Journal of
*Cybersecurity and Privacy*

MDPI

*Article*

# Model for Quantifying the Quality of Secure Service

**Paul M. Simon *, Scott Graham *, Christopher Talbot and Micah Hayden**

Air Force Institute of Technology, 2950 Hobson Way, Wright-Patterson AFB, OH 45433, USA; christopher.talbot@afit.edu (C.T.); michah.hayden@afit.edu (M.H.)
* Correspondence: paul.simon.ctr@afit.edu (P.M.S.); scott.graham@afit.edu (S.G.)

**Abstract:** Although not common today, communications networks could adjust security postures based on changing mission security requirements, environmental conditions, or adversarial capability, through the coordinated use of multiple channels. This will require the ability to measure the security of communications networks in a meaningful way. To address this need, in this paper, we introduce the Quality of Secure Service (QoSS) model, a methodology to evaluate how well a system meets its security requirements. This construct enables a repeatable and quantifiable measure of security in a single- or multi-channel network under static configurations. In this approach, the quantification of security is based upon the probabilities that adversarial listeners and disruptors may gain access to or manipulate transmitted data. The initial model development, albeit a snap-shot of the network security, provides insights into what may affect end-to-end security and to what degree. The model was compared against the performance and expected security of several point-to-point networks, and three simplified architectures are presented as examples. Message fragmentation and duplication across the available channels provides a security performance trade-space, with an accompanying comprehensive measurement of the QoSS. The results indicate that security may be improved with message fragmentation across multiple channels when compared to the number of adversarial listeners or disruptors. This, in turn, points to the need, in future work, to build a full simulation environment with specific protocols and networks to validate the initial modeled results.

**Keywords:** communication model; security; metrics; probability; confidentiality; integrity

check for updates

**Citation:** Simon, P.M.; Graham, S.; Talbot, C.; Hayden, M. Model for Quantifying the Quality of Secure Service. *J. Cybersecur. Priv.* **2021**, *1*, 289–301. https://doi.org/10.3390/jcp1020016

Academic Editor: Thaier Hayajneh

Received: 27 February 2021
Accepted: 29 April 2021
Published: 7 May 2021

## 1. Introduction

Communication networks rely on a series of wired or wireless channels between intermediate nodes. In addition to noise, these channels may be affected by any combination of three malicious attack vectors: Denial of Service (DoS), data injection, or eavesdropping. A DoS attack may involve cutting a wire or overpowering a particular frequency (jamming). A data injection, or spoofing attack, involves the adversary sending fabricated data that takes the place of actual data. Finally, and the most difficult to discover, is an eavesdropping attack, which involves an adversary intercepting and extracting useful information from the channel. Managing those threats requires an ability to accurately gauge the likelihood or severity of the threat, and adapt the security features available in the system to meet it.

This paper describes a mathematical model for quantifying the Quality of Secure Service (QoSS) deployed in static communications networks. Just as Quality of Service (QoS) metrics describe measurable aspects of the available network, QoSS describes, in measurable and repeatable terms, the security available to an end-user, facilitating meaningful comparisons.

Even when security is momentarily adequate in a communication system, security mechanisms tend to be static, implemented at installation or while running [1], and cannot be adjusted dynamically based on changing environmental conditions or adversarial capability. This document illustrates the mathematical framework and analysis to define the design requirements for networks and provides a foundation for subsequent work analyzing dynamic network security performance in the presence of varied environmental characteristics[1]. The final model demonstrates the probability of data surviving intact against multiple forms of adversarial actions.

## 2. Goals and Approach

The current literature suggests three primary characteristics that define the security of traditional Information Technology (IT) systems. These are confidentiality, integrity, and availability, i.e., the CIA triad [2,3]. To quantify an overall level of security, we must have objective metrics to represent each of these individual characteristics. While objective metrics for availability are well established as QoS metrics, confidentiality and integrity [4] remain rather subjective and without commonly accepted quantifiable definitions. In addition, the user requirements for security may change based on changing operational conditions. Then, what are the appropriate measures for communication security?

To address the need, we propose a model to quantify the security characteristics of point-to-point communication between two devices[2]. The model is patterned after existing quantification models [5,6], and helps to define security requirements that, in the presence of adversarial actions, would enable communications to be successful. By comparison, this model does not rely on the application of security controls [7], but rather the analysis of the system architecture and probabilistic aspects of the network.

## 3. Components of a Security Model

According to Lundin [1], an equation to describe the tunable security for a communication system could be

$$TS : T \times Env \rightarrow R \tag{1}$$

where $TS$ is the tunable security, which may be dynamically adjusted based on the user security requirements. The transmitter capabilities[3] are represented by $T$, the environmental descriptions are represented by $Env$, and the overall system security requirements are represented by $R$. The goal is to map the tunable security services to the system security requirements. To achieve this, the tunable security services must first be decomposed into the constituent parts, such as the available number of channels, the use or disuse of encryption, and the amount of fragmentation across the network. In many cases, the environmental descriptions are directly reflected in the traditional QoS measurements available from the service provider.

This initial version of the QoSS model is a static snap-shot, reflecting the system security at one point in time. The multiplication operator in Equation (1) does not adequately address the numerous non-linear relationships between system capability and environmental aspects. Instead, QoSS captures those factors as an array of features or values and then relates the transmitter capabilities and the environmental description to the CIA triad, where confidentiality, $C$, and integrity, $I$, replace the transmitter capabilities, and availability, $A$, replaces the environmental descriptors.

