

TRUSTED PASSIVE OPTICAL NETWORKS ACCESS AUTHENTICATION USING DISTANCE CONDITIONED BIT ERROR RATE FINGERPRINTING AND A PERMISSIONED BLOCKCHAIN

XIANGQING WANG ^{1,2,3,4}, XIAOLING CHENG ¹, DONGFEI WANG ^{1,2}, XIAOKUN YANG ^{1,2,3},
NANNAN YU ^{4*}

¹ Nanchang Institute of Technology, School of Electronic Information, 901, Yingxiong Avenue,
Nanchang City, Jiangxi Province, 330044, China

² Wuhan Institute of Technology & Business, Wuhan 430065, P. R. China, 3, Huangjiahu West Road,
Hongshan District, Wuhan, Hubei Province, China, 430065, China

³ Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu
University of Information Technology, 610225, Chengdu, Sichuan, China

⁴ Fuyang Normal University, 100 Qinghe West Road, Yingzhou District, Fuyang, Anhui Province,
236037, China

*Corresponding author: 202404004@fynu.edu.cn

Received: 07.09.2026

Abstract. To address credential cloning and limited auditability in passive optical networks (PONs), we present a simulation-based proof of concept for access authentication that integrates distance-conditioned bit-error-rate (*BER*) fingerprinting with a permissioned blockchain. A *BER*-distance reference template is constructed under registered link conditions. During authentication, normalized deviations between real-time pre-forward-error-correction *BER* and registered references serve as channel fingerprints for physical-layer authentication, while an adaptive threshold, calibrated on simulated legitimate observations, assesses physical-path consistency. Nonce-bound signed measurement evidence supports auditable authorization through practical Byzantine fault tolerance consensus. On an independent simulated test set, the validation-selected threshold yields a false rejection rate of 0.493% and a false acceptance rate of 0.019%; the uncertainty-scaled, relative, and absolute *BER*-deviation measures yield area under the curve values of 0.99999, 0.99990, and 0.90524, respectively. The results support feasibility under the modeled conditions; hardware validation remains necessary, and compensation attacks limit *BER*-based discrimination.

Keywords: passive optical network, physical layer authentication, channel fingerprint, permissioned blockchain, practical Byzantine fault tolerance

UDC: 621.391.63:621.391

DOI: 10.3116/16091833/Ukr.J.Phys.Opt.2027.01063

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

1. Introduction

Passive optical networks (PONs) provide shared optical access for residential and enterprise services. Recent advances in simplified coherent reception and burst-mode digital signal processing (DSP) enable higher transmission rates while addressing receiver complexity and upstream acquisition requirements [1-3]. However, increased transmission capability does not confirm whether an optical network unit (ONU) remains connected to its registered physical branch. If an adversary obtains reusable credentials, conventional identity verification may accept a device operating over a different optical path.

Optical-layer security therefore requires attention beyond credential management. Network monitoring can identify evolving physical-layer threats [4], whereas chaotic encryption and integrated optical encryption primarily protect transmitted information [5,6]. Physical-layer authentication more directly addresses device or channel identification. Existing approaches

include channel-characteristic fingerprints in wavelength-division-multiplexed PONs, Siamese-network hardware authentication, and deep-neural-network authentication in optical links [7-9]. Optical-fiber physical unclonable function readers and delayed self-homodyne detection provide additional identification mechanisms based on fiber responses or device-dependent laser fluctuations [10,11]. These studies establish the relevance of physical fingerprints to access security but differ in measurement requirements, feature representations, and classification procedures.

The pre-forward-error-correction (pre-FEC) bit error rate provides a complementary observable for evaluating registered-path consistency. When receiver diagnostics expose suitable error statistics, *BER* estimation may avoid the need for a dedicated optical interrogation module at each ONU; its implementation requirements remain to be assessed on a physical PON platform. Its dependence on received power and receiver noise provides a physical basis for comparison with registered conditions. Nevertheless, a common absolute *BER* threshold can be biased by the markedly different reference error rates of individual links. Temperature drift, component variation, and finite observation windows also affect legitimate measurements. Distance-conditioned reference templates and uncertainty-aware thresholds are therefore needed to distinguish relevant deviations from expected fluctuations. Such evidence indicates consistency with a registered transmission state; it does not establish a cryptographically unique channel identity. An adversary that can adjust optical power, receiver gain, or insertion loss may reproduce a *BER* close to the registered reference without replicating the legitimate physical path.

