Communications Network Utility as a Function of Node Entropy

Jason Q. McClintic*, Murali Tummala†, John McEachen†, James Scrofani†

* Ship Repair Facility–Japan Regional Maintenance Center Detachment Sasebo
United States Navy
Sasebo, Kyushu, Japan
† Department of Electrical and Computer Engineering
Graduate School of Engineering and Applied Science
Naval Postgraduate School
Monterey, CA 93943
Email: jason.mcclintic@srf.navy.mil, mtummala@nps.edu, mceachen@nps.edu, jwscrofa@nps.edu

Abstract—Communications networks are valuable in proportion to the trustworthy information they carry. Network security policies are designed to classify nodes as trustworthy or not with some probability of error when the true status of each node is unknown. By making an analogy with the binary symmetric channel model, properties of networks with optimal security policies are derived. Additive and multiplicative utility models with and without aversion to misclassification risk are considered.

Index Terms—network security, optimization, access control

I. INTRODUCTION

Communication networks are a ubiquitous feature of human society. Modern web-based social networks claim millions of users and allow connections between individuals at their discretion [1]. Such networks present problems ranging from optimal security investments [2] to access control [3] to resource allocation [4]. One commonality is that they all address the idea of trust.

Trust is an ambiguous concept. It has many definitions across different fields depending on the exact problem at hand [1], [3], [4], and [5]. The definitions used in [2] and [4] are very different. We propose the following definition: users are untrustworthy if and only if any positive allocation of resources (entropy or access thereto) is detrimental to the value of the overall network. For example, the value of an internal corporate research network is lessened if a corporate spy is inadvertently given access thereto.

This paper is related to several existing threads of literature. Fouad et al. present two models of the risk and utility of a social network such that risk is defined in terms of leakage of information outside the user’s group of friends [1]. They point out that it is critical for models to incorporate both the risks and rewards of participation in a social network as only considering risk implies we should never participate, a conclusion which is wrong on its face. Likewise, we present models that incorporate both risk and utility. Unlike [1], we abstract away from considering specific kinds of information or levels of granularity by considering entropy allocations. Ma et al. propose a formal model of using trust for access control in which the trustworthiness of each node ranges between zero and one. They then make risk decisions based on those trust values for a variety of purposes [6]. We propose a model analogous to the binary symmetric channel in which the security policy makes a decision about the trustworthiness of each node with some probability of misclassification. This is also similar to the way in which the methods presented in [1] make recommendations about whether or not a particular prospective friend is trustworthy. Like [2], we are concerned with optimal security investments in security. We differ in that our analysis is based in classical optimization vice game theory.
theory and that we characterize the outcome of an optimal investment in terms of misclassification probabilities. Nin and Torra proposed a method for aggregating trust information from many users to make access decisions [3]. Our problem is likewise tied to access control; however, we solve for overall levels of network access ranging from zero (user is denied access) to potentially unlimited access to information vice trying to make a yes/no access decision for a specific resource. This paper also differs from the existing literature by utilizing the concept of relative risk aversion from economics [7].

While the problem considered here is presented in a framework of social networks, it is easily adapted to a wide variety of scenarios. For example, the nodes could be autonomous wireless sensors subject to unknown degradation. In such a scenario, the idea of trust is tied up in whether or not the information from the node is believed to be accurate to some specified standard. Another example is that the computers on a LAN may be infected with malware which can spread through the network or be used to extract information from the network by a malicious user. Trust then reflects the belief that a computer is not infected.

The objective of this paper is to formulate models of network utility and risk in order to analyze their properties when access control schemes are optimal. To this end, we propose a simple model of the action of a trust-based security scheme and four models of network utility. For each utility model, its properties and the misclassification probability of the optimal security policy are derived. In addition, we derive the optimal entropy allocation.

The model of node trustworthiness and security policy action is presented in Section II. Results in utility-maximizing networks are presented in Section IV. Section V discusses the results. Section VI concludes the paper.