Security measures are typically subjective. To achieve objectivity, we substitute measurements of confidentiality and integrity with the probability of each, designated as $P(C)$ and $P(I)$, respectively, as discussed in subsequent sections. Although it is unconventional to consider a DoS attack as impacting data integrity (described in subsequent sections), doing so has the added benefit of collecting all adversarial influences into the metrics for confidentiality and integrity, leaving only the system and network capabilities to be considered as availability. Availability is a specific set of objective performance metrics, or QoS, provided by the transmitter, e.g., data or bit rate, jitter, bandwidth, transmission frequency, or power. The resulting QoSS equation is

$$QoSS : [P(C), P(I), A] \rightarrow Security\ Requirements \tag{2}$$

representing a snapshot of QoSS metrics mapped to the security requirements. If the array of metrics does not directly map to the security requirements, then the QoSS for that network is inadequate, and the system must be redesigned. The array of metrics also provides a foundation to perform one-to-one comparisons between two networks.

### *3.1. Probability of Confidentiality*

Numerous researchers have attempted to quantify confidentiality with varying success [8,9]. Confidentiality is the aspect of a network that protects against unauthorized message receipt, i.e., preventing an eavesdropper from either receiving or decoding messages. One approach to quantifying confidentiality is to redefine it as a probability so that

$$P(C) = 1 - P(l) \tag{3}$$

where $P(C)$ is the probability of confidentiality and $P(l)$ is the probability of leakage. Leakage refers to an untrusted listener having access to an "information flow from secret inputs to public outputs" [10]. Inspired by Perfectly Secure Message Tranmission (PSMT) [11], the set of all adversarial listeners, $A_L$, maps to a set of wires (channels), $\sigma$, that the listeners have access to; if one of the members of $A_L$ has access to the information, then the probability of leakage exists.

For leakage to occur, a listener must intercept the message, decrypt it (if applicable), and then decode the data contained in the message. The probability of interception, $P(int)$, quantifies the probability that a listener with channel access will receive the message. The probability of decryption, $P(dcr)$, quantifies the probability that the adversary will decrypt it[4]. Finally, the probability of decoding, $P(dco)$, quantifies the probability that an adversary will decode the message[5].

Consider the relationship between the probabilities of interception, decryption, and decoding. For data leakage to occur, an adversary must be able to achieve all three actions, i.e., decryption is irrelevant if the adversary is unable to receive any messages. Conversely, receiving every transmission ever sent is irrelevant if an adversary is unable to decrypt or decode the messages. The logical binary relationship of how $P(l)$ relates to $P(int)$, $P(dcr)$, and $P(dco)$ is captured in Table 1. The proposed equation to describe $P(l)$ in terms of $P(int)$, $P(dcr)$, and $P(dco)$ is

$$P(l) = P(int) \times P(dcr) \times P(dco). \tag{4}$$

**Table 1.** Logical binary relationship for the probability of leakage.

| *P*(*int*) | *P*(*dcr*) | *P*(*dco*) | *P*(*l*) |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 0 |
| 0 | 1 | 0 | 0 |
| 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 0 |
| 1 | 0 | 1 | 0 |
| 1 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 |

### *3.2. Probability of Integrity*

Quantifying integrity is equally challenging. Integrity is a measure of the consistency, accuracy, and trustworthiness of data. Integrity implies that data has not been changed by unauthorized users in transit. One method of quantifying integrity is the "prevention of unauthorized modification of information" [10]. Under this assumption, unauthorized modification is *corruption*, resulting in

$$P(I) = 1 - P(c) \tag{5}$$

where $P(I)$ is the probability of integrity and $P(c)$ is the probability of corruption. Corruption here captures any damage to integrity yielding "two notions of corruption " where the "first leads us to a measure that we call *contamination*" and the "second leads us to ... *suppression*" [10]. Contamination may arise from adversarial action, *injection*, or non-adversarial input, *noise*. Further, an adversary may carefully inject portions of false data (a spoofing attack), inject massive amounts of false data to disable communications (the traditional DoS attack), or overtly jam a message with a false signal (traditional RF jamming).

Therefore, we choose to classify DoS attacks as being an attack on the integrity of the data or message, not as an attack on the availability of the network. Again, inspired by PSMT [11], the set of all adversarial disruptors, $A_D$, maps to a number of wires, $\rho$, that the disruptors have access to; if one of the members of $A_D$ has access to the information, then the probability of corruption exists.

We, therefore, posit that corruption has three components: noise, data suppression, and data injection. The probability of noise occurring in a message, $P(n)$, is the probability that a message will be adversely affected by noise. Noise is a natural phenomenon that happens regardless of the transmitter's capability. The probability of suppression, $P(s)$, quantifies the probability that an adversary will suppress or jam the message, thus, preventing the receiver from obtaining the message[6]. Finally, the probability of injection, $P(inj)$, quantifies the probability that an adversary will inject false data into the message. $P(inj)$ requires the ability to insert malicious data into a data stream, a much more sophisticated activity than that of jamming[7]. Since noise is a natural phenomenon, it is consistently present and may influence $P(s)$ and $P(inj)$. Noise works cooperatively with $P(s)$ since both cause the receiver to incorrectly receive the intended message. Based on these probabilities, the logical binary relationship for $P(c)$ is shown in Table 2 and reflected as

$$1 - P(c) = \big(1 - P(n)\big) \times \big(1 - P(s)\big) \times \big(1 - P(inj)\big). \tag{6}$$

Equation (6) does not adequately capture the behavior of the system. Noise may be detrimental to data injection, making the injected data unusable. Due to the interaction between $P(n)$ and $P(inj)$, namely that noise affects both intended and malicious transmissions, a more comprehensive equation is

$$\begin{aligned} P(c) =& \Big(\big(1 - P(n)\big) \times P(inj)\Big) + \big(P(n) + P(s)\big) - \big(P(n) \times P(s)\big) \\ & - \Big(\big(1 - P(n)\big) \times P(inj) \times \big(P(n) + P(s)\big)\Big). \end{aligned} \tag{7}$$

While less elegant than Equation (6), Equation (7) provides realistic results that account for all probabilities between 0 and 1 for each of the factors.

