Toward Deceptive and Agile Wireless Infrastructures against Adversarial Traffic Analysis Attacks

Haadi Jafarian, Ilan Shomorony, Alireza Vahid

Technical Report, September 2019

1 Introduction

While more robust security models 3GPP 5G security architecture [1, 29] provide a variety of cryptographic systems for ensuring confidentiality, integrity and authenticity of wireless communications, they are not sufficient to address traffic analysis attacks. In fact, network traffic has been long used to infer network internal characteristics [6–8, 12, 13, 16, 30]. There are also ever-growing side-channel attacks that rely on sophisticated machine learning algorithms to classify the encrypted packets based on unencryptable features of the traffic, such as packet sizes and counts, flow rates, and timing (inter-arrival times), to infer sensitive information from eavesdropped wireless communications. Examples include traffic analysis attacks that succeed to identify the language spoken or even the speaker in a conversation over an encrypted VoIP traffic [22, 33, 35, 37], to identify web pages or other user activities from encrypted packets [2, 4, 5, 25, 27, 28, 34, 42], or to detect drones through WiFi statistical fingerprint analysis of their traffic [3]. Recent advances in artificial intelligence (AI), along with massive network densification and the ubiquity of wireless communications will naturally lead to the emergence of more sophisticated traffic analysis attacks. However, conventional encryption or detection-based defensive paradigms are not sufficient to address these new challenges [2, 36, 39]. Solutions based on traffic reshaping including packet quantization and traffic morphing [5, 14, 39, 41], or disguising base stations by creating fake paths and activity [10, 23, 24, 26, 43] provide partial countermeasure against specific attacks, but do not provide provable guarantees.

In this work, we explore a new approach to inhibit the broad class of eavesdropping and traffic analysis attacks. In the proposed research, we combine two novel security paradigms to protect wireless communications. First, building on the notion of cyber deception for defense [15, 17, 20], we obfuscate real communications among fake packets to disrupt and deceive traffic analysis attacks. Second, building on the notion of cyber agility for defense [18, 19, 44], we randomize both real and fake packets over multiple multi-hop paths (subnetworks) between transmitters and receivers to confuse attackers about where to eavesdrop. We show that a combination of both techniques provides a robust solution with provable security against eavesdropping and traffic analysis attacks.

2 Related Work

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 *et al.* [34] identified web pages within SSL-encrypted connections by examining the sizes of the HTML objects returned in the HTTP response. Liberatore and Levine [25] 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 *et al.* [38] 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 *et al.* [32] 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 [39]. 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 [39]. 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 *et al.* [39] 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 his earlier works, co-PI Jafarian investigates the detrimental effect of eavesdropping attacks on TCP/IP networks and shows that they are significantly aggravated by adoption of deterministic single-path routing schemes. This gives adversaries significant advantages to gradually learn network routes and plan attacks accurately. For instance, intruders can eavesdrop on a session simply by attacking one of the intermediate links along the deterministic route route. Such an attack is feasible since only one single predictable route is chosen, and this predictable and static route enables intruders to discover the route and target it.

To address this, co-PI Jafarian present a proactive defense approach, called random route mutation (RRM) [11, 18], which protects designated flows by routing them via not one, but a number of randomly-chosen routes such that each route satisfies security, capacity, overlap and QoS constraints of the network. The objective of RRM is to transmit a designated flow between a source and destination, such that the proportion of the flow that could be eavesdropped by the attacker is minimized. To this aim, RRM selects an optimal set of routes such that each route is used for a certain duration, called *mutation interval*. At the beginning of each interval, the defender randomly selects a route from the qualified set and transmits a portion of flow using that route. The qualified routes are determined such that each route satisfies security and performance constraints of the network. This problem is modeled as a constraint satisfaction problem using generalized Boolean/arithmetic format of Satisfiability Modulo Theory (SMT), and solved using off-the-shelf SMT solvers [9].

