Predicting Operational Failure and Security Risks in DL04 QSDC protocol via Machine Learning

Myke D. M. Valadão[1], Celso B. Carvalho[1], Waldir S. S. Júnior[1]
[1]Federal University of Amazonas and Center for R&D in Elec. and Inf. Tech. (UFAM/CETELI), AM-Brazil
Emails: {mykedouglas, ccarvalho_, waldirjr}@ufam.edu.br

***Abstract*— Quantum communication protocols offer theoretically unbreakable security by leveraging the fundamental principles of quantum mechanics. Among them, the DL04 protocol enables direct, deterministic secure communication without requiring a pre-shared key. However, practical implementations remain vulnerable to performance degradation due to channel losses, detector inefficiencies, and increased QBER, which may compromise security. This paper presents a machine learning-based framework for predicting operational failures and assessing security risks in DL04 QSDC systems. A dataset of 48 simulated scenarios was generated, varying key physical parameters such as attenuation, depolarization, and detector efficiency over a range of transmission distances. Using regression models—including ensemble methods such as Gradient Boosting and Random Forest—we achieved highly accurate predictions of secure key rate and QBER. These models enable real-time monitoring, anomaly detection, and dynamic adjustment of protocol parameters, enhancing both performance and security. Results demonstrate that machine learning can effectively anticipate system behavior under different conditions, providing a foundation for intelligent, adaptive QKD systems. This approach represents a significant step toward resilient quantum communication architectures, particularly under realistic noise and hardware constraints.**

***Keywords*— Quantum Key Distribution, DL04 Protocol, Quantum Communication, Machine Learning**

I. Introduction

The exponential growth in data generation, transmission, and consumption has pushed modern communication systems to their limits in terms of both capacity and security [1]. As classical communication approaches the boundaries of Shannon's limit and becomes increasingly vulnerable to sophisticated cyberattacks, new paradigms are needed to ensure the confidentiality, integrity, and efficiency of data exchange [1][2]. In this context, quantum communication has emerged as a promising solution, leveraging the principles of quantum mechanics to enable fundamentally secure information transfer and potentially revolutionize long-distance communication infrastructures [3][4].

At the heart of quantum communication lies the exploitation of quantum properties such as superposition, entanglement, and no-cloning, which enable information to be encoded and transmitted in quantum states, typically represented by qubits [5]. Quantum key distribution (QKD) protocols, for instance, utilize these properties to enable two parties—commonly referred to as Alice and Bob—to establish a shared secret key that is theoretically immune to interception [6][7]. Any attempt by an eavesdropper (Eve) to measure or duplicate the quantum states inevitably introduces disturbances that can be detected by the legitimate users, thus providing an intrinsic security layer that classical systems lack [8].

Among the various QKD protocols developed, the DL04 protocol stands out as a practical and robust approach for deterministic secure direct communication [9]. It is based on the controlled manipulation of quantum states and enables direct transmission of secret messages without requiring a pre-shared key. However, in practical implementations, several challenges arise, such as operational failure due to channel noise, detector imperfections, and potential security vulnerabilities in the presence of malicious interference [7]. These factors can lead to increased quantum bit error rate (QBER) and compromised secure key rates, both of which degrade the overall reliability and safety of the quantum communication system [7].

To address these issues, this study proposes a machine learning-based framework to enhance the reliability and security of the DL04 quantum secure direct communication (QSDC) protocol. By leveraging supervised learning techniques, we aim to predict and monitor the QBER and secure key rate under varying operational conditions. Our models are trained on simulation data that incorporate realistic physical channel parameters, enabling accurate forecasting of system performance and the early detection of potential anomalies or failures. This predictive capability not only supports dynamic adaptation of protocol parameters but also contributes to real-time security assessment, offering a significant step toward practical and resilient quantum communication systems.

