Cyber Deception against Adversarial Traffic Analysis in wireless Networks

1 Motivation

Security is an essential service for wired and wireless network communications due to their open-medium nature which allows malicious actors to eavesdrop or manipulate the traffic. Cryptographic solutions, such as or WPA2 and CCMP for Wireless LANs and 3GPP for 5G Cellular communications, are widely used to preserve confidentiality and integrity of communications.

However, while encryption prohibits attackers from accessing the plain data in wireless communications, it does not protect them from passive traffic analysis attacks that rely on the (a) packet sizes, (b) packet counts, (c) flow rates, or (d) packet timing (inter-arrivals) to infer sensitive information from eavesdropped communication patterns, no matter if encrypted. These features are not changed via encryption, thus enabling adversaries to classify and characterize the encrypted traffic through statistical or machine-learning-based techniques. For example, Sun [**?**] identified web pages within SSL-encrypted connections by examining the sizes of the HTML objects returned in the HTTP response. Liberatore and Levine [**?**] showed that a similar attack is still possible, with some modifications, for HTTP traffic that uses persistent connections or that is tunneled through SSH port forwarding. Wright [**?**] showed that the statistical distribution of packet sizes in encrypted Voice over IP (VoIP) connections can be used to identify the language spoken in a conversation when the voice stream is encoded using certain kinds of variable bit rate compression schemes. Work by Saponas [**?**] showed that variable bit rate encoders for streaming video leak information in a similar fashion, allowing an observer in the network to identify movies within encrypted connections.

Several solutions based on traffic reshaping have been proposed in the literature. A straightforward solution is eliminating any identifiable pattern in traffic through quantization []. For example, by padding packets to the size of maximum transmission unit (MTU), one can defeat traffic analysis techniques that rely on packet sizes for traffic characterization []. However, padding comes at the cost of degrading the efficiency and performance of the underlying network protocols. Thus, such excessive padding is simply not a satisfactory solution to the problem. As another example of quantization, to defeat traffic analysis attacks based on packet timing and inter-arrival distribution, the transmitters can intentionally delay transmission of certain packets. However, these delays would significantly degrade network throughput and thus are not very practical.

Traffic morphing by Wright [] morphs a given source distribution to a given destination distribution, through traffic manipulation. A proxy pads the packets or breaks them into smaller sizes to match the source traffic distribution to the destination one.

In this proposed research, we propose a novel out-of-box methodology for protecting wireless networks against passive traffic analysis by proactive, effective, and efficient obfuscation of wireless traffic: (1) efficient and adversary-aware route randomization to confuse attacker's about where to eavesdrop, and (2) robust obfuscation of real traffic by intelligent and efficient injection of deceptive (fake) frames.

2 Initial Results: Formulation for Single-Unicast Networks

Consider a single-unicast wireless network $G = (V, E)$ with $s, t \in V$. Let $\mathcal{P} = \{p_1, p_2, ...\}$ be the set of all s-t paths on G. Assume that all the paths are disjoint and orthogonal. Let r_i denote the transmission rate of path p_i. Accordingly, let $R = \sum_i r_i$ be the aggregate rate that could be guaranteed between s and t.

Suppose S denotes the minimum required rate, where $S < R$. Our objective is to determine $k_i \leq r_i$ for each path p_i as the rate dedicated to transmission of real (non-deceptive) traffic on the path, such that $(\sum_i k_i) \geq S$. We also denote by $f_i = r_i - k_i$ the rate of deceptive traffic on path p_i.

Assume $\beta_i = \frac{f_i}{k_i}$ defines the ratio of deceptive over real traffic on path p_i. We model the problem as a static game of complete and perfect (no adversary types) information, as follows:

- Players: $P = \{d(efender), a(dversary)\}$.
- Defender's pure strategies: strategies of the form $\{[k_1, k_2, \ldots]\}$ s.t $\forall i : k_i \leq r_i$.
- Adversary's pure strategies: $S_a = \{p_1, p_2, \ldots\}$. Assumption here is that adversary will attack only one path.

- Adversary's utility function: the threat model is eavesdropping for traffic analysis. By attacking path p_i, attacker will capture real traffic with rate k_i, but will also capture f_i which is the deceptive traffic rate. We assume that the adversary's payoff is linear w.r.t both real and fake traffic rates:

$$U_a([k_1, k_2, \ldots], p_j) = \max((1 - \beta_j^n) \cdot k_j, 0), \forall i : k_i \leq r_i \wedge \sum_i k_i = S \tag{1}$$

  For example, if $n = 1$ the attacker's utility will be $\max(k_j - f_j, 0)$ which means that the deceptive traffic rate has linearly affects (deteriorates) the accuracy of the traffic analysis. When $n = 2$, the effect of fake traffic on adversarial traffic analysis increases quadratically. In this utility function, regardless of the value of n, when half of captured traffic is fake ($x_j = k_j$), the adversary can not deduce any useful information from the analysis, so adversary's payoff is 0. A justification for this is that the statistical analysis aims to derive statistical estimators (mean, deviation, median) from the data (traffic). The breakdown point of an estimator is the proportion of incorrect observations (e.g. arbitrarily large observations) an estimator can handle before giving an incorrect (e.g., arbitrarily large) result. Breakdown point of an estimator cannot exceed 50% because if more than half of the observations are contaminated, it is not possible to distinguish between the underlying distribution and the contaminating distribution [**?**]. For example, median has a breakdown point of 50%.