**Table 2.** Logical binary relationship for the probability of corruption.

| ***P*(*n*)** | ***P*(*s*)** | ***P*(*inj*)** | ***P*(*c*)** |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |

### *3.3. Availability*

Methods exist for assessing and improving the performance of a system based on QoS measures [12]. For the QoSS model, the metrics used to describe availability are already conveyed in the QoS metrics. This is reflected as $A = QoS$, where QoS is the set of metrics that include cost, jitter, latency, bandwidth, and bit rate, which already provide a repeatable method of measuring availability.

### 3.4. Multiple Channels

Using multiple channels can improve the performance of data-in-transit in diverse ways. A straightforward example is directly increasing the data rate, such that additional channels provide more bandwidth, e.g., channel bonding within IEEE 802.11 [13–16]. Another example is frequency hopping through multiple channels, which is one of several techniques known as the spread spectrum and which provides protection from noise or jamming as the signal is "spread across a channel greater than that necessary to transmit the information" [17]. This technique is currently used in Bluetooth, and such transmission diversity is also a key element of 5G wireless [18,19].

An example of data-at-rest performance improvement through multiple channels is found in the Redundant Array of Inexpensive Disks (RAID) architecture. Developed in 1987, RAID demonstrated that by utilizing redundancy, an array could be more reliable than any one disk drive while allowing greater data throughput (In a RAID array, data is split across various disks so that if one disk should fail, the data may be fully recovered despite not having all the original blocks of data. Various combinations of nested RAID levels may be used to reduce the vulnerabilities of simultaneous disk failures [20]. The data may also be encrypted before or after splitting, or both, as a manner of increasing confidentiality.). Despite significant overhead, the ability to survive disk failures has made it very attractive in critical server environments.

Many applications in control systems maintain separate channels for data and control. For example, in SS7[8], the signaling path is separate and distinct from the voice channels that carry the telephone conversation. Having different channels, at different frequencies and differing bandwidths, allows for greater flexibility and higher-speed communications between network assets without the need to rely upon the availability or limitations of analog voice channels (In reality, these two channels are not entirely separated. The dual-tone, multi-frequency (DTMF) digits dialed by a caller begin within the voice channel, but are recognized by the control channel and are an example of the signaling messages, including dialing a phone number, entering control functions like call-forwarding, or advanced billing information [21,22]).

An abstract form of multi-channel communication is two-factor authentication (2FA), a subset of multi-factor authentication. This is an authentication methodology that requires a user to present two or more pieces of evidence to confirm the user's identity via separate delivery paths[9] [23]. By using multiple authentication factors sent via divergent paths, the likelihood that both messages are intercepted decreases. Even if a malicious actor intercepts one factor, full authentication by the malicious actor cannot occur without intercepting the other. Numerous other forms of 2FA also exist [24].

Central to the theme of this paper, *multiple channel* architecture may also be used to improve security through data fragmentation across heterogeneous channels [25–28]. This security focused capability, in concert with the performance advantages of multi-channel communications, is the motivation for creating a tunable multi-channel communication protocol and associated analysis techniques to determine the appropriate trade-offs under varying security and performance requirements.

## 4. The Quality of Secure Service Model

Although a communication network typically uses only one network channel between two given nodes, the possibility exists to utilize multiple paths between nodes, as shown in Figure 1. This figure shows an arbitrary network with eight individual channels, any of which may be used to transport data. A message sent through the network in Figure 1 may travel across one of the channels influenced by the set of adversarial listeners, $A_L$, or the set of adversarial disruptors, $A_D$.

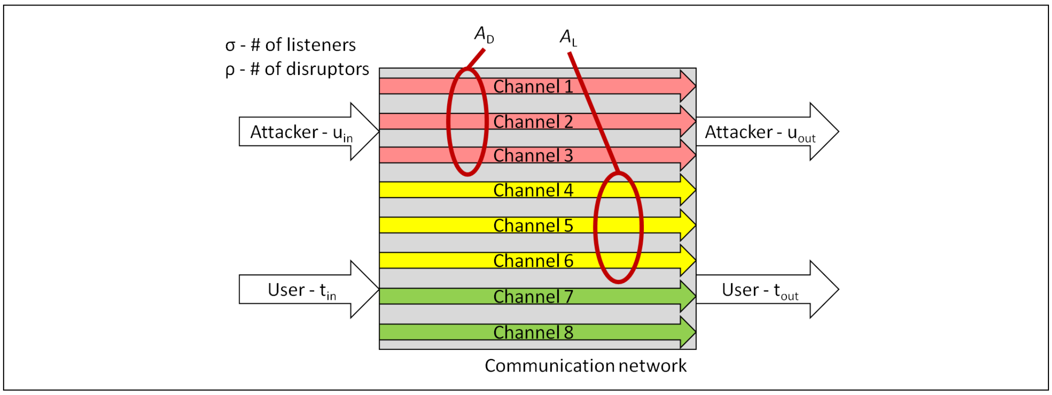

**Figure 1.** A network configuration with multiple possible channels.

The relationship between listeners, disruptors, and the total number of needed channels is described by PSMT, which "abstract[s] away the network entirely and concentrate[s] on solving the Secure Message Transmission Problem" for a single transmitter and receiver pair [11]. Additional articles explore multi-channel architectures [29,30], while others strive to prove the general case and optimize the statistical reliability and secrecy [31,32].