A. Contributions

This study makes several significant contributions to the field of quantum communication, particularly in enhancing the security and operational reliability of the DL04 QSDC protocol. Firstly, it introduces a novel dataset comprising 48 distinct QKD scenarios across multiple transmission distances, which enables the training of supervised learning models for accurately predicting system performance indicators, such as the measured QBER and secure key rate. Secondly, the study demonstrates the effectiveness of various machine learning models—especially ensemble methods like Gradient Boosting and Random Forest—in predicting these key performance metrics with high accuracy. Such predictive capabilities can facilitate real-time system monitoring and the proactive adjustment of protocol parameters. Furthermore, by modeling QBER using regression techniques, the research highlights how machine learning can also serve in assessing security risks, identifying anomalies that may signal threats like

eavesdropping or system malfunctions. Finally, the proposed approach lays the groundwork for developing intelligent QKD systems, promoting the integration of artificial intelligence into quantum communication to enable data-driven decision-making and dynamic protocol adaptation based on real-time insights.

II. Related Works

Bommi et al. [10] present a robust integration of machine learning techniques into the BB84 protocol, aiming to optimize QKD in practical settings plagued by noise, eavesdropping, and hardware imperfections. Their approach utilizes deep learning for photon state optimization, unsupervised learning for anomaly detection, and reinforcement learning for adaptive parameter tuning, yielding notable improvements in key generation rate (25%), QBER reduction (33.3%), and eavesdropping detection (7.8% gain). While their work demonstrates the effectiveness of machine learning for increasing system efficiency and robustness, it largely focuses on BB84 and general QKD protocols. Our work advances this direction by targeting the DL04 QSDC protocol—offering direct message transmission instead of key generation. Furthermore, our contribution is unique in generating a specialized dataset simulating realistic noise conditions and applying regression models to predict both QBER and secure key rate, enabling real-time anomaly detection and adaptive protocol control.

Mafu's [11] review systematically explores the application of ML and AI to quantum communication paradigms, including QKD, quantum teleportation, and quantum networking. It highlights how models such as random forests, neural networks, and reinforcement learning have been employed for tasks like parameter optimization, attack detection, and long-term system stability. For instance, it cites machine learning-enhanced calibration using long short term memory (LSTM) and secure key rate predictions through ensemble models. However, Mafu's paper primarily aggregates and discusses existing machine learning integrations across various protocols rather than proposing and validating a specific implementation. In contrast, our study builds a concrete, simulation-based experimental framework for the DL04 QSDC protocol and rigorously benchmarks multiple machine learning models, demonstrating Gradient Boosting's superior performance in predicting critical security parameters, thus contributing a practical and reproducible pathway for intelligent QSDC systems.

III. Methods

This section details the methodology employed to generate a comprehensive dataset for benchmarking the performance of an entanglement-based QKD protocol over optical fiber. The simulation framework incorporates key physical limitations of the transmission channel and detector imperfections to evaluate the achievable QBER and secure key rate under various operational parameters. In this entanglement-based QKD scenario, Alice and Bob aim to establish a shared secret key by exploiting the properties of entangled quantum states [11]. The security of the key distribution relies on the fundamental principles of quantum mechanics, such as the no-cloning theorem and the disturbance caused by measurement. While the current simulation primarily focuses on the legitimate communication between Alice and Bob under channel noise and detector limitations, the underlying security analysis in QKD inherently considers the potential presence of an eavesdropper, typically referred to as Eve.

The process begins with entangled pair generation, where Alice prepares pairs of entangled qubits. In this simulation, the initial quantum state is assumed to be the Bell state [12], represented mathematically as

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{1}$$

Once entangled, distribution takes place. Alice retains one qubit from each pair and transmits the other to Bob through a quantum channel, typically implemented as an optical fiber.

Following transmission, the measurement stage occurs. Both Alice and Bob independently measure their respective qubits [11]. For a selected subset of the entangled pairs—defined by a predetermined security check fraction—they publicly disclose their measurement bases and outcomes. This information is used to estimate the QBER. For the remaining pairs, the measurement results are kept secret and used to derive a shared cryptographic key. The security of this key relies on the strong correlations induced by entanglement and the sensitivity of quantum states to any external disturbance.

Finally, eavesdropping is considered in the security analysis. An adversary, Eve, may attempt to intercept or measure the qubits exchanged between Alice and Bob in order to gain information about the key. However, due to the no-cloning theorem and the inherent disturbance caused by quantum measurements, such actions would increase the QBER [11]. During the security check, if the measured QBER remains below a defined threshold, Alice and Bob can infer that the influence of any eavesdropper is negligible. Any residual information potentially accessible to Eve can then be eliminated through classical post-processing steps such as privacy amplification, ensuring a highly secure key.