  We also assume that U_a is never negative. Intuitively, this means if rate of fake rate is larger than real ($f_i > k_i$) it has no security harm (benefit) for attacker (defender). The game could still be zero-sum.

- Defender's utility function: Defender would lose k_j if adversary attacks p_j, but the noise on the path will complicate the traffic analysis for adversary:

$$U_d([k_1, k_2, \ldots], p_j) = \min((\beta_j^n - 1) \cdot k_j, 0) \tag{2}$$

$$\forall i : k_i \leq r_i \wedge \sum_i k_i = S \tag{3}$$

We define the game as a zero-sum two-person static game. Assuming that vectors $\mathbf{x}$ and $\mathbf{y}$ denote defender and attacker's optimal mixed strategies in the equilibrium respectively, the attacker's payoff, V, is calculated as follows:

$$V = \sum_i \sum_j x_i \cdot y_j \cdot U_a(i, j) \tag{4}$$

The optimal value of n must be derived by understanding the effect of fake traffic on various traffic analysis techniques.

Figure 1 quantifies the effect of fake traffic on median. Figure shows a linear correlation between β_i as the ratio of fake over real traffic, and probability that median is changed as a result of injecting the fake packets. The y-axis essentially shows (1 - attacker's utility). Therefore, $n = 1$ is a good estimator for quantifying this effect.

2.1 Example

Assume p_1, p_2, p_3 are the paths, and $\boldsymbol{r} = [3, 2, 5]$. Also assume required rate $S = 6$. Goal is to determine $\boldsymbol{k}$ where k_i denotes rate of real traffic assigned to path p_i. We also assume that $f_i = r_i - k_i$.

Since the problem is a zero-sum two-person game, it can be solved based on the Minimax and Duality Theorem, and using linear programming. We can use Matlab as discussed in [**?**] to solve the problem.

Defender's optimal strategy is to use $[1.5, 1, 3.5]$ for 33.33%, $[1.5, 2, 2.5]$ for 33% and strategy $[2.5, 1, 2.5]$ for 33%. Also, attacker's optimal strategy is to attack path p_1 for 33% of the time, path p_2 for 33% and attack p_3 for 33% of the time. The attacker's payoff in this case is $V = 0.666$ which shows attacker's gain in equilibrium.

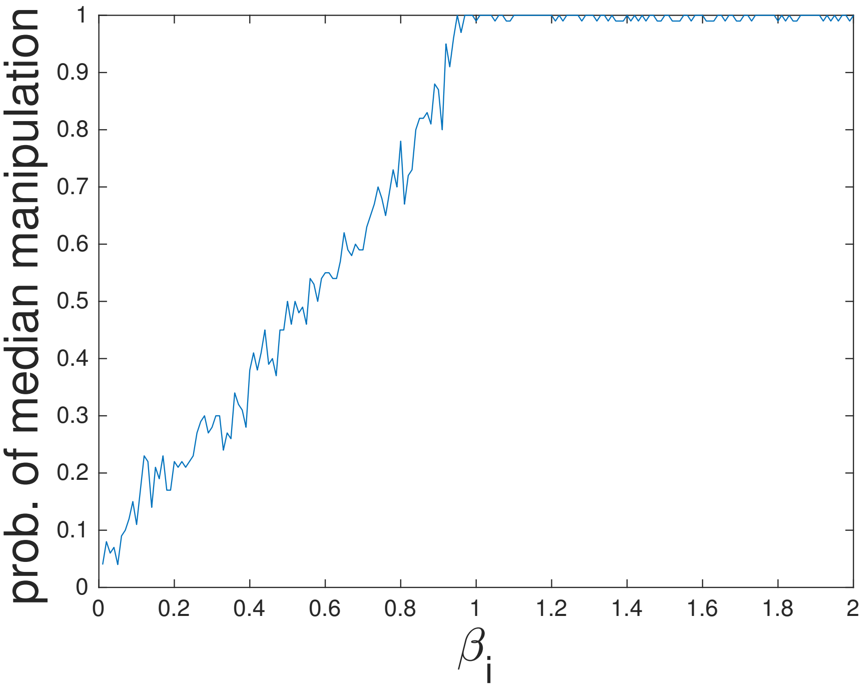

Figure 1: Median manipulation probability for different fake/real traffic ratios

3 Solving game over continuous strategies

Let's focus on the case where $U_a([k_1,...,k_n],p_j) = (k_j - x_j)^+ = (2k_j - r_j)^+$. Suppose the defender can choose any strategy $k = (k_1,...,k_n)$ with $k \geq 0$ and $\sum k_i = S$. The defender wants to solve the problem