Distributed authorization also requires explicit policies and traceable evidence. Blockchain architectures and consensus protocols provide mechanisms for coordinating state updates among participating entities [12,13]. In optical networks, related applications include event anchoring, virtual PON resource sharing, collaborative trust management, and digital-twin component management [14-17]. Blockchain-based access-control systems likewise demonstrate distributed policy enforcement in the Internet of Things [18,19]. However, agreement on a ledger entry does not establish the accuracy of the underlying measurement. This distinction is central to the blockchain oracle problem and requires a clearly defined trust boundary for off-chain evidence [20]. As summarized in Table 1, building on existing *BER*- and channel-feature-based authentication studies [8,21], this work introduces a permissioned blockchain that integrates distance-conditioned *BER* decisions with nonce-bound signed evidence and practical Byzantine fault tolerance (PBFT) authorization, supporting evidence integrity and freshness checks and traceable authorization records. The main novelty is the cross-layer integration of physical-path consistency assessment with auditable access control.

This paper presents a PON access-authentication framework that links physical-path consistency assessment to auditable authorization and is evaluated as a simulation-based proof of concept. Certificate verification establishes credential possession, while distance-conditioned *BER* templates and uncertainty-aware adaptive thresholds provide a complementary physical-layer consistency check. A trusted optical line terminal (OLT) measurement process binds signed *BER* evidence to a fresh challenge and the registered template version. Smart contracts manage template digests, signed evidence, and authorization states, with PBFT providing consensus confirmation. Raw *BER* observations are retained off-chain. The contribution integrates physical-layer assessment with evidence binding and distributed authorization. The framework assumes

Table 1. Comparison with prior optical physical-layer authentication studies

Dimension	Wang et al. (2020) [21]	Wang et al. (2024) [8]	Proposed framework
Fingerprint	<i>BER</i> variation of an optical-fiber loop	Channel features conditioned on negotiated distance and device power	Distance- and temperature-conditioned <i>BER</i> deviation
Decision mechanism	<i>BER</i> -variation threshold	DNN classification	Adaptive threshold incorporating finite bit uncertainty
Evidence and authorization	Local physical-layer decision	OLT-side classification	Nonce-bound signed evidence and PBFT authorization
Main objective	<i>BER</i> -based channel authentication	Channel-feature-based ONU identification	Physical-path consistency and authorization traceability

trusted OLT measurements; consensus cannot independently establish their physical accuracy. Performance and robustness under real operating conditions remain to be validated on a physical PON platform and an implemented blockchain.

2. Theoretical analysis of distance-dependent *BER* physical fingerprint authentication

2.1. Received power and decision *Q*-factor

Let d be the registration distance, P_t the launched optical power, $P_r(d, T)$ the received optical power, L_s the splitter loss, L_c the connector and insertion-loss margin, T the operating temperature, and T_0 the reference temperature. Using a first-order temperature extension of the standard logarithmic fiber-loss relation [22, 23], the received power is:

$$P_r(d, T) = P_t \exp_{10} \left(- \frac{[\alpha_0 + \kappa_T(T - T_0)]d + L_s + L_c}{10} \right). \quad (1)$$

Here, α_0 is the fiber attenuation coefficient at the reference temperature, and κ_T is its temperature coefficient. For the avalanche-photodiode receiver used in the numerical model, the decision *Q*-factor is [24]

$$Q(d, T) = \frac{I_1(d, T) - I_0(d, T)}{\sigma_1(d, T) + \sigma_0(d, T)}. \quad (2)$$

In Eq. (2), I_1 and I_0 are the mean sampled currents for logical one and zero, and σ_1 and σ_0 are their root-mean-square noise currents. The avalanche photodiode (APD) signal, shot-noise, and thermal-noise contributions are evaluated in the numerical receiver model.