While Eve's actions are not explicitly simulated in terms of directly implementing eavesdropping strategies, the impact of her potential presence is implicitly considered through the QBER threshold. A higher noise level in the channel (part of which could be attributed to Eve's interference) leads to a higher QBER. If this QBER exceeds the pre-established threshold, Alice and Bob would abort the key generation process, as the security of the key cannot be guaranteed. The QBER threshold is derived from security proofs that quantify the maximum tolerable error rate in the presence of an eavesdropper using optimal strategies.

Therefore, the simulation focuses on modeling the physical channel limitations that contribute to errors detectable by Alice and Bob (which would also be exacerbated by Eve's presence). The security of the QKD protocol is then evaluated based on whether the observed error rate (QBER) is below a level that theoretical security proofs guarantee resilience against eavesdropping.

A. Physical channel model

The simulation explores the impact of several crucial parameters on the performance of the QKD system. These parameters are systematically varied across predefined ranges during the experimental phase of the study. It is important to emphasize that although the parameters are assigned specific values in each simulation run (as detailed in Section IV), the methodology is designed to capture their general influence on system behavior.

One key parameter is optical fiber attenuation, denoted by α and measured in decibels per kilometer ($\mathrm{dB/km}$), which represents the loss of photon intensity as it propagates through the quantum channel [13]. The transmittance T over a distance L (in kilometers) is given by the equation:

$$T = 10^{-\frac{\alpha L}{10}}. \tag{2}$$

This directly affects the probability of successful photon transmission, influencing the rate at which entangled photon pairs can contribute to secure key generation. A higher attenuation leads to fewer photons reaching Bob, thereby reducing the overall key rate.

Another critical factor is the depolarization rate, denoted by γ and measured in inverse kilometers (km^{-1}), which models the likelihood of qubit depolarization per unit length of fiber [14]. The probability of depolarization over a distance L is approximated as:

$$p_{depol} = \min(1.0, \gamma L). \tag{3}$$

This depolarization introduces random Pauli errors (X, Y, Z) to the transmitted qubits, increasing the QBER. A higher depolarization rate can push the QBER beyond the tolerable security threshold, compromising key generation.

The efficiency of Bob's detector, η_{det}, is a dimensionless parameter between 0 and 1 that represents the probability of successfully detecting an incoming photon. This efficiency significantly influences the probability of a successful Bell state measurement when accounting for losses in the channel [12]. A low detector efficiency results in fewer detected entangled pairs, thereby decreasing the secure key rate.

The security check fraction, f_{check}, is also a dimensionless parameter ranging from 0 to 1, which specifies the proportion of entangled pairs used exclusively to estimate the QBER. These pairs are sacrificed for monitoring purposes and are not used for key distillation. While a larger check fraction improves the accuracy of the QBER estimation, it simultaneously reduces the number of pairs available for key generation, potentially decreasing the final key rate.

The QBER threshold, Q_{th}, defines the maximum tolerable QBER for the protocol to be considered secure. If the measured QBER exceeds this value, the data is regarded as compromised, and no key is distilled. This parameter plays a vital role in determining both the maximum transmission distance and the secure operating regime of the QKD system.

Additionally, the number of entangled pairs simulated per parameter-distance combination, denoted by N_{pairs}, affects the statistical confidence of the simulation outcomes. A higher number of simulated pairs provides more accurate estimates of QBER and key rate but increases the computational complexity and time required for simulation.

Lastly, the system performance is analyzed across a variety of optical fiber distances, L, to understand how channel length impacts secure transmission. Varying this parameter allows researchers to determine the maximum secure distance for each parameter set, offering insights into the scalability and limitations of the QKD implementation.

B. Machine learning models proposed

In this study, we applied supervised machine learning models to predict two key performance indicators of the DL04 QSDC protocol: the QBER and the secure key rate per entangled pair. The input features used for training include optical fiber attenuation (α), depolarization rate (γ), detector efficiency (η_{det}), and transmission distance (L). These parameters were selected because of their direct influence on photon loss and qubit disturbance during quantum communication.