To quantify effectiveness of this route randomization, co-PI Jafarian propose a metric called MPE (Mutation Protection Effectiveness) as the proportion of a given flow that is transmitted between a source s and a destination d without being compromised (e.g., eavesdropped). The results are driven for an attacker who has the capability of attacking r nodes simultaneously, and knows the topology and thus routes between s and d. The optimal attack strategy is to target the links in the min-cut of the selected routes between s and d. If m disjointed routes exists for transmission, the min-cut size is m and the attacker would be able to compromise $1 - r/m$ ratio of the flow ($r <= m$) on average. But if the $s - d$ min-cut is smaller than m (e.g. min-cut = $\lg(m)$), then the attacker can attack more routes by attacking the same number of nodes.

Figure 1 shows expected MPE for various m, min-cut sizes and r. Note that when the number of simultaneous attacked nodes (r) is even 1 and even with disjointed routes, expected MPE for a network with single-path routing is 0. Note that with higher m, expected MPE increases significantly. However, as the attacker's capability (r) increases, the average MPE decreases, especially with networks with lower min-cut sizes. For example when min-cut size is $\lg(m)$, and $m = 100$, the attacker only needs to attack $r = 7$ nodes to drop expected MPE to 0. Note that the effectiveness of route randomization is bounded by the min-cut of the routes between the protected $s - d$ pair. In fact if an attacker's capability , r, is larger than the largest min-cut between $s - d$, MPE will be 0 even with route randomization.

Jafarian *et al.* provide an implementation of RRM on software-defined networks, using Openflow switches and POX controller [21]. In this implementation, changing routes is accomplished via a series of flow table updates in all the switches both along the old and new routes. Authors show that the implementation preserves end-to-end reachability and is lossless.

3 Methodology

3.1 Problem Formulation

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:

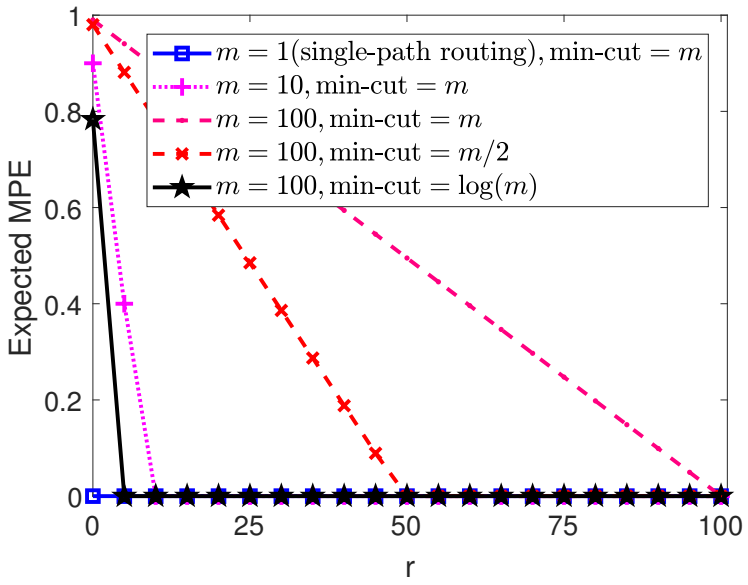

Figure 1: Expected MPE for various r and min-cut sizes

- 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 [31]. 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 2 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.