$$\begin{aligned} \min_{k_1,...,k_n} \ \max_{j} \quad & (2k_j - r_j)^+ \\ \text{s.t.} \quad & 0 \leq k_j \leq r_j, \quad j = 1,...,n \\ & \sum k_i = S. \end{aligned}$$

As it turns out, the solution to this problem can be seen as a type of water-filling. As illustrated in Figure 2, we have n columns, each with height r_i, $i = 1,...,n$, all of them placed so that their middle points $(r_i/2)$ are aligned. An S amount of water is dropped into this container, and the resulting level in each column is the optimal value of k_i.

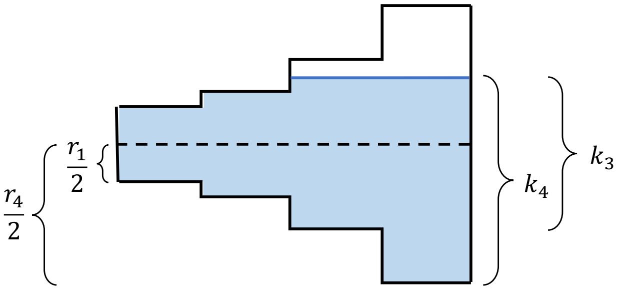

Figure 2: Water-filling solution to find k_1, k_2, k_3, k_4

In order to show that this approach yields the optimal solution, we convert the optimization problem into a linear program and then use KKT conditions. Let $R = \sum r_i$. If $S \leq R/2$, the water level will be below $r_i/2$ in each column, and a payoff of 0 is guaranteed. So we focus on the case where $S > R/2$. Notice that, for a feasible $(k_1,...,k_n)$, if $k_\ell < r_\ell/2$ and $k_i > r_i/2$, it is possible to increase k_ℓ and decrease k_i, and $\max_j (2k_j - r_j)^+$ can only go down. Hence, we can focus on the case where $k_j \geq r_j/2$ for $j = 1, ..., n$. We can then define $\tilde{k}_j = k_j - r_j/2$ and rewrite the problem above as

$$\begin{aligned} \min_{\tilde{k}_1,...,\tilde{k}_n} \quad \max_j \quad & \tilde{k}_j \\ \text{s.t.} \quad & \tilde{k}_j \leq r_j/2, \quad j = 1, ..., n \\ & \sum \tilde{k}_i = S - R/2. \end{aligned}$$

This is equivalent to the linear program

$$\begin{aligned} \min_{\tilde{k}_1,...,\tilde{k}_n,v} \quad & v \\ \text{s.t.} \quad & \tilde{k}_j \leq v, \quad j = 1, ..., n \\ & \tilde{k}_j \leq r_j/2, \quad j = 1, ..., n \\ & \sum \tilde{k}_i = S - R/2. \end{aligned}$$

The Lagrangian for this problem is given by

$$L(v, \tilde{k}, \lambda, \mu, \xi) = v + \sum_{j=1}^{n} \lambda_j (\tilde{k}_j - v) + \sum_{j=1}^{n} \mu_j (\tilde{k}_j - r_j/2) + \xi \left(\sum_{j=1}^{n} \tilde{k}_j - S + R/2 \right).$$

The KKT conditions for optimality require that

$$\begin{aligned} \frac{\partial L}{\partial \tilde{k}_j} &= \lambda_j + \mu_j + \xi = 0 \\ \frac{\partial L}{\partial v} &= 1 - \sum \lambda_j = 0 \end{aligned}$$

Since $\lambda_j, \mu_j \geq 0$, we must have $\xi < 0$. From complementary slackness, we know that for each j for which $\tilde{k}_j < r_j/2$, $\mu_j = 0$. Hence, for each j with $\tilde{k}_j < r_j/2$ (i.e., where $k_i < r_i$), $\lambda_j = -\xi > 0$, and the corresponding constraint $\tilde{k}_j \leq v$ must be met with equality. We conclude that, if we assume wlog that $r_1 \leq r_2 \leq ... \leq r_n$, the solution must have

$$\begin{aligned} \tilde{k}_i &= r_i/2, \quad \text{for } i = 1, ..., t \\ \tilde{k}_i &= v, \quad \text{for } i = t + 1, ..., n, \end{aligned}$$

for some t. This is the water-filling solution described above.

4 Proposed Research