In our model, $\sigma$ represents the number of wires (channels) between the transmitter and receiver available to the adversarial listener set, $A_L$, and $\rho$ is the number of channels between the transmitter and receiver available to the adversarial disruptor set, $A_D$[10]. Communication is two-way between the transmitter and receiver and, following PSMT, the number of channels that must exist between transmitter and receiver is given by

$$n \geq max\{\sigma + \rho + 1;\ 2\rho + 1\}. \tag{8}$$

With this equation, we know how many channels must be used to maintain secure and reliable communication. If a channel is unavailable, then it must not be counted as part of $n$. If we assume the number of channels accessible to a listener or disruptor, then we can arrive at a specific quantification of $n$. For example, when $n = 8$ and $\sigma = 3$, the probability that any one channel of the eight could be listened to is 0.375. The probability of leakage for each channel within a multi-channel architecture becomes

$$P(l) = \frac{P(int) \cdot P(dcr) \cdot P(dco) \cdot \sigma}{n}. \tag{9}$$

Similarly, the probability of corruption for each channel within multi-channel architecture becomes

$$P(c) = \frac{\left(\begin{array}{r}(1-P(n))P(inj)+(P(n)+P(s))-(P(n)P(s))\\ -(1-P(n))(P(n)+P(s))P(inj)\end{array}\right)\rho}{n}. \tag{10}$$

Therefore, the more channels there are in a network, the lower the probability of adversarial interference of the data[11]. This, then, follows the premise of PSMT: to have more channels than the combined set of listeners and disruptors $A_L \cup A_D$.

In the same manner that multiple channels may thwart adversarial interference, message fragmentation may also thwart eavesdropping. Message fragmentation is the splitting of data across the available channels, effectively parallelizing the data. Fragmentation describes how many portions the original message is divided into. Various methods of fragmentation are possible, including uniform or non-uniform fragmentation from 1-bit to the total $m$-bits in message $M$. Research has been published on particular approaches to fragmentation [28,33]; however, in this paper,we focuse on the security effects and apply the assumption that fragments are of equal size across the network. If $C_n$ is the set of $n$ channels, and $F_M$ is the set of $k$ fragments of $1 \leq |f_i| \leq m$-bits of the message $M$, then

$$F_M = \{f_{(M,1)}, f_{(M,2)}, f_{(M,3)}, \ldots, f_{(M,k)}\} \tag{11}$$

$$f_{(M,i)} \subseteq M \; for \; 1 \leq i \leq k \tag{12}$$

where each fragment is unique. The channel load, $L$, is the percentage of $M$ on a particular channel $j$, such that

$$L_{(j,M)} = \frac{\sum_{i=1}^{n} |f_i| \; for \; f_i \in C_{(j,M)}}{|M|} \tag{13}$$

and the Average Loading (AL) for the set of channels is

$$AL_M = \frac{\sum_{i=1}^{n} L_{(j,M)}}{n}. \tag{14}$$

For example, $F_M = \{f_1, f_2, f_3, f_4, f_5, f_6, f_7, f_8\}$ is the set of eight fragments of message $M$ on a network that has $n = 8$ channels, and each channel transmits two fragments. Therefore, $AL = 0.25$. Message fragmentation also allows for duplicating data across channels. The Duplication Factor (DF) measures the average number of times a given fragment is transmitted, indicating the network redundancy. The DF may increase as compensatory tuning for known adversarial interactions. For the previous example, $DF = 2$, since each fragment is sent across two channels and, thus, duplicated twice. For these calculations of DF and AL, the fragment sizes are uniform.

The AL and DF directly affect $P(C)$ and $P(I)$. Of the constituent parts of $P(C)$, $P(int)$ is only affected by DF in aggregation across all channels because the probability of interception of a single channel is not necessarily improved by duplication or fragmentation. However, $P(int)$ may be increased by the message $M$ being duplicated across multiple channels, offering an adversary more opportunities to intercept portions of the message.

Therefore, DF is only multiplied by $P(int)$ when averaging all the channels into a composite probability of leakage. For the constituent parts of $P(I)$, duplication directly affects $P(s)$ because sending fragments multiple times decreases the probability of lost data through suppression. $P(n)$ and $P(inj)$ are not directly influenced by duplication. Thus, $P(s)$ is divided by $DF$ for each channel, giving

$$P(c) = \frac{\begin{pmatrix} (1-P(n))P(inj) + (P(n) + \frac{P(s)}{DF}) - (P(n)\frac{P(s)}{DF}) \\ \qquad - (1-P(n))(P(n) + \frac{P(s)}{DF})P(inj) \end{pmatrix}\rho}{n}. \tag{15}$$

Fragmentation does not necessarily increase or decrease $P(s)$ except that it allows for duplication. However, fragmentation does directly affect $P(inj)$ since each fragment sent needs to be modified by the adversary in order to have malicious data accepted at the receiver. Thus, $P(inj)$ is multiplied by AL for each channel, giving

$$P(c) = \frac{\begin{pmatrix} (1-P(n))P(inj)AL + (P(n) + \frac{P(s)}{DF}) - (P(n)\frac{P(s)}{DF}) \\ \qquad - (1-P(n))(P(n) + \frac{P(s)}{DF})P(inj)AL \end{pmatrix}\rho}{n}. \tag{16}$$

Applying the PSMT and decomposing the network into constituent channels yields

$$QoSS : \begin{bmatrix} P_1(C), & P_1(I), & QoS_1 \\ P_2(C), & P_2(I), & QoS_2 \\ \vdots & \vdots & \vdots \\ P_n(C), & P_n(I), & QoS_n \end{bmatrix} \rightarrow Sec \; Reqs, \tag{17}$$

which highlights that each channel has its own characteristics. From the end-user perspective, only the aggregated QoSS for the entire network is apparent. With insight into each channel's QoSS, an analyst may suggest a different quantity of channels, different fragmentation or duplication, or a different encoding or encryption algorithm if adversarial actors attempt to influence communications.