II. NODE TRUSTWORTHINESS AND SECURITY POLICY

In the most basic formulation, each node is trustworthy or untrustworthy according to a draw from the Bernoulli random variable $T$. This information is unknown to the network and must be estimated by the black-box mechanisms of the network security policy. Nin et al would term this a reputation model [3] and this differs from [1] in that it is a network-vice user-level model. The action of network security policy is like that of a binary symmetric channel in that it maps the true value of $T$ for each node to an estimated value with some probability of misclassification. A diagram of this model is shown in Fig. 1. The Bernoulli random variable $T$ is one when the node is trustworthy and zero otherwise. The variable $\hat{T}$ is the estimate of whether or not the node is trustworthy. For convenience, define the events $A = (\hat{T} = 1 \cap T = 1)$, $B = (\hat{T} = 1 \cap T = 0)$, $C = (\hat{T} = 0 \cap T = 1)$, and $D = (\hat{T} = 0 \cap T = 0)$. By construction, these are both Bernoulli random variables. Likewise, $A_i$, $B_i$, $C_i$, and $D_i$ are the corresponding events for the node specified by the subscript.

An alternative model to account for the loss associated with allocating entropy to a node by incorporating the idea of risk aversion [7]. Risk aversion is when the expected utility of a node is penalized as a function of its trustworthiness. One such model is the constant relative risk aversion model in which the utility $u(c)$ is given by

$$u(c) = \frac{c^{1-R}}{1-R}$$

(1)

where $R = 1/a$ and $c$ is the entropy. An example of this for a node with unit entropy allocation is shown in Fig. 2 with $R = 1/2$. The horizontal axis is the actual entropy for perfectly trustworthy nodes or the expected value of the entropy multiplied by the trustworthiness variable. It may be seen in Fig. 2 that in a risk averse network, the utility of a possibly trustworthy node is equal to that of a known trustworthy node with a lower entropy allocation. We may then express the utility of a
node trustworthy with probability $t$ in terms of the entropy of a known trustworthy node with the same utility. This may be done by setting (1) equal to $tE_i$ for $c$. This yields the equation

$$c = [E_i t(1 - R)]^{1/(1-R)}.$$

(2)

It should be noted that this approach is only applicable when $R < 1$. A plot of (2) with $R = 0.5$ is shown in Fig. 3. It is useful to note that

$$\frac{dc}{dE_i} = t^{1/(1-R)}[(1 - R)E_i]^{R/(1-R)}.$$

(3)

### III. NETWORK UTILITY MODEL

The utility of a network is determined by which nodes are included and we assume only nodes determined to be trustworthy are included in the network. Therefore, the utility of the network is given by

$$U = f(U_1, U_2, \ldots, U_N)$$

(4)

where each $U_i$ is the utility of the $i$th node of the network. Choose to express $U_i$ as a function of two additional terms, the entropy $E_i \geq 0$ node $i$ contributes to the network and a penalty $L_i \geq 0$ which may be chosen to be a function of $E_i$. The entropy and corresponding utility is accrued if the node is trustworthy and included in the network (event $A$). The penalty is accrued if the node is untrustworthy and included in the network (event $B$). The penalty is chosen to be positive in order to clarify the analysis. Should a trustworthy node be misclassified (event $C$), then no entropy is allocated and the utility is zero. If an untrustworthy node is correctly classified (event $D$), then no entropy is allocated and there is no utility. There are a variety of utility models from which to choose [1], [3], [4], [7]. Four are considered in this paper, the simple linear model, the linear model with risk aversion, the multiplicative model, and the multiplicative model with risk aversion.

