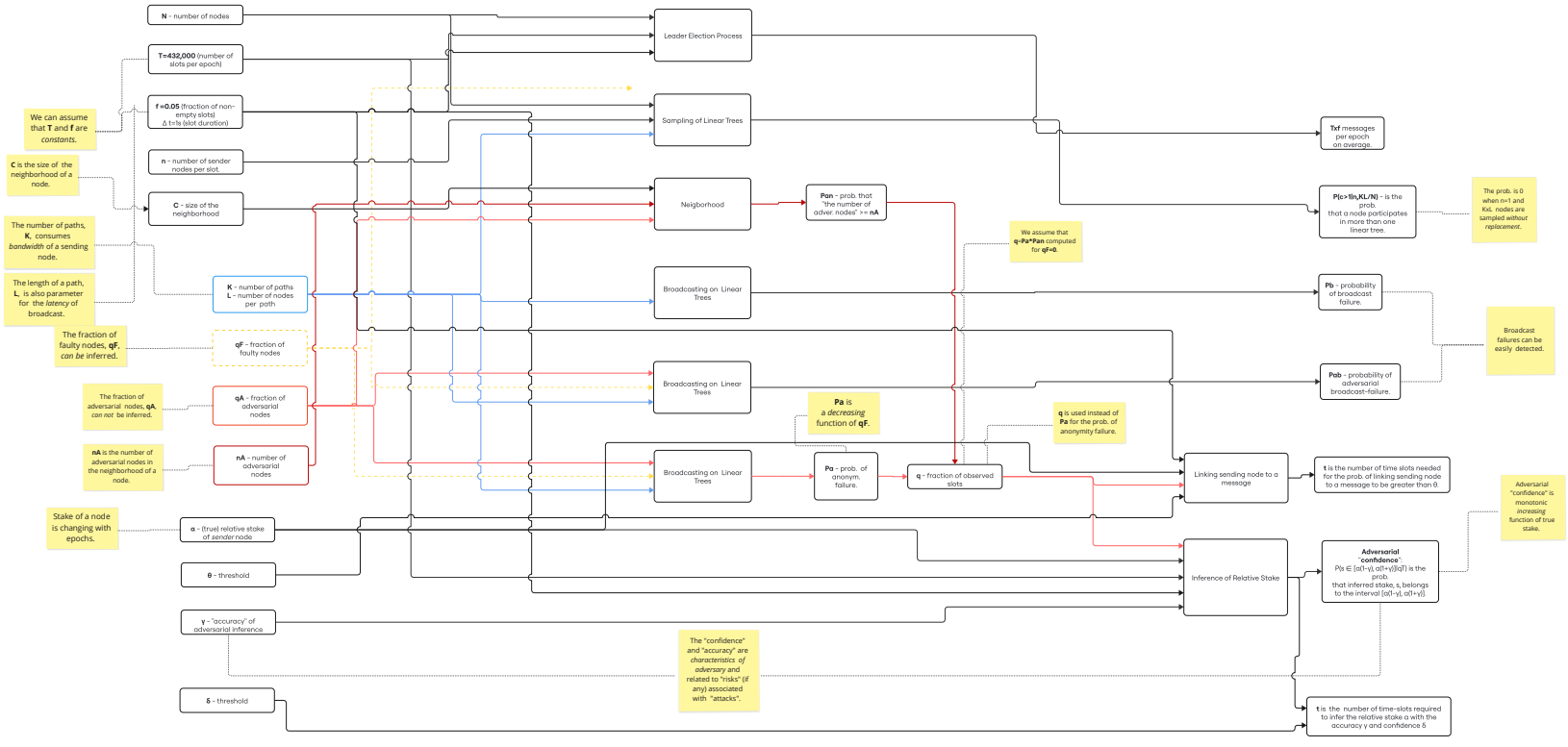
N - number of nodes
T=432,000 (number of slots per epoch)
f =0.05 (fraction of non-empty slots)
Δ t=1s (slot duration)
n - number of sender nodes per slot.
C - size of the neighborhood
K - number of paths
L - number of nodes per path
qF - fraction of faulty nodes
qA - fraction of adversarial nodes
nA - number of adversarial nodes
α - (true) relative stake of sender node
θ - threshold
γ - "accuracy" of adversarial inference
δ - threshold
Leader Election Process
Sampling of Linear Trees
Neigborhood
Broadcasting on Linear Trees
Broadcasting on Linear Trees
Broadcasting on Linear Trees
Pan - prob. that "the number of adver. nodes" >= nA
Pa - prob. of anonym. failure.
q - fraction of observed slots
Linking sending node to a message
Inference of Relative Stake
Txf messages per epoch on average.
P(>1ln,KL/N) - is the prob. that a node participates in more than one linear tree.
Pb - probability of broadcast failure.
Pab - probability of adversarial broadcast-failure.
t is the number of time slots needed for the prob. of a sending node to a message to be greater than θ.
Adversarial "confidence": P(s ∈ [α(1-γ), α(1+γ)]|qT) is the prob. that inferred stake, s, belongs to the interval [α(1-γ), α(1+γ)].
t is the number of time-slots required to infer the relative stake α with the accuracy γ and confidence δ
We can assume that T and f are constants.
C is the size of the neighborhood of a node.
The number of paths, K, consumes bandwidth of a sending node.
The length of a path, L, is also parameter for the latency of broadcast.
The fraction of faulty nodes, qF, can be inferred.
The fraction of adversarial nodes, qA, can not be inferred.
nA is the number of adversarial nodes in the neighborhood of a node.
Stake of a node is changing with epochs.
The "confidence" and "accuracy" are characteristics of adversary and related to "risks" (if any) associated with "attacks".
We assume that q=Pa*Pan computed for qF=0.
Pa is a decreasing function of qF.
q is used instead of Pa for the prob. of anonymity failure.
The prob. is 0 when n=1 and KxL nodes are sampled without replacement.
Broadcast failures can be easily detected.
Adversarial "confidence" is monotonic increasing function of true stake.