## 5. Case Studies of Multi-Channel QoSS

The three example networks presented here are used to highlight the initial estimates and are intended to be refined as the network understanding is increased. For simplicity, the probabilities used in the following examples are discrete values; however, any value between 0 and 1 is possible. In developing the QoSS model, estimating the intermediate values is a challenge. As a starting point, 0 may be used for a network that has absolutely no encryption, 0.5 may be used for a system that has minimal or sub-standard encryption, and 1 may be used for a system that employs strong encryption.

Incremental changes may be employed as desired or as needed after a baseline understanding is developed, much like understanding the incremental difference between AES-128 and AES-256, or the difference between DES, triple-DES, and AES. The primary goal of the initial model development is to apply estimates for each of the constituent elements as implied by [34]. Further refinement of those estimates may be applied after more thorough system analyses.

During the early stages of analysis, the difference between a probability of 0.76 and 0.77 remains undefined and the numbers tend to be more arbitrary. This serves to assign a starting point for analysis, thus, establishing a baseline. Given the three example networks that follow and some initial probabilistic estimates for the various characteristics, the QoSS model is applied. Each case has a realistic configuration that allows for one-to-one comparison.

### *5.1. Single-Channel Network*

The first example is a network that utilizes a single wireless channel to provide a realistic baseline. With $n = 1$, there is $\sigma = 1$ listener, and $\rho = 1$ disruptor. $AL = 1$ because the message cannot be split, and $DF = 1$ since, for this architecture, the message is only sent once. Table 3 shows notional probabilities for a network that has no encryption, standard data encoding, and a moderate probability of interception because it uses a standard broadcast frequency and a moderately strong broadcast signal, which also results in a low probability of noise.

We assign a high probability of suppression under the assumption of an omnidirectional receiver, susceptible to jamming. The probability for injection is moderately high, though not as high as the probability of suppression, because injection is more challenging than suppression. These values serve as a baseline to demonstrate the effects of multiple channels in the subsequent examples.

**Table 3.** Input and output values for a single-channel network.

| **Channel** | $P(int)$ | $P(dcr)$ | $P(dco)$ | $P(l)$ | $P(C)$ | $P(n)$ | $P(s)$ | $P(inj)$ | $P(c)$ | $P(I)$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.5 | 1 | 1 | 0.5 | 0.5 | 0.25 | 1 | 0.33 | 0.9381 | 0.0619 |

Based on these constraints, the single-channel network has a high probability of leakage, with a corresponding probability of confidentiality. The probability of corruption is also very high, with a correspondingly low probability of integrity. These probabilities may be improved by using encryption and by using directional receivers or a wired connection.

### *5.2. Three-Channel Network*

The second example applies PSMT to the communication architecture, and demonstrates the initial application of multiple channels. In this example, the communication network uses three discrete, heterogeneous channels to communicate between the transmitter and the receiver. For this example, $n = 3$, $\sigma = 1$ listener, and $\rho = 1$ disruptor. One difference between the single channel case and the three-channel case is the AL. The original message is fragmented into three equal portions, $f_1$, $f_2$, and $f_3$, which are each transmitted twice as follows: $\{f_1, f_2\}$ on Channel 1, $\{f_2, f_3\}$ on Channel 2, and $\{f_3, f_1\}$ on Channel 3. For this case $AL = 0.66$, and $DF = 2$ (because each fragment is sent twice).

Table 4 shows the theorized characteristics for a network with various probability of interception and fixed values for probability of decryption and decoding. Additionally, Table 4 shows that the network has various probabilities of injection with fixed values for probability of noise and suppression.

Channel 1 has identical input factors to the single-channel network as demonstrated in Table 3; however, the message is fragmented across multiple channels, which causes the probability of confidentiality and probability of integrity to increase, not only for Channel 1, but for each channel in the network[12]. The average probability of confidentiality is 0.83 even without encryption, indicating that fracturing data across the multiple channels improves the probability of confidentiality and over-all QoSS, partially mitigating the lack of encryption.

**Table 4.** Input and output values for a three-channel network.

| $Channel\ (n)$ | $P_n(int)$ | $P_n(dcr)$ | $P_n(dco)$ | $P_n(l)$ | $P_n(C)$ | $P_n(n)$ | $P_n(s)$ | $P_n(inj)$ | $P_n(c)$ | $P_n(I)$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.5 | 1 | 1 | 0.1667 | 0.8333 | 0.25 | 1 | 0.33 | 0.2219 | 0.7781 |
| 2 | 0.75 | 1 | 1 | 0.2500 | 0.7500 | 0.25 | 1 | 0.4 | 0.2248 | 0.7752 |
| 3 | 0.25 | 1 | 1 | 0.0833 | 0.9167 | 0.25 | 1 | 0.26 | 0.2191 | 0.7809 |
| Avg | 0.5 | 1 | 1 | 0.1667 | 0.8333 | 0.25 | 1 | 0.33 | 0.2219 | 0.7781 |

### *5.3. Eight-Channel Network*

The third example presents a communication network with eight discrete, heterogeneous channels. In this example, $n = 8$, $\sigma = 3$ listeners, and $\rho = 3$ disruptors. The original message is fragmented into eight equal portions, $\{f_1, f_2, ..., f_8\}$, of which $\{f_1, f_2\}$ are transmitted on Channel 1, $\{f_2, f_3\}$ on Channel 2, $\{f_3, f_4\}$ on Channel 3, and so on. Here, $AL = 0.25$, and $DF = 2$ because each fragment is sent twice. Table 5 shows the theorized input for the eight-channel network.