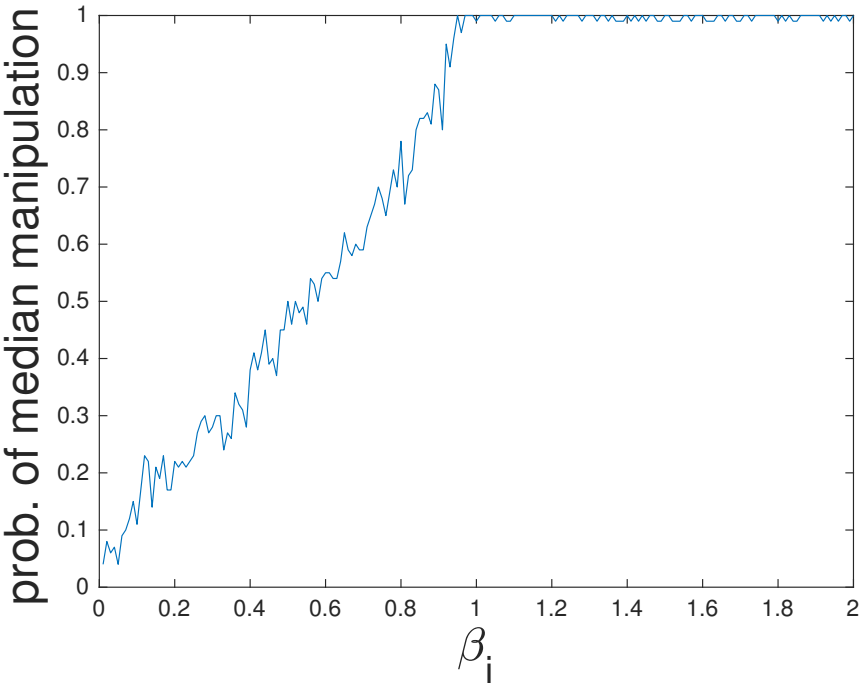

Figure 2: Median manipulation probability for different fake/real traffic ratios

3.2 Solution over Discrete Strategy Space

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 [40] to solve the problem.

As an 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 $f_i = r_i - k_i$.

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.

3.3 Solution over Continuous Strategy Space

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:

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

As it turns out, the solution to this problem can be seen as a type of water-filling. As illustrated in Figure 3, 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.

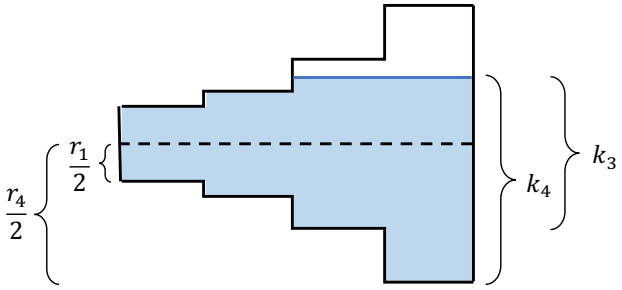

Figure 3: Water-filling solution to find k_1, k_2, k_3, k_4

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.

References

[1] NGMN Alliance. 5g security recommendations package. *White paper*, 2016.

[2] John S Atkinson, O Adetoye, Miguel Rio, John E Mitchell, and George Matich. Your wifi is leaking: Inferring user behaviour, encryption irrelevant. In *2013 IEEE Wireless Communications and Networking Conference (WCNC)*, pages 1097–1102. IEEE, 2013.

[3] Igor Bisio, Chiara Garibotto, Fabio Lavagetto, Andrea Sciarrone, and Sandro Zappatore. Unauthorized amateur uav detection based on wifi statistical fingerprint analysis. *IEEE Communications Magazine*, 56(4):106–111, 2018.

[4] George Dean Bissias, Marc Liberatore, David Jensen, and Brian Neil Levine. Privacy vulnerabilities in encrypted http streams. In *International Workshop on Privacy Enhancing Technologies*, pages 1–11. Springer, 2005.

[5] Xiang Cai, Xin Cheng Zhang, Brijesh Joshi, and Rob Johnson. Touching from a distance: Website fingerprinting attacks and defenses. In *Proceedings of the 2012 ACM conference on Computer and communications security*, pages 605–616. ACM, 2012.

[6] Rui Castro, Mark Coates, Gang Liang, Robert Nowak, and Bin Yu. Network tomography: Recent developments. *Statistical science*, pages 499–517, 2004.

[7] AHeroIII Coates, Alfred O Hero III, Robert Nowak, and Bin Yu. Internet tomography. *IEEE Signal processing magazine*, 19(3):47–65, 2002.