The machine learning models evaluated include both linear and non-linear regressors. Linear Regression was used as a baseline model due to its simplicity and interpretability. To address potential multicollinearity and improve generalization, we also tested Ridge and Lasso regressions, which introduce L_2 and L_1 regularization, respectively [15]. For capturing non-linear relationships in the data, we employed a Decision Tree Regressor, as well as two ensemble methods: Random Forest and Gradient Boosting [16]. These ensemble models are known for their robustness and high accuracy in complex regression tasks. Additionally, a Multilayer Perceptron (MLP) neural network was tested to evaluate the performance of deep learning in this context.

C. Metrics

To evaluate the regression models used for predicting the QBER and the secure key rate, we employed standard performance metrics [16]. These metrics assess the discrepancy between the predicted values $\hat{y}_i$ and the ground truth values y_i across a total of N samples.

The first metric used is the mean squared error (MSE), which penalizes larger errors more heavily and provides a quadratic measure of prediction error:

$$\mathrm{MSE} = \frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2. \tag{4}$$

The mean absolute error (MAE) offers the average magnitude of the errors, without considering their direction:

$$\mathrm{MAE} = \frac{1}{N}\sum_{i=1}^{N}|y_i - \hat{y}_i|. \tag{5}$$

Another useful metric is the root mean squared error (RMSE), which is the square root of the MSE. It is expressed in the same unit as the target variable, making it more interpretable:

$$\mathrm{RMSE} = \sqrt{\frac{1}{N}\sum_{i=1}^{N}(y_i - \hat{y}_i)^2}. \tag{6}$$

Finally, we consider the coefficient of determination or R^2 score, which indicates the proportion of variance in the dependent variable that is predictable from the independent variables:

$$R^2 = 1 - \frac{\sum_{i=1}^{N}(y_i - \hat{y}_i)^2}{\sum_{i=1}^{N}(y_i - \bar{y})^2}. \quad (7)$$

Values of R^2 close to 1.0 represent better model fit.

These metrics provide complementary perspectives on model performance and were computed for both QBER and secure key rate prediction tasks across all evaluated models.

IV. Experiments and Results

A. Simulation parameters

The dataset utilized in this study was generated through a series of simulations designed to model the performance of an entanglement-based QKD system [17]. These simulations encompassed 48 distinct scenarios, systematically varying key QKD parameters: optical fiber attenuation, depolarization rate increase, and Bob's detector efficiency, Table I. For each scenario, the simulation calculated performance metrics across a range of distances, generating data points for subsequent analysis. Machine learning models were trained with the dual objective of predicting two critical QKD performance indicators: the measured QBER and the secure key rate per entangled pair. This dual-target approach allows for a comprehensive assessment of both the security and operational efficiency of the simulated QKD system.

TABLE I
Parameters for Entanglement-Based QKD - Dataset Generation

Parameter	Values/Description
Optical Fiber Attenuation (α)	$[0.18, 0.20, 0.22]$ dB/km
Depolarization Rate Increase (γ)	$[0.0005, 0.001, 0.002, 0.004]$ km^{-1}
Bob's Detector Efficiency (η_{det})	$[0.7, 0.8, 0.9, 0.95]$
Security Check Fraction (f_{check})	0.5
QBER Threshold (Q_{th})	0.05
Pairs per Simulation Point (N_{pairs})	5000
Simulation Distances (L)	`np.linspace(1, 200, 100)` km

B. Predicting security key rate

TABLE II
Regression Model Performance on Secure Key Rate Prediction

Model	MSE	MAE	RMSE	R^2
Linear Regression	0.00916	0.05838	0.0957	0.2598
Ridge Regression	0.00917	0.05831	0.0957	0.2592
Lasso Regression	0.00954	0.05161	0.0976	0.2309
Decision Tree Regressor	0.000060	0.00263	0.0077	0.9951
Random Forest Regressor	0.000042	0.00224	0.0065	0.9967
Gradient Boosting Regressor	0.000032	0.00232	0.0057	0.9974
Neural Network (MLP)	0.00177	0.00846	0.0421	0.9658

The results presented in Table II are highly relevant for understanding and optimizing the performance of QKD systems. The main objective in QKD is to establish a secure key rate between two parties (Alice and Bob) despite limitations imposed by the physical transmission channel and various system imperfections. Being able to accurately predict the secure key rate based on system parameters is essential for multiple reasons.