Of particular note, Table 5 has the same input as Table 4 for Channels 1–3, and other values for Channels 4–8, although with different results[13]. The only difference from the three-channel case is that, with eight channels, the message is fragmented across more channels, causing the confidentiality and integrity to increase. The average values for $P(int)$, $P(dcr)$, and $P(dco)$ are the same for the single-channel, three-channel, and eight-channel networks, although the average $P(l)$ and $P(C)$ are notably different.

**Table 5.** Input and output values for an eight-channel network.

| $Channel\ (n)$ | $P_n(int)$ | $P_n(dcr)$ | $P_n(dco)$ | $P_n(l)$ | $P_n(C)$ | $P_n(n)$ | $P_n(s)$ | $P_n(inj)$ | $P_n(c)$ | $P_n(I)$ |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.5 | 1 | 1 | 0.1875 | 0.8125 | 0.25 | 1 | 0.33 | 0.2402 | 0.7598 |
| 2 | 0.75 | 1 | 1 | 0.2813 | 0.7188 | 0.25 | 1 | 0.4 | 0.2414 | 0.7586 |
| 3 | 0.25 | 1 | 1 | 0.0938 | 0.9063 | 0.25 | 1 | 0.26 | 0.2389 | 0.7611 |
| 4 | 0.2 | 1 | 1 | 0.0750 | 0.9250 | 0.25 | 1 | 0.05 | 0.2353 | 0.7647 |
| 5 | 0.35 | 1 | 1 | 0.1313 | 0.8688 | 0.25 | 1 | 0.1 | 0.2361 | 0.7639 |
| 6 | 0.4 | 1 | 1 | 0.1500 | 0.8500 | 0.25 | 1 | 0.2 | 0.2379 | 0.7621 |
| 7 | 0.7 | 1 | 1 | 0.2625 | 0.7375 | 0.25 | 1 | 0.6 | 0.2449 | 0.7551 |
| 8 | 0.85 | 1 | 1 | 0.3188 | 0.6813 | 0.25 | 1 | 0.7 | 0.2467 | 0.7533 |
| Avg | 0.5 | 1 | 1 | 0.1875 | 0.8125 | 0.25 | 1 | 0.33 | 0.2402 | 0.7598 |

As expected, the single-channel network has the lowest theorized QoSS values. With a slightly higher percentage of listeners, the eight-channel network has a slightly higher $P(l)$ and correspondingly lower $P(C)$ than the three-channel network[14]. Similarly, the average values for $P(n)$, $P(s)$, and $P(inj)$ are the same for the single-channel, three-channel, and eight-channel networks, yet the $P(c)$ and $P(I)$ are significantly different.

### 5.4. Implications of Results

The most difficult aspect of developing the QoSS metrics is making assumptions about the network characteristics. For these examples, we began with an assumption that $P(dcr) = 1$ was a baseline value that an adversary would be able to access all critical data. What does this mean for $P(dcr) = 1$? Perhaps the assumption implies that no encryption is used, despite the fact that the use of encryption is strongly encouraged for all communications systems.

Similarly, is this possible for $P(dcr) = 0$? This assumption implies that the encryption is unbreakable at this time and under these communication and environmental conditions. The fact that we do not know the adversary's fullest capabilities, nor do we know the adversary's intentions, are considerations that must be included, within a range, in the estimate for the probabilistic aspect of our metrics. More accurately, we estimate what is possible within the current state-of-the-art and under a set of operational characteristics.

Adversarial intention is much more difficult to estimate; intentions may change rapidly or may vary on a case-by-case basis. In light of that, we have attempted to reflect all the adversarial intentions, whether it is jamming, spoofing, or eavesdropping, within the generalized probability of confidentiality and probability of integrity. With these estimations, both adversarial capability and intention are difficult to concretely quantify in the initial pass, and they are, thus, cast in probabilistic terms.

This version of the QoSS model is a single snap-shot in time; a time-varying QoSS model is in development in which the model estimations may be updated based on new research, information, or changing environmental and systemic conditions. As the QoSS model becomes more mature and broadly adopted, future iterations will benefit from increased understanding of these probabilistic approaches and an initial coarse estimate for design requirements may converge to refined security requirements if applied in an iterative manner.

These iterations point directly to the eventual need for a simulation environment and all the supporting protocols that allow for the verification and validation of the security metrics. To achieve that end, the network performance will need to be influenced by a simulated adversarial actor, and the amount of data leakage or corruption will be directly quantified based on the amount of transmitted data. Only with that final step of validation will we be certain that the model portrays a realistic version of a communication network.

## 6. Conclusions and Future Work

This manuscript represents an initial model intended to be used in developing an understanding of how real-world networks function in the presence of adversarial influence. The current analysis does not address the nuances of specific communication scenarios, and there is no existing network to validate our model. Quantifying security in real-world communication networks is difficult and mostly subjective. Without a metric for confidentiality and integrity, it is nearly impossible to state how secure one network is compared to another.

Using a probabilistic model that considers data leakage and data corruption in place of confidentiality and integrity, a set of metrics may be used to quantify the QoSS. This model allows the direct and repeatable quantification of the security available in a single- or multi-channel network under static configurations. The quantification of security is based directly upon the probabilities that adversarial listeners and disruptors are able to gain access to or change the original message.