#### A. Simple Linear Utility Model

The simple linear utility model gives the utility of the network as

$$U = \sum_{i=1}^{N} A_i E_i - L_i(E_i)B_i$$

(5)

such that

$$L_i = \frac{dL_i}{dE_i}E_i.$$

(6)
When choosing $L_i$ to be a function of $E_i$, then $\partial L_i/\partial E_i$ is the sensitivity of the penalty with respect to the entropy allocation. This work chooses to assume that the slope will be positive because including untrustworthy nodes is generally unacceptable (reducing the utility of the network) and large because of risk aversion.

As the utility function is linear, the expected utility function may be computed term by term. The expected utility of the $i$th node in the network is given by

$$ U_i = E_i \Pr(\hat{T}_i = 1 \cap T_i = 1) - L_i \Pr(\hat{T}_i = 1 \cap T_i = 0). \quad (7) $$

This may be rewritten as

$$ U_i = E_i \Pr(\hat{T}_i = 1|T_i = 1)\Pr(T_i = 1) - L_i \Pr(\hat{T}_i = 1|T_i = 0)\Pr(T_i = 0) \quad (8) $$

Computing the probabilities yields

$$ U_i = E_i(1-p)t - L_i p(1-t) \quad (9) $$

where $E\{T_i\} = t = \Pr(T_i = 1)$. Therefore, the expected utility of the network is given by

$$ \bar{U} = \sum_{i=1}^{N} E_i(1-p)t - L_i E_i p(1-t). \quad (10) $$

### B. Linear Model with Risk Aversion

In order to incorporate risk aversion into the linear model, choose to compute the utility of the network as

$$ U_{CRRA} = \sum_{i=1}^{N} \phi(E_i A_i) - L_i (E_i) B_i \quad (11) $$

where $E[\phi(X)] = c(E[X])$ for any random variable $X$. Taking the expected value yields (see appendix)

$$ \bar{U}_{CRRA} = \sum_{i=1}^{N} c(E_i(1-p)t) - L_i(E_i)p(1-t) \quad (12) $$

### C. Multiplicative Model

While the linear model with risk aversion is an improvement over the more basic version, it does not recognize any kind of network externality. Network externalities are additional, synergistic gains in value the network accrues as it grows. In order to try to capture these effects, a multiplicative model may be employed. As the situation is symmetric for an attacker, the loss term must also have a multiplicative form. These considerations yield the utility equation

$$ U_M = \prod_{i=1}^{N} E_i A_i - \prod_{i=1}^{N} L_i(E_i) B_i \quad (13) $$

whose expected value is given by

$$ \bar{U}_M = (1-p)^N t^N \prod_{i=1}^{N} E_i - (1-t)^N p^N \prod_{i=1}^{N} L_i(E_i) B_i. \quad (14) $$

### D. Multiplicative Model with Constant Relative Risk Aversion

Like the basic linear model, the multiplicative model may be extended by incorporating risk aversion. Recalling the definition of $\phi(\cdot)$, the utility function may be written as

$$ U_{CRRA,M} = \prod_{i=1}^{N} \phi(E_i A_i) - \prod_{i=1}^{N} L_i(E_i) B_i. \quad (15) $$

Taking the expectation of $U_{CRRA,M}$ yields

$$ \bar{U}_{CRRA,M} = \prod_{i=1}^{N} c(E_i(1-p)t) - \prod_{i=1}^{N} L_i(E_i)p(1-t) \quad (16) $$

as $\{A_i\}$ and $\{B_i\}$ are sets of independent random variables by hypothesis.

### IV. Properties of Utility-Optimizing Networks

The properties of an optimal network vary depending on the structure of the optimization problem. Various properties of interest may be derived from the constrained or unconstrained optimization problem.