First, from a system design and optimization perspective, the models enable predictions of secure key rate under diverse operational conditions, such as varying fiber lengths, attenuation levels, and detector efficiencies. This predictive capability supports informed decisions when designing the system or tuning its parameters to maximize both the key rate and transmission distance. For example, the models can assist in evaluating the trade-off between detector efficiency and maximum achievable distance.

Second, the models are useful for performance prediction and real-time monitoring. By observing the system parameters in operation, it becomes possible to anticipate potential drops in secure key rate and implement proactive adjustments to mitigate disruptions. This also makes the models valuable for fault diagnosis and troubleshooting. Significant deviations between the predicted and measured key rates may indicate system malfunctions or even potential security breaches, allowing the models to help pinpoint the root cause of such issues.

Additionally, the models contribute to security assessment. The QBER, which is intrinsically related to the secure key rate, is a critical parameter for evaluating the system's resilience. Although the models focus on predicting the secure key rate directly, their accuracy indirectly reflects how well they capture the underlying physical and operational factors that influence security.

Finally, in the context of a QKD network, the models provide insights that aid in resource allocation. By predicting the achievable key rates across different links, the system can make informed routing decisions and optimize the overall usage of network resources.

The high accuracy of the ensemble models (Random Forest and Gradient Boosting) in predicting the secure key rate suggests that these models effectively capture the complex relationships between system parameters and performance. This capability can be leveraged to develop more robust and efficient QKD systems. However, the trade-off between model complexity and computational cost must be considered, especially in real-time applications.

C. Predicting QBER measured

Remember that the QBER is a crucial metric in QKD because it quantifies the error rate in the transmission of quantum information. In a secure QKD system, the QBER must remain below a certain threshold to ensure that the amount of information an eavesdropper (Eve) might have obtained is limited and can be reduced to zero through post-processing (such as privacy amplification).

The results show that ensemble models (Gradient Boosting and Random Forest) are more effective at predicting QBER, meaning they can provide more reliable estimates of the expected QBER behavior, Table III. However, even for these models, the R^2 isn't close to 1, indicating that there's some

TABLE III
REGRESSION MODEL PERFORMANCE ON QBER PREDICTION

Model	MSE	MAE	RMSE	R^2
Linear Regression	0.0725	0.2001	0.2693	0.2740
Ridge Regression	0.0780	0.2082	0.2792	0.2072
Lasso Regression	0.0795	0.2035	0.2819	0.1992
Decision Tree Regressor	0.1067	0.1450	0.3266	-0.0730
Random Forest Regressor	0.0667	0.1368	0.2582	0.3270
Gradient Boosting Regressor	0.0559	0.1317	0.2364	0.4394
Neural Network (MLP)	0.0681	0.1749	0.2610	0.2990

variability in the QBER that isn't explained by the features we are using. This could mean that other factors (not included in the model) are influencing the QBER, or that there's an inherent level of randomness in the process. In terms of security risk, this means that while you can use these models to get an estimate of the expected QBER, you should still exercise caution and design your QKD system to be tolerant of unexpected deviations in the QBER. In summary, QBER prediction models are valuable tools for enhancing the security of QKD systems, enabling more sophisticated monitoring, anomaly detection, and dynamic adaptation of security protocols. However, it's essential to interpret model results cautiously and consider their limitations.

V. CONCLUSIONS

This study presented a predictive framework based on machine learning to enhance the operational reliability and security assessment of the DL04 QSDC protocol. By generating a comprehensive dataset simulating realistic physical conditions—such as optical fiber attenuation, depolarization effects, and detector inefficiencies—we trained and evaluated several regression models to predict key performance indicators, namely the QBER and secure key rate.

The experimental results demonstrated that ensemble-based models, particularly Gradient Boosting and Random Forest, consistently outperformed linear models and neural networks in terms of prediction accuracy. These models achieved high R^2 scores for secure key rate prediction and offered valuable insights into QBER trends, albeit with moderate explanatory power. Such predictive capabilities enable early detection of anomalies, support dynamic protocol adaptation, and provide real-time risk evaluation mechanisms, which are critical for maintaining the integrity of quantum communication systems.

Ultimately, the integration of machine learning into quantum communication represents a promising avenue for the development of intelligent QKD systems. By forecasting degradation in performance and identifying potential security threats before they manifest, this approach contributes to the realization of scalable, resilient, and practically deployable quantum networks.