[8] Mark Coates, Rui Castro, Robert Nowak, Manik Gadhiok, Ryan King, and Yolanda Tsang. Maximum likelihood network topology identification from edge-based unicast measurements. In *ACM SIGMETRICS Performance Evaluation Review*, volume 30, pages 11–20. ACM, 2002.

[9] Leonardo De Moura and Nikolaj Bjørner. Z3: An efficient smt solver. In *International conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 337–340. Springer, 2008.

[10] Jing Deng, Richard Han, and Shivakant Mishra. Countermeasures against traffic analysis attacks in wireless sensor networks. In *SecureComm*, volume 5, pages 113–124, 2005.

[11] Qi Duan, Ehab Al-Shaer, and Haadi Jafarian. Efficient random route mutation considering flow and network constraints. In *2013 IEEE Conference on Communications and Network Security (CNS)*, pages 260–268. IEEE, 2013.

[12] Nick Duffield. Network tomography of binary network performance characteristics. *IEEE Transactions on Information Theory*, 52(12):5373–5388, 2006.

[13] Nick G Duffield, Joseph Horowitz, F Lo Presti, and Don Towsley. Multicast topology inference from measured end-to-end loss. *IEEE Transactions on Information Theory*, 48(1):26–45, 2002.

[14] Taher Ahmed Ghaleb. Techniques and countermeasures of website/wireless traffic analysis and fingerprinting. *Cluster Computing*, 19(1):427–438, 2016.

[15] Kristin E Heckman, Michael J Walsh, Frank J Stech, Todd A O'boyle, Stephen R DiCato, and Audra F Herber. Active cyber defense with denial and deception: A cyber-wargame experiment. *computers & security*, 37:72–77, 2013.

[16] Ibrahim Issa, Sudeep Kamath, and Aaron B Wagner. An operational measure of information leakage. In *2016 Annual Conference on Information Science and Systems (CISS)*, pages 234–239. IEEE, 2016.

[17] Jafar Haadi Jafarian. *Cyber Agility for Attack Deterrence and Deception*. PhD thesis, The University of North Carolina at Charlotte, 2017.

[18] Jafar Haadi Jafarian, Ehab Al-Shaer, and Qi Duan. Formal approach for route agility against persistent attackers. In *European Symposium on Research in Computer Security*, pages 237–254. Springer, 2013.

[19] Sushil Jajodia, Anup K Ghosh, Vipin Swarup, Cliff Wang, and X Sean Wang. *Moving target defense: creating asymmetric uncertainty for cyber threats*, volume 54. Springer Science & Business Media, 2011.

[20] Sushil Jajodia, VS Subrahmanian, Vipin Swarup, and Cliff Wang. *Cyber deception*. Springer, 2016.

[21] Sukhveer Kaur, Japinder Singh, and Navtej Singh Ghumman. Network programmability using pox controller. In *ICCCS International Conference on Communication, Computing & Systems, IEEE*, volume 138, 2014.

[22] Liaqat Ali Khan, Muhammad Shamim Baig, and Amr M Youssef. Speaker recognition from encrypted voip communications. *digital investigation*, 7(1-2):65–73, 2010.

[23] CK-L Lee, Xiao-Hui Lin, and Yu-Kwong Kwok. A multipath ad hoc routing approach to combat wireless link insecurity. In *IEEE International Conference on Communications, 2003. ICC'03.*, volume 1, pages 448–452. IEEE, 2003.

[24] Patrick PC Lee, Vishal Misra, and Dan Rubenstein. Distributed algorithms for secure multipath routing in attack-resistant networks. *IEEE/ACM Transactions on Networking*, 15(6):1490–1501, 2007.

[25] Marc Liberatore and Brian Neil Levine. Inferring the source of encrypted http connections. In *Proceedings of the 13th ACM conference on Computer and communications security*, pages 255–263. ACM, 2006.

[26] Wenjing Lou, Wei Liu, and Yuguang Fang. Spread: Enhancing data confidentiality in mobile ad hoc networks. In *ieee infocom*, volume 4, pages 2404–2413. Citeseer, 2004.