#### A. Linear Utility with Linear Loss

The optimization problem for the optimal security policy is to choose the size of $E_i$ for each $i$ such that
the expected value of (10) is maximized. Taking the partial derivative of $\bar{U}$ with respect to $E_i$ gives

$$\frac{\partial \bar{U}}{\partial E_i} = (1 - p) t - \frac{\partial L_i}{\partial E_i} (1 - t) p(1 - t) = 0. \quad (17)$$

Solving for the value of $p$ at the optimum yields

$$p = \frac{t}{t + \frac{\partial L_i}{\partial E_i} - \frac{\partial L_i}{\partial E_i} t_{r,i}} \quad \frac{1}{1 + \frac{\partial L_i}{\partial E_i} t_{r,i}} \quad (18)$$

where $t_{r,i} = (1 - t)/t$. As the nodes are assumed to be identically distributed, this simplifies to

$$p = \frac{1}{1 + \frac{\partial L_i}{\partial E_i} t_{r,i}} \quad (19)$$

When $t_r$ is high, then the nodes in the class are unlikely to be trustworthy. A plot of the optimal misclassification probability is shown in Fig. 4. When nodes are likely to be trustworthy ($t_r$ is small) and the loss sensitivity is small, then the optimal probability of misclassification becomes large. Conversely, when the loss sensitivity is high and nodes tend to be untrustworthy, the optimal misclassification probability becomes very small.

B. Constant Relative Risk Aversion with Linear Loss

Taking the partial derivative of (12) gives

$$\frac{\partial \bar{U}}{\partial E_i} = \exp \left\{ \ln \left[ E_i (1 - p) t \right] + \ln (1 - R) \right\} \frac{1}{1 - R} \cdot \left( \frac{1}{E_i(1 - R)} - \frac{\partial L_i(E_i)}{\partial E_i} p(1 - t) \right) = 0 \quad (20)$$

at the unconstrained optimum. Solving this equation for $E_i$ yields

$$E_i = \left[ \frac{\partial L_i(E_i)}{\partial E_i} (1 - t) p \right]^{(1 - R)/R} \quad [((1 - p)t)^{1/R}(1 - R)] \quad (21)$$

Contour plots of the optimal $E_i$ value as a function of $t$ and $p$ given $\partial L_i/\partial E_i = 1$ and $R \in \{0.25, 0.75\}$ are shown in Figures 5 and 6.

Solving (20) equation for $p$ yields

$$\ln \left[ \frac{1 - p}{p^{(1 - R)}} \right] = (1 - R) \ln \left( \frac{\exp \left\{ \ln (1 - R) \right\}}{1 - R} \right. \cdot \frac{\partial L_i}{\partial E_i} \left. \cdot t_{r,i} \right) \quad (22)$$
Figure 6. Contour plot of the unconstrained optimal $E_i$ given $R = 0.75$ and $\partial L_i/\partial E_i = 1$ as a function of node trustworthiness and misclassification probability.

Figure 7. Contour plot of the unconstrained optimal $p$ given $R = 0.25$ as a function of node trustworthiness and loss sensitivity.

Figure 8. Contour plot of the unconstrained optimal $p$ given $R = 0.75$ as a function of node trustworthiness and loss sensitivity.

C. Multiplicative Model

First note the derivative of (14) is
where \( \{N\}/i \) is the set of integers 1, 2, \ldots, \( N \) with \( i \) removed. At the optimum, this implies

\[
(1 - p)^N \prod_{\{N\}/i} E_j - (1 - t)^N p^N \frac{\partial L_i(E_i)}{\partial E_i} \prod_{\{N\}/i} L_j(E_j) = 0
\]

which implies

\[
p = \frac{1}{1 + t_r \alpha^{(N-1)/N} \left[ \prod_{j=1}^{N} \frac{\partial L_i(E_j)}{\partial E_j} \right]^{1/N}}.
\]

This is very similar to the result for the basic linear model.