ACKNOWLEDGMENT

This research, carried out by UFAM/CETELI and ENVISION (TPV Group), was funded by ENVISION Indústria de Produtos Eletrônicos LTDA, in accordance with Article 39 of Decree No. 10.521/2020, following the guidelines of Brazilian federal law No. 8.387/91 (SUFRAMA).

REFERENCES

[1] Andrew Feutrill and Matthew Roughan. A review of shannon and differential entropy rate estimation. *Entropy*, 23(8):1046, 2021.

[2] Yangfei Lin, Celimuge Wu, Xianfu Chen, Yusheng Ji, et al. Meta-networking: Beyond the shannon limit with multi-faceted information, semantic communication, iov, multi-faceted inforamtion. *Authorea Preprints*, 2023.

[3] Matteo Rosati and Gabriella Cincotti. Optical communications at the quantum limit. In *2024 24th International Conference on Transparent Optical Networks (ICTON)*, pages 1–4. IEEE, 2024.

[4] Angeles Vázquez-Castro and Zhu Han. Interplay of classical-quantum resources in space-terrestrial integrated networks. *IEEE Communications Magazine*, 62(10):54–60, 2024.

[5] Frédéric Bouchard, Duncan England, Philip J Bustard, Khabat Heshami, and Benjamin Sussman. Quantum communication with ultrafast time-bin qubits. *PRX Quantum*, 3(1):010332, 2022.

[6] Mujtaba Zahidy, Domenico Ribezzo, Claudia De Lazzari, Ilaria Vagniluca, Nicola Biagi, Ronny Müller, Tommaso Occhipinti, Leif K Oxenløwe, Michael Galili, Tetsuya Hayashi, et al. Practical high-dimensional quantum key distribution protocol over deployed multicore fiber. *Nature Communications*, 15(1):1651, 2024.

[7] Asif Iqbal Saiyed. Optimizing quantum key distribution (qkd) protocols for secure communication in noisy quantum networks. *Annals of Applied Sciences*, 6(1), 2025.

[8] Ashutosh Bhatia, Sainath Bitragunta, and Kamlesh Tiwari. Enhanced lightweight quantum key distribution protocol for improved efficiency and security. *IEEE Open Journal of the Communications Society*, 2025.

[9] Gui-Lu Long and Haoran Zhang. Drastic increase of channel capacity in quantum secure direct communication using masking. *Science Bulletin*, 66(13):1267–1269, 2021.

[10] RM Bommi, M Nalini, N Vijayaraj, and A Mary Joy Kinol. Enhancing quantum key distribution protocols with machine learning techniques. In *2023 Intelligent Computing and Control for Engineering and Business Systems (ICCEBS)*, pages 1–4. IEEE, 2023.

[11] Mhlambululi Mafu. Advances in artificial intelligence and machine learning for quantum communication applications. *IET Quantum Communication*, 5(3):202–231, 2024.

[12] Amélie Piveteau, Jef Pauwels, Emil Håkansson, Sadiq Muhammad, Mohamed Bourennane, and Armin Tavakoli. Entanglement-assisted quantum communication with simple measurements. *Nature communications*, 13(1):7878, 2022.

[13] Sreraman Muralidharan, Linshu Li, Jungsang Kim, Norbert Lütkenhaus, Mikhail D Lukin, and Liang Jiang. Optimal architectures for long distance quantum communication. *Scientific reports*, 6(1):20463, 2016.

[14] Marcel Kokorsch and Guido Dietl. Usability regions of quantum repeaters for depolarization channels. In *GLOBECOM 2024-2024 IEEE Global Communications Conference*, pages 3485–3490. IEEE, 2024.

[15] Xiaoxing Yang and Wushao Wen. Ridge and lasso regression models for cross-version defect prediction. *IEEE Transactions on Reliability*, 67(3):885–896, 2018.

[16] Myke Valadão, Diego Amoedo, André Costa, Celso Carvalho, and Waldir Sabino. Predicting noise and user distances from spectrum sensing signals using transformer and regression models. *Applied Sciences*, 15(8):4296, 2025.

[17] J Robert Johansson, Paul D Nation, and Franco Nori. Qutip: An open-source python framework for the dynamics of open quantum systems. *Computer physics communications*, 183(8):1760–1772, 2012.