[27] Katsiaryna Mirylenka, Vassilis Christophides, Themis Palpanas, Ioannis Pefkianakis, and Martin May. Characterizing home device usage from wireless traffic time series. 2016.

[28] Andriy Panchenko, Lukas Niessen, Andreas Zinnen, and Thomas Engel. Website fingerprinting in onion routing based anonymization networks. In *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*, pages 103–114. ACM, 2011.

[29] Anand Prasad, Alf Zugenmaier, Adrian Escott, and Mirko Cano Soveri. *3GPP 5G Security*, 2018 (accessed September, 2019).

[30] Michael Rabbat, Robert Nowak, and Mark Coates. Multiple source, multiple destination network tomography. In *IEEE INFOCOM 2004*, volume 3, pages 1628–1639. IEEE, 2004.

[31] Peter J Rousseeuw and Annick M Leroy. *Robust regression and outlier detection*, volume 589. John wiley & sons, 2005.

[32] T Scott Saponas, Jonathan Lester, Carl Hartung, Sameer Agarwal, Tadayoshi Kohno, et al. Devices that tell on you: Privacy trends in consumer ubiquitous computing. In *USENIX Security Symposium*, pages 55–70, 2007.

[33] Dawn Song. Timing analysis of keystrokes and ssh timing attacks. In *Proc. of 10th USENIX Security Symposium, 2001*, 2001.

[34] Qixiang Sun, Daniel R Simon, Yi-Min Wang, Wilf Russell, Venkata N Padmanabhan, and Lili Qiu. Statistical identification of encrypted web browsing traffic. In *Proceedings 2002 IEEE Symposium on Security and Privacy*, pages 19–30. IEEE, 2002.

[35] Mahbod Tavallaee, Wei Lu, and Ali A Ghorbani. Online classification of network flows. In *2009 Seventh Annual Communication Networks and Services Research Conference*, pages 78–85. IEEE, 2009.

[36] Wade Trappe. The challenges facing physical layer security. *IEEE Communications Magazine*, 53(6):16–20, 2015.

[37] Charles V Wright, Lucas Ballard, Scott E Coull, Fabian Monrose, and Gerald M Masson. Spot me if you can: Uncovering spoken phrases in encrypted voip conversations. In *2008 IEEE Symposium on Security and Privacy (sp 2008)*, pages 35–49. IEEE, 2008.

[38] Charles V Wright, Lucas Ballard, Fabian Monrose, and Gerald M Masson. Language identification of encrypted voip traffic: Alejandra y roberto or alice and bob? In *USENIX Security Symposium*, volume 3, pages 43–54, 2007.

[39] Charles V Wright, Scott E Coull, and Fabian Monrose. Traffic morphing: An efficient defense against statistical traffic analysis. In *NDSS*, volume 9. Citeseer, 2009.

[40] Yan Mei Yang, Yan Guo, Li Chao Feng, and Jian Yong Di. Solving two-person zero-sum game by matlab. In *Applied Mechanics and Materials*, volume 50, pages 262–265. Trans Tech Publ, 2011.

[41] Fan Zhang, Wenbo He, and Xue Liu. Defending against traffic analysis in wireless networks through traffic reshaping. In *2011 31st International Conference on Distributed Computing Systems*, pages 593–602. IEEE, 2011.

[42] Fan Zhang, Wenbo He, Xue Liu, and Patrick G Bridges. Inferring users' online activities through traffic analysis. In *Proceedings of the fourth ACM conference on Wireless network security*, pages 59–70. ACM, 2011.

[43] Xiangyun Zhou, Radha Krishna Ganti, and Jeffrey G Andrews. Secure wireless network connectivity with multi-antenna transmission. *IEEE Transactions on Wireless Communications*, 10(2):425–430, 2010.

[44] Rui Zhuang, Scott A DeLoach, and Xinming Ou. Towards a theory of moving target defense. In *Proceedings of the First ACM Workshop on Moving Target Defense*, pages 31–40. ACM, 2014.