Under the Gaussian decision approximation, the pre-FEC *BER* is [24]:

$$BER_{phy}(d, T) = \frac{1}{2} \operatorname{erfc} \left[\frac{Q(d, T)}{\sqrt{2}} \right]. \quad (3)$$

Power attenuation caused by increasing distance is nonlinearly mapped to *BER* rise via the *Q*-factor. Temperature shifts the curve but does not change its monotonicity within the operating range.

2.2. *BER* template calibration and on-chain integrity protection

To mitigate model deviations from device dispersion and unmodeled losses, we calibrate the physical model with legitimate calibration samples. Since *BER* spans multiple orders of

magnitude, logarithmic-domain fitting prevents high-BER samples from dominating the fitting error. In this work, a quadratic distance term is introduced to fit receiver nonlinearity, and a temperature term to fit attenuation drift, yielding the BER fitting model:

$$\log_{10} BER_{ref}(d, T) = \beta_0 + \beta_1 d + \beta_2 d^2 + \beta_3 (T - T_0), \quad (4)$$

where BER_{ref} is the actual BER value obtained from the logarithmic fit, and the coefficient vector $\beta = (\beta_0, \beta_1, \beta_2, \beta_3)$ is estimated via least squares. The template parameters are hashed with SHA-256 and stored in the blockchain state contract. The consistency between the local and on-chain digests is verified before authentication to prevent parameter tampering attacks.

2.3. Real-time BER measurement and normalized features

The OLT sends a pseudo-random binary sequence (PRBS). L_{PRBS} denotes its period, whereas N_b is the total number of observed bits in one authentication window. If N_e bit errors are counted, the measured BER is the corresponding sample proportion [25]:

$$BER_{mean} = \frac{N_e}{N_b}. \quad (5)$$

For a true bit-error probability p , the error count is binomial. Dividing the binomial standard deviation by the observation length gives the standard deviation of the measured BER [25]:

$$\sigma_{BER} = \sqrt{\frac{p(1-p)}{N_b}}. \quad (6)$$

During authentication, p is evaluated under the legitimate hypothesis using the registered reference [21]. To enable comparison among ONUs with different reference BER levels, the normalized absolute deviation used in Figs. 1 and 2 is defined as

$$\eta_i = \frac{|BER_{mean,i} - BER_{ref,i}|}{BER_{ref,i}}. \quad (7)$$

2.4. Adaptive decision threshold and two error rates

Let μ_η and σ_η be the mean and standard deviation of the normalized absolute deviation in Eq. (7), estimated from legitimate training observations over the registered temperature range and routine receiver drift. Combining this empirical spread with the corrected finite-bit term in Eq. (6), we define:

$$\theta_i(k) = \mu_\eta + k\sigma_\eta + z_{1-\delta/2} \sqrt{\frac{1 - BER_{ref,i}}{N_b BER_{ref,i}}}, \quad (8)$$

Here, $BER_{ref,i}$ is the registered reference for attempt i , $z_{1-\delta/2}$ is the standard-normal quantile, and k is selected on the validation set. An attempt is accepted when $\eta_i \leq \theta_i(k)$. Note that the radical term in Eq. (8) does not describe any physical transmission medium or hardware environment, but strictly captures the mathematical sampling statistical fluctuations inherently induced by the finite-bit observation window N_b .

Let H_0 denote legitimate access and H_1 denote adversarial access. The false rejection rate (FRR) and false acceptance rate (FAR) are :

$$FRR(k) = P[\eta_i > \theta_i(k) | H_0], \quad (9)$$

$$FAR(k) = P[\eta_i \leq \theta_i(k) | H_1]. \quad (10)$$

Adjusting k balances security and availability. Section 4.3 therefore reports the full FAR - FRR threshold sweep, a detection error trade-off (DET) view, security-critical FAR operating points, Wilson confidence intervals, and the underlying authentication counts.

2.5. Practical Byzantine fault tolerance distributed consensus and system performance

In a PBFT deployment with n validators, the proposed protocol defines validator j 's local vote on authentication attempt i as follows [26]:

$$v_{ij} = I\{\eta_i \leq \theta_i(k) \wedge h_{ij} = h_{chain}\}. \quad (11)$$

The indicator equals one only when the physical-consistency test passes and validator j obtains a local template hash h_{ij} matching the registered on-chain hash h_{chain} .