**D. Multiplicative Model with Constant Relative Risk Aversion**

The derivative of (16) is

\[
\frac{\partial U_{CRRA,M}}{\partial E_i} = t^{1/(1-R)} [(1 - R) E_i]^{R/(1-R)} \cdot \prod_{j \in \{N\}/i} \left[ \frac{[E_j(1 - p)t]^{1-R}}{1 - R} \right] - \frac{\partial L_i(E_i)}{\partial E_i} \prod_{j \in \{N\}/i} L_j(E_j) p(1 - t) = 0
\]

at the optimum. Proceeding similarly to IV-C, taking ratios yields

\[
\left( \frac{E_i}{E_k} \right)^{1-R} \left( \frac{E_k}{E_i} \right)^{1-R} = \left( \frac{\partial L_i/\partial E_i}{\partial L_k/\partial E_k} \right) \left( \frac{L_k}{L_i} \right)
\]

which simplifies to

\[
\left( \frac{E_k}{E_i} \right)^{1-3R+R^2} = \left( \frac{\partial L_i/\partial E_i}{\partial L_k/\partial E_k} \right) \left( \frac{L_k}{L_i} \right).
\]

This implies

\[
\frac{\partial L_i(E_i)}{\partial E_i} = \frac{L_i(E_i)}{\alpha E_i^{1-3R+R^2}(1-R)}
\]

where \( \alpha \) is a constant of proportionality. As expected, when \( R = 0 \), the corresponding result for the non-CRRA case discussed in IV-C is obtained. Recognizing (35) is a separable differential equation, the behavior of the loss function near the optimum is given by

\[
L_i(E_i) = \begin{cases} 
C_i E_i^{1/\alpha} & R = 0 \\
C_i \exp \left\{ \frac{1-R}{\alpha(2R-R^2)} E_i^{(2R-R^2)/(1-R)} \right\} & R \neq 0
\end{cases}
\]

where \( C_i \) is the constant of integration.
V. DISCUSSION

The analogy between a binary symmetric channel and the action of a security policy in making hard decisions about which nodes to trust is very strong. This is because real network security policies as embodied by their security mechanisms must make a hard decision to accept or reject packets from a node on the basis of the associated trust decision. Black- and white-lists are simple examples of security policies that act in this way.

The basic linear model suggests a counterintuitive result; to wit, that the security policy which maximizes the expected utility of a network can have an arbitrarily large probability of misclassification. This will only occur when nodes are overwhelmingly likely to be trustworthy and the sensitivity of the loss term to the size of the entropy allocation is small.

The linear constant relative risk aversion model is a generalization of the basic linear model. This modification penalizes classes of nodes that are in general less trustworthy. This is especially useful when the network may allocate capacity across multiple classes of nodes. By inspection, if the risk aversion coefficient \( R = 0 \), then the original linear model is obtained.

A standard example of a network such that its value grows faster as it becomes larger is a social network. Capturing this kind of behavior is the goal of the multiplicative model.

All of the models are formulated with normalized units of entropy; therefore, all of the results are also in terms of the normalized entropy unit. Consequently, all of the results are as applicable to networks where the basic unit of information capacity is bits as it is to a network where the basic unit is bytes.

VI. CONCLUSION

Systems for trust-based access control are actively researched. This paper proposed a simple model of the action of an access control system which is analogous to the binary symmetric channel model. Using this model as a starting point, the properties of four different network utility models are derived. The results show that the probability a user is trustworthy, the sensitivity to loss, and the degree of risk aversion have significant impacts on the optimal misclassification probability and the size of the entropy allocation.

APPENDIX

A. The Partial Derivative of \( \bar{U}_{CRRA} \) with respect to \( E_i \)

The derivative of (12) may be computed as follows:

\[
\frac{\partial \bar{U}_{CRRA}}{\partial E_i} = \frac{\partial}{\partial E_i} c(E_i(1 - p)t) - \frac{\partial}{\partial E_i} L_i(E_i)(1 - t)p = \frac{\partial}{\partial E_i} [E_i(1 - p)t(1 - R)]^{1/(1 - R)} - \frac{\partial L_i(E_i)}{\partial E_i}(1 - t)p = \frac{[(1 - p)t(1 - R)]^{1/(1 - R)}}{1 - R} E_i^{1 - R - 1} - \frac{\partial L_i(E_i)}{\partial E_i}(1 - t)p = \frac{[(1 - p)t(1 - R)]^{1/(1 - R)}}{1 - R} E_i^{R/(1 - R)} - \frac{\partial L_i(E_i)}{\partial E_i}(1 - t)p.
\] (37)