Traditional measurements of QoS provide a foundation, and message fragmentation and duplication across the available channels provide demonstrably improved theoretical performance. A fully developed simulation would be useful in validating the modeled results. However, at this time, there is no existing network or simulation of a real network to validate the theoretical QoSS model. A simulation environment is in the process of development in order to include the ability to estimate an adversary's influence, as are the experiments and the network prototype that will be used to test the theoretical QoSS model.

Two additional manuscripts are nearing completion that will address two of the many thorny issues contained within real networks—in particular, multi-hop networks and the changes to the QoSS metrics that occur over time. This future work may require building specific data-handling protocols, and would monitor how the network end-points respond. With the simulation environment developed, the modeled results may be verified and the QoSS model may be validated or improved with additional data and insight.

**Author Contributions:** Conceptualization, P.M.S., S.G. and C.T.; refinement, P.M.S., S.G. and M.H.; methodology, P.M.S. and S.G.; software, P.M.S.; validation, P.M.S.; investigation, P.M.S.; resources, P.M.S.; writing—original draft preparation, P.M.S.; writing—review and editing, P.M.S., S.G. and M.H.; All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded in part by the Air Force Institute of Technology, Center for Cyberspace Research (CCR).

**Institutional Review Board Statement:** This article does not contain any studies with human participants or animals performed by any of the authors.

**Informed Consent Statement:** Not applicable.

**Acknowledgments:** The views expressed in this paper are those of the authors, and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the U.S. Government. This document has been approved for public release.

**Conflicts of Interest:** All authors declare that they have no conflict of interest.

## Notes

[1] Analysis of the dynamic aspects of mobile networks or tunable security mechanisms is left for a subsequent paper, as are changing environmental conditions and temporal adversarial intrusions.

[2] Multi-hop architectures are outside the scope of this paper but are a straightforward extension of the model that will be addressed in a subsequent paper.

[3] Wired and wireless networks have different characteristic values based on the specific technologies and protocols used.

[4] This value reflects the quality of the encryption used, be it no encryption, a simple ROT13 algorithm, or a sophisticated encryption algorithm.

[5] This value highlights the differences in binary strings, and if the adversary has the ability to recognize those differences. For example, an adversary with a .mp3 file who mistakenly believes it is a .txt file, will not be able to derive useful information from that particular file.

[6] To clarify, $P(s)$ is the active jamming by an adversary as quantified at the receiver, whereas availability is quantified by the transmitter's capabilities.

[7] As the adversarial intent of suppression is counter to that of injection, it is unlikely, although not impossible, to have high $P(s)$ and high $P(inj)$. This would be akin to an adversary steering a receiving channel to a compromised channel by jamming the intended channel. Neither of these speaks directly to the intent of an adversary but rather to the requirements and built-in capabilities of the transmitter and receiver.

[8] Signaling System Number 7 (SS7) was developed in 1975 as a set of protocols used to set up and tear down public switched telephone network (PSTN) communication connections.

[9] The user's identity is verified by using a combination of two or more factors: something they know, something they have, or something they are.

[10] In the general case, $A_L$ or $A_D$ may be subsets of or intersect with each other; i.e., $A_L \subseteq A_D$, or $A_D \subseteq A_L$ or $A_L \cap A_D$.

[11] One potential implication is that each channel may carry both a portion of the data and be used as a method to check for errors on the others channels

[12] In a real communication architecture, all three channels would likely have more similar characteristics.

[13] As in the Three-Channel example, a real communication system would likely have channels with similar characteristics.

[14] Note the number of channels with respect to Equation (8) for this multi-channel space. For the eight-channel network, $n = 8$ even though seven channels would be sufficient based on $\sigma = 3$ listeners, $\rho = 3$ disruptors, and Equation (8).

