0.1 Mathematical Logic

To understand better how the protocol is working, we derived two equations that will explain the ***security models***:

1. First equation will explain the ***round complexity*** of the best, average and the worst case scenarios.

2. Second equation will explain the ***communication complexity***.

Round Complexity: Is defined as the number of rounds it takes the protocol to send p packets over n channels.
Let $n =$ total number of channels
Let $b =$ number of bad/corrupted channels
Let $p =$ number of packets to be sent
Let $q =$ max number of rounds
Consider $p = n$ for simplicity
Assume always $b < n$
General form of b : $b = c \times n$ Where c is the fraction of corrupted channels out of n.

Examples of the form of b:

$$b = \frac{2}{3}n, \qquad b = \frac{3}{4}n, \qquad b = \frac{1}{2}n$$

As an example, assume the total number of channels $n =$ 10, the total number of packets to send $p =$ 10, the number of corrupted channels is $b = 5$. So, $b = \frac{1}{2}n$.

In the best case scenario:

- In round 1, we expect $\frac{1}{2}$ of the total packets to be delivered.

- In round 2, we expect the other $\frac{1}{2}$ of the packets to be correctly delivered.

According to that, we can derive the equation of the best case scenario:
#packets correctly delivered after q rounds =

$$\frac{p}{n-q} \tag{1}$$

In the worst case scenario:

- In round 1, we expect $\frac{1}{2}$ of the total packets to be delivered.

- In round 2, we expect $\frac{1}{2}$ of the remaining packets to be correctly delivered.

- In round 3, we expect $\frac{1}{2}$ of the remaining packets to be correctly delivered.

Based on this, we deduce the #packets that are correctly received in each round to be:

- ***Round*** #1: $(n-nc)$ packets, which translates to half of the packets are correctly delivered.

- ***Round*** #2: $(nc - nc^2)$ packets, which translates to half of the remaining packets will be correctly delivered.

- ***Round*** #3: $(nc^2 - nc^3)$ packets, which translates to half of the remaining packets will be correctly delivered.

- ***Round*** #q: $(nc^{(q-1)} - nc^q)$ packets, as this is the final round, all the remaining packets will be delivered in this round.

According to that, we can derive the equation:
#packets correctly delivered after q rounds =

$$\sum_{i=1}^{q}[(1-c) \times c^{(i-1)} \times n] \tag{2}$$

Now, in the case where $p > n$. Then, the general form of p will be: $p = m \times n + r$
Where m is the coefficient and r is the remainder.
Examples of the form of p:

$$p = 4n + 2, \qquad p = 3n + 5, \qquad p = 17n + 2$$

In this case, the general form of the equation will become:
#packets correctly delivered after q rounds =

$$m[\sum_{i=1}^{q}[(1-c) \times c^{(i-1)} \times n]] + \sum_{i=\frac{n}{r}}^{q}[(1-c) \times c^{(i-1)} \times n] \tag{3}$$

In the case where $r = 0$. Then the equation will become:
#packets correctly delivered after q rounds =

$$m[\sum_{i=1}^{q}[(1-c) \times c^{(i-1)} \times n]] \tag{4}$$

Note: The above equation assumes that the watcher will always corrupt the maximum number of packets. In other words, this equation calculates the #packets of packets correctly delivered over each round in the worst case scenario.

The average case scenario:

$$average = \frac{best + worst}{2} \tag{5}$$

Communication Complexity: Is defined as the total number of bytes we're sending in order to deliver the complete file with respect to the number of bytes of the file.
Let n = The total number of channels.
Let s = The size of the packet.
Let r = The total number of rounds.
let f = The file size.

The Communication complexity equation is:

$$cc = n \times s \times r \tag{6}$$

Also, we define the efficiency of the protocol which is:

$$\epsilon = \frac{f}{cc} \times 100 \tag{7}$$