PBFT requires at least $3f + 1$ validators to tolerate f Byzantine validators, and a quorum contains $2f + 1$ matching votes. Thus, the access decision is [26]:

$$A_i = I\left\{\sum_{j=1}^n v_{ij} \geq 2f + 1\right\}, \quad n \geq 3f + 1. \quad (12)$$

For the numerical scalability study, we use an empirical latency fit whose coefficients are obtained from the simulated communication latency [27]:

$$L_{auth}(n) = L_{meas} + L_{exec} + a + bn(n-1) + L_{commit}, \quad (13)$$

where L_{meas} is physical-measurement latency, L_{exec} is contract-execution latency, a and b are coefficients fitted to the simulated communication latency, and L_{commit} is block-commit latency.

3. Cross-layer authentication system based on BER fingerprinting and a permissioned blockchain

3.1. System model

Fig. 1 presents the cross-layer architecture of the proposed system. The PON physical layer comprises an OLT, a passive splitter, and multiple ONUs. During registration, the OLT collects legitimate pre-FEC BER measurements under different distance and temperature conditions and constructs a distance-conditioned BER reference surface. During online operation, the receiver DSP extracts the instantaneous BER sequence and compares it with the registered template of the requesting ONU. Measurements from a legitimate path should remain close to the reference distribution, whereas ONU substitution or an additional fiber segment changes the link loss and receiver noise, producing a detectable fingerprint mismatch. The normalized BER deviation is therefore evaluated against an adaptive threshold to distinguish path anomalies from normal fluctuations.

As shown in Fig. 1, the system calculates the normalized deviation η_i of real-time pre-FEC BER using the distance- and temperature-conditioned reference template $BER_{ref}(d, T)$. When $\eta_i \leq \theta_i(k)$, the OLT generates signed evidence E_i binding the device identifier, nonce, template version, and measurement digest for smart-contract verification. Authentication succeeds only after PBFT consensus confirms and commits the authorization state, followed by access-token issuance. Requests failing the physical consistency check are rejected or quarantined. Block headers link successive blocks through previous-block hashes, while Merkle roots support integrity verification of the evidence transactions. Template and evidence digests, signatures, and authorization states are recorded on-chain, whereas raw BER observations remain off-chain, linking physical-path consistency assessment to auditable authorization.

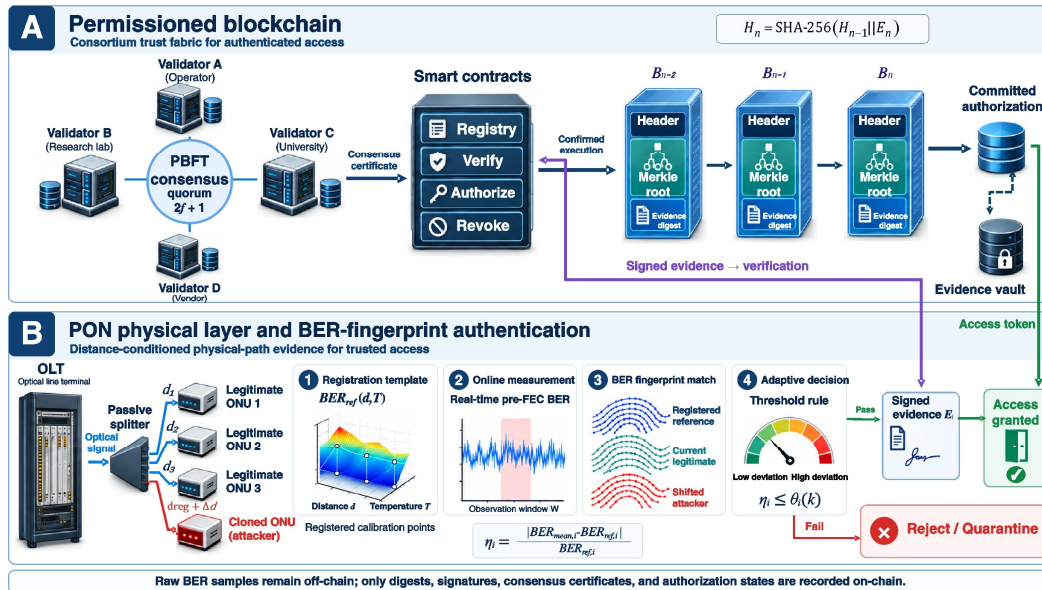


Fig. 1. Cross-layer trusted-access architecture based on *BER* fingerprinting and a permissioned blockchain.