B. Computation of the Optimal Entropy Allocation Scheme for the Linear CRRA Model

The value-maximizing \( E_i \) may be computed as

\[
\frac{[(1 - p)t(1 - R)]^{1/(1 - R)}}{1 - R} E_i^{R/(1 - R)} = \frac{\partial L_i(E_i)}{\partial E_i}(1 - t)p \Rightarrow E_i^{R/(1 - R)} = \frac{\partial L_i(E_i)}{\partial E_i}(1 - t)p(1 - R) \Rightarrow E_i = \left[ \frac{\partial L_i(E_i)}{\partial E_i}(1 - t)p \right]^{(1 - R)/R} \left\{ \frac{1}{[(1 - p)t]^{1/(1 - R)(1 - R)^{R/(1 - R)}}} \right\}^{1 - R/R}.
\]
so long as $R \in (0, 1)$.

C. Computation of the Optimal Misclassification Probability for the Linear CRRA Model

In addition, (22) may be computed as follows:

\[
\begin{align*}
\exp \left\{ \ln \left[ \frac{E_i(1-p)}{1-R} \right] \right\} & \exp \left\{ \ln \left[ \frac{1-R}{1-R} \right] \right\} \\
= \frac{\partial L_i}{\partial E_i} E_i(1-t)p(1-R) \\
\Rightarrow \exp \left\{ \frac{\ln(1-p)}{1-R} \right\} & \exp \left\{ \frac{\ln E_i t}{1-R} \right\} \\
= \frac{\partial L_i}{\partial E_i} E_i(1-t)p(1-R) \\
\Rightarrow \frac{\ln(1-p)}{1-R} + \ln E_i t \\
= \ln \left( \frac{\partial L_i}{\partial E_i} E_i(1-t)(1-R) \right) & + \ln p \\
\Rightarrow \frac{\ln(1-p)}{1-R} - \ln p \\
= \ln \left( \frac{\partial L_i}{\partial E_i} E_i(1-t)(1-R) \right) & - \ln E_i t \\
\Rightarrow \ln(1-p) - (1-R) \ln p = \ln \left( \frac{1-p}{p^{1-R}} \right) \\
= (1-R) \ln \left( \frac{\partial L_i}{\partial E_i} (1-t)(1-R) \right) & t \exp \left\{ \frac{\ln(1-R)}{1-R} \right\} \\
= (1-p) \ln \left( \frac{\partial L_i}{\partial E_i} (1-t)(1-0) \right) & t \exp \left\{ \frac{\ln(1-0)}{1-0} \right\} \\
\Rightarrow \ln \left( \frac{1-p}{p} \right) = \ln \left( \frac{\partial L_i}{\partial E_i} (1-t) \right) \\
\Rightarrow \frac{1-p}{p} = \frac{\partial L_i}{\partial E_i} (1-t) \\
\Rightarrow (1-p)t = \frac{\partial L_i}{\partial E_i} (1-t)p \\
\Rightarrow t - pt = \frac{\partial L_i}{\partial E_i} (1-t)p \\
\Rightarrow \left[ t + \frac{\partial L_i}{\partial E_i} (1-t) \right] p = t \\
\Rightarrow p = \frac{t}{t + \frac{\partial L_i}{\partial E_i} (1-t)} = \frac{1}{1 + \frac{\partial L_i}{\partial E_i} \frac{1-t}{t}}
\end{align*}
\]

D. Proof the Linear Model is a Special Case of the Linear CRRA Model

Setting $R = 0$ in (22) reduces it to (19) as

\[
\ln \left( \frac{1-p}{p^{1-0}} \right)
\]

REFERENCES