## References

1. Reine, L.; Lindskog, S.; Brunstrom, A. A Model-based Analysis of Tunability in Privacy Services. In *IFIP International Summer School on the Future of Identity in the Information Society*; Springer: Boston, MA, USA, 2007.
2. Hughes, J.; Cybenko, G. Quantitative metrics and risk assessment: The three tenets model of cybersecurity. *Technol. Innov. Manag. Rev.* **2013**, *3*, 15–24. [CrossRef]
3. Jabbour, K.; Poisson, J. Cyber risk assessment in distributed information systems. *Cyber Def. Rev.* **2016**, *1*, 91–112.
4. Wang, J.A.; Xia, M.; Zhang, F. Metrics for information security vulnerabilities. *J. Appl. Glob. Res.* **2008**, *1*, 48–58.
5. Duan, Q. Modeling and analysis of end-to-end quality of service provisioning in virtualization-based future Internet. In Proceedings of the 2010 Proceedings of 19th International Conference on Computer Communications and Networks, Zurich, Switzerland, 2–5 August 2010.
6. Firoiu, V.; Le Boudec, J.Y.; Towsley, D.; Zhang, Z.L. Theories and models for internet quality of service. *Proc. IEEE* **2002**, *90*, 1565–1591. [CrossRef]
7. Leon, P.G.; Saxena, A. An approach to quantitatively measure information security. In Proceedings of the 3rd India Software Engineering Conference, Mysore, India, 25–27 February 2010.
8. Clarkson, M. Quantification and Formalization of Security. Ph.D. Dissertation, Cornell University, Ithaca, NY, USA, 2010. Available online: https://ecommons.cornell.edu/handle/1813/14744 (accessed on 15 March 2021).
9. Nikhat, P.; Beg, M.R.; Khan, M.H. Model to quantify confidentiality at requirement phase. In Proceedings of the 2015 International Conference on Advanced Research in Computer Science Engineering & Technology (ICARCSET 2015), Unnao, India, 6–7 March 2015.
10. Clarkson, M.R.; Schneider, F.B. Quantification of integrity. *Math. Struct. Comput. Sci.* **2015**, *25*, 207–258. [CrossRef]
11. Dolev, D.; Dwork, C.; Waarts, O.; Yung, M. Perfectly secure message transmission. *J. ACM (JACM)* **1993**, *40*, 17–47. [CrossRef]
12. Almerhag, I.A.; Almarimi, A.A.; Goweder, A.M.; Elbekai, A.A. Network security for QoS routing metrics. In Proceedings of the International Conference on Computer and Communication Engineering (ICCCE'10), Kuala Lumpur, Malaysia, 11–12 May 2010.
13. Faridi, A.; Bellalta, B.; Checco, A. Analysis of dynamic channel bonding in dense networks of WLANs. *IEEE Trans. Mob. Comput.* **2016**, *16*, 2118–2131. [CrossRef]
14. Han, M.; Khairy, S.; Cai, L.X.; Cheng, Y. Performance analysis of opportunistic channel bonding in multi-channel WLANs. In Proceedings of the 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, USA, 4–8 December 2016.
15. Lee, S.; Kim, T.; Lee, S.; Kim, K.; Kim, Y.H.; Golmie, N. Dynamic Channel Bonding Algorithm for Densely Deployed 802.11 ac Networks. *IEEE Trans. Commun.* **2019**, *67*, 8517–8531. [CrossRef]
16. Bukhari, S.H.R.; Rehmani, M.H.; Siraj, S. A survey of channel bonding for wireless networks and guidelines of channel bonding for futuristic cognitive radio sensor networks. *IEEE Commun. Surv. Tutor.* **2015**, *18*, 924–948.
17. Cook, C.; Marsh, H. An introduction to spread spectrum. *IEEE Commun. Mag.* **1983**, *21*, 8–16. [CrossRef]
18. Gao, J.; Zhang, Y.; Liu, Y. A novel diversity receiver design for cooperative transmission system. *IEEE Access* **2018**, *6*, 27176–27182. [CrossRef]
19. Moulika, V.; Bhagyalakshmi, L. Performance Investigation of Cooperative Diversity Techniques for 5G Wireless Networks. In Proceedings of the 2019 IEEE 1st International Conference on Energy, Systems and Information Processing (ICESIP), Chennai, India, 4–6 July 2019.
20. Hennessy, L.J.; Patterson, D.A. *Computer Architecture: A Quantitative Approach*; Elsevier: Amsterdam, The Netherlands, 2011.
21. Russell, T. *Signaling System # 7*; McGraw-Hill: New York, NY, USA, 2002; Volume 2.
22. Modarressi, A.R.; Ronald, A.S. Signaling system no. 7: A tutorial. *IEEE Commun. Mag.* **1990**, *28*, 19–20. [CrossRef]
23. Shankar, K.S. Special feature the total computer security problem: An oveview. *Computer* **1977**, *10*, 50–73. [CrossRef]
24. Archana, B.S.; Chandrashekar, A.; Bangi, A.G.; Sanjana, B.M.; Akram, S. Survey on usable and secure two-factor authentication. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017.
25. Ciriani, V.; Vimercati, S.D.C.D.; Foresti, S.; Jajodia, S.; Paraboschi, S.; Samarati, P. Combining fragmentation and encryption to protect privacy in data storage. *ACM Trans. Inf. Syst. Secur. (TISSEC)* **2010**, *13*, 1–33. [CrossRef]
26. Feng, L.; Zhang, Y.; Li, H. Large file transmission using self-adaptive data fragmentation in opportunistic networks. In Proceedings of the 2015 Fifth International Conference on Communication Systems and Network Technologies, Gwalior, India, 4–6 April 2015.
27. Mikko, P.; Keranen, A.; Ott, J. Message fragmentation in opportunistic DTNs. In Proceedings of the 2008 International Symposium on a World of Wireless, Mobile and Multimedia Networks, Newport Beach, CA, USA, 23–26 June 2008.
28. Wampler, J.A.; Chien, H.; Andrew, T. Efficient distribution of fragmented sensor data for obfuscation. In Proceedings of the MILCOM 2017—2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, USA, 23–25 October 2017.
29. Abdel-Rahman, M.J.; Shankar, H.K.; Krunz, M. QoS-aware parallel sensing/probing architecture and adaptive cross-layer protocol design for opportunistic networks. *IEEE Trans. Veh. Technol.* **2015**, *65*, 2231–2242. [CrossRef]
30. Pohly, D.J.; Patrick, M. Modeling Privacy and Tradeoffs in Multichannel Secret Sharing Protocols. In Proceedings of the 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Toulouse, France, 28 June–1 July 2016.
31. Desmedt, Y.; Wang, Y. Perfectly secure message transmission revisited. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2002.

32. Srinathan, K.; Arvind, N.; Pandu, C.R. Optimal perfectly secure message transmission. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 2004.
33. Hudic, A.; Islam, S.; Kieseberg, P.; Rennert, S.; Weippl, E.R. Data confidentiality using fragmentation in cloud computing. *Int. J. Commun. Netw. Distrib. Syst.* **2012**, *1*, 1. [CrossRef]
34. Sweet, I.; Trilla, J.M.C.; Scherrer, C.; Hicks, M.; Magill, S. What's the Over/Under? Probabilistic Bounds on Information Leakage. In *International Conference on Principles of Security and Trust*; Springer: Cham, Switzerland, 2018.