The OLT measurement process and its signing key are assumed to be trusted. Validators verify the authenticity and freshness of the submitted evidence and enforce the registered authorization policy; they do not independently establish the physical correctness of the *BER* observation. A compromised OLT can therefore submit false but correctly signed measurements, which cannot be detected by blockchain consensus alone.

3.2. Registration and authentication procedure

Fig. 2 illustrates the proposed PON authentication workflow. During registration, legitimate ONU *BER* samples are used to construct the distance-conditioned template $BER_{ref}(d, T)$ and determine the adaptive threshold $\theta_i(k)$, while the template digest and policy are committed to the permissioned blockchain. During online authentication, the normalized *BER* deviation η_i is evaluated, and signed evidence E_i is generated only when the threshold condition is met. Blockchain nodes then verify the evidence and complete authorization and state recording via PBFT consensus. Raw *BER* data remain off-chain, while digests, signatures, and access states are maintained on-chain.

Step 1: Sample calibration. The OLT collects legitimate *BER* samples, fits a distance- and temperature-conditioned template, and evaluates its residual distribution, repeatability, and valid operating range.

Step 2: Template registration. A qualified template is assigned a version number, and its adaptive threshold $\theta_i(k)$ is estimated. The template digest and access policy are encapsulated in registration transaction *R*. Once confirmed by the registry contract, the transaction produces the verified reference state *V*.

Step 3: Online measurement. When an ONU requests access, the OLT retrieves *V*, generates a one-time nonce, and issues a PRBS challenge. The receiver estimates the real-time pre-FEC *BER* over a prescribed observation window and calculates the normalized deviation η_i .

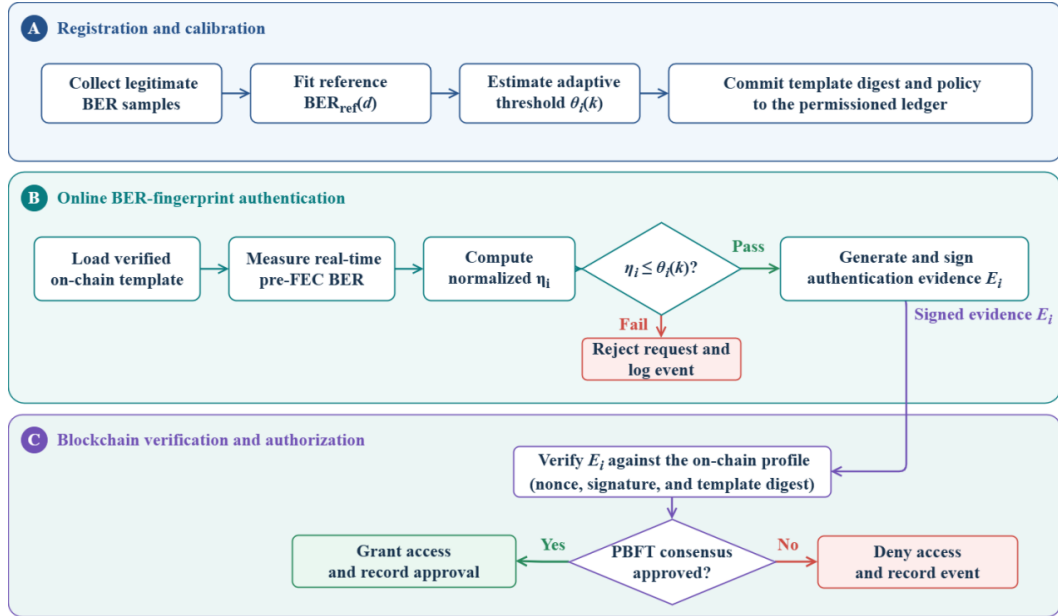


Fig. 2. PON access authentication workflow based on distance-conditioned *BER* fingerprinting and a permissioned blockchain.

Step 4: Evidence construction. If the measurement confidence is insufficient or the result lies close to the decision boundary, the observation window is extended. Otherwise, the nonce, timestamp, template version, *BER* digest, and local decision are packaged as evidence *E* and signed by the OLT agent.

Step 5: Consensus validation. Validator nodes verify evidence freshness, signature validity, template integrity, and decision consistency before executing PBFT. The final state is jointly determined by physical consistency and the consensus quorum:

$$D_i = I\{\eta_i \leq \theta_i(k) \wedge A_i = 1\}, \quad (14)$$

where $D_i = 1$ denotes successful authentication, η_i and $\theta_i(k)$ are the physical-layer feature and threshold shown in Figs. 1 and 2, and A_i is the PBFT authorization result in Eq. (12).

Step 6: State execution. If Eq. (14) is satisfied, the authorization contract commits the approved decision and issues a short-lived access token. Otherwise, the rejection contract revokes the pending authorization and discards the request. The template digest, evidence digest, consensus certificate, and contract result are recorded on the permissioned ledger. The threshold $\theta_i(k)$ determines the *FRR-FAR* operating point evaluated later, whereas n and f govern the PBFT latency.

4. Performance evaluation and analysis

This section evaluates the distance-conditioned *BER* template, environmental perturbations, threshold operating point, authentication performance, attack-detection boundary, and consensus overhead. The results use the registered *BER* reference, the normalized deviation defined in Eq. (7), and the joint rule in Eq. (14).

4.1. *BER* template validation

Fig. 3 compares the APD receiver model, the fitted reference $BER_{ref}(d)$, and the calibration points obtained from legitimate ONUs. The fitted curve closely follows the physical model

over the registered distance range, yielding $R^2 = 0.9991$. The template therefore accurately captures the increase in pre-FEC BER with fiber distance. Consequently, $BER_{ref}(d)$ can serve as an individualized authentication baseline without introducing the distance bias associated with a uniform absolute threshold.

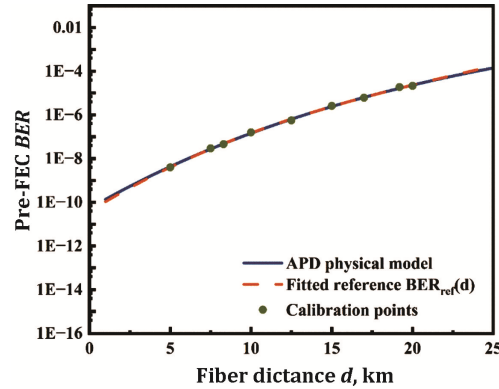


Fig. 3. Distance-conditioned BER template validation.

4.2. Environmental perturbations

Fig. 4 presents the BER-distance curves for different fiber types and temperatures. Variations in the attenuation coefficient and temperature shift the curves but do not alter their monotonic increase with transmission distance. This result confirms the physical consistency of distance-induced BER variation while demonstrating that each template must remain associated with its operating conditions. Fiber type, valid temperature range, and model version should therefore be included in the registration profile. Recalibration is required when the operating conditions exceed the valid template range.

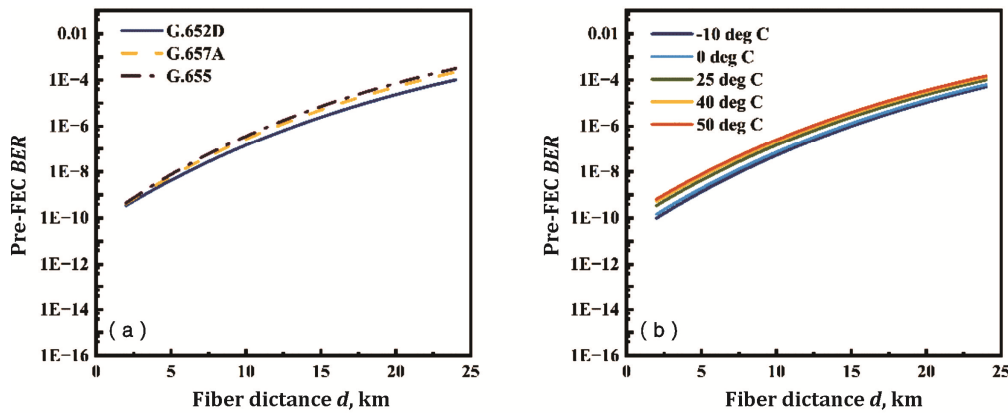


Fig. 4. Environmental sensitivity of the BER-distance relationship: (a) different fiber types; (b) temperature variation.

4.3. Threshold selection

Fig. 5 shows the influence of the threshold coefficient on FRR and FAR . Increasing the coefficient widens the acceptance interval, reducing FRR while increasing FAR . The coefficient was selected using 22,500 legitimate and 120,000 attack validation observations. At $k = 2.150$, 222 of the 45,000 legitimate test attempts were rejected, giving an FRR of 0.493%; the corresponding 95% Wilson interval ranges from 0.433% to 0.562%. Among 120,000 independent attack attempts, 23 were accepted, giving an FAR of 0.019%; its 95% Wilson interval ranges from 0.0128% to 0.0288%.

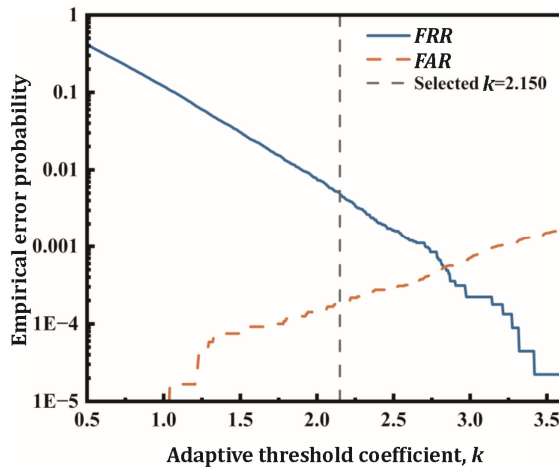


Fig. 5. Validation-set FAR and FRR versus the adaptive threshold coefficient.

on normal-deviate probability axes. The descending trend is expected because a wider acceptance interval increases FAR while decreasing FRR. A half-count correction is used only to display zero empirical rates on the probability scale; the reported rates and confidence intervals are calculated from the observed counts.

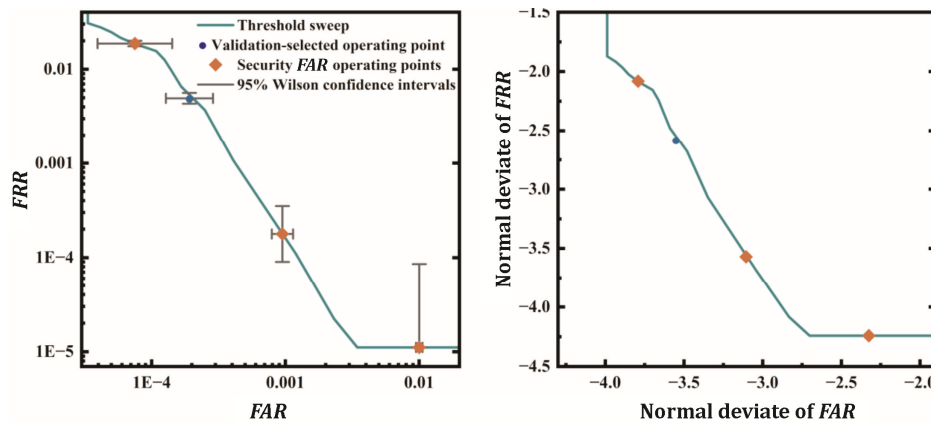


Fig. 6. Low-error authentication performance under threshold variation: (a) FAR-FRR tradeoff with 95% Wilson confidence intervals and security-critical FAR operating points; (b) DET representation of the same threshold sweep using normal-deviate axes.

Fig. 6 evaluates the proposed authentication method's low-error operating characteristics using an independent test set of 45,000 legitimate attempts and 120,000 attack attempts. As shown in Fig. 6a, tightening the decision threshold reduces FAR but increases FRR, revealing an explicit security-availability tradeoff. At operating points close to FAR levels of 10^{-2} , 10^{-3} , and 10^{-4} , the empirical FARs are approximately 1.0017%, 0.0950%, and 0.0075%, with corresponding FRRs of 0%, 0.0178%, and 1.8667%, respectively. Horizontal and vertical error bars represent the 95% Wilson confidence intervals of FAR and FRR. Fig. 6b shows the DET representation of the same threshold sweep using normal-deviate axes, which provides a clearer view of the low-error region. These results show that tightening the threshold can reduce FAR, but this improvement comes with increased FRR. Accordingly, the threshold should be selected according to the required security-availability balance rather than relying on a single attack-rejection rate.

4.4. Authentication performance

Fig. 7 examines how the *BER*-deviation statistic affects discrimination on the same independent test population. Scaling the deviation by its finite-sample uncertainty gives an area under the curve (AUC) of 0.99999, while the normalized absolute-deviation statistic in

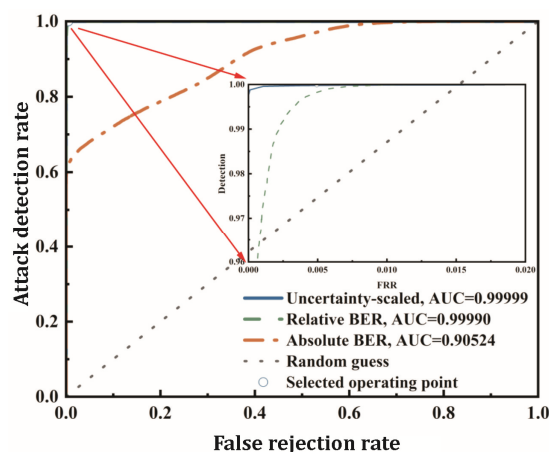


Fig. 7. Independent-test ROC comparison for three *BER*-deviation scores.

4.5. Path displacement

Fig. 8 presents the attack-rejection rate as a function of additional fiber length or path-distance displacement. Small displacements produce limited *BER* changes and constitute the most difficult detection case. The rejection rate exceeds 90% at approximately 1 km and

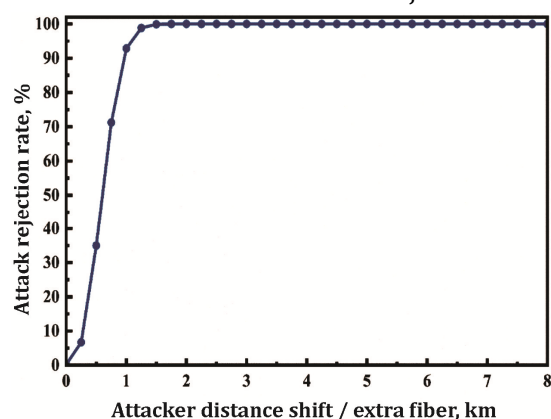


Fig. 8. Detection sensitivity to path-distance displacement.

4.6. Scenario robustness

Fig. 9a compares the decision-score distributions for legitimate access and nine active manipulations, and Fig. 9b reports the corresponding rejection rates with 95% Wilson intervals. Each attack class contains 30,000 observations. Distance change is rejected in 99.99% of attempts. Receiver-gain manipulation, ONU replacement with different noise characteristics, and combined distance-power changes yield rejection rates of 99.21%, 96.79%, and 95.70%, respectively. Transmitter-power variation, connector or insertion-loss manipulation, and temperature compensation are rejected in all simulated attempts; for each of these zero-miss results, the lower 95% Wilson bound is 99.987%. Optical-power compensation and model-based forcing of the measured *BER* toward the registered

Eq. (7) gives an AUC of 0.99990. The unnormalized absolute *BER* difference gives a lower AUC of 0.90524, consistent with its failure to account for the distance-dependent *BER* scale. The inset zooms in on the low-*FRR* region and identifies the operating point selected on the validation set. This ROC analysis summarizes ranking performance across all thresholds, whereas Fig. 6 reports the security-relevant error rates and confidence intervals.

approaches saturation beyond approximately 1.5 km. This result quantifies the sensitivity of the distance-induced *BER* fingerprint. The feature verifies consistency with the registered optical path rather than acting as an unclonable device identifier. Sub-kilometer path changes should therefore trigger longer observation windows or supplementary physical-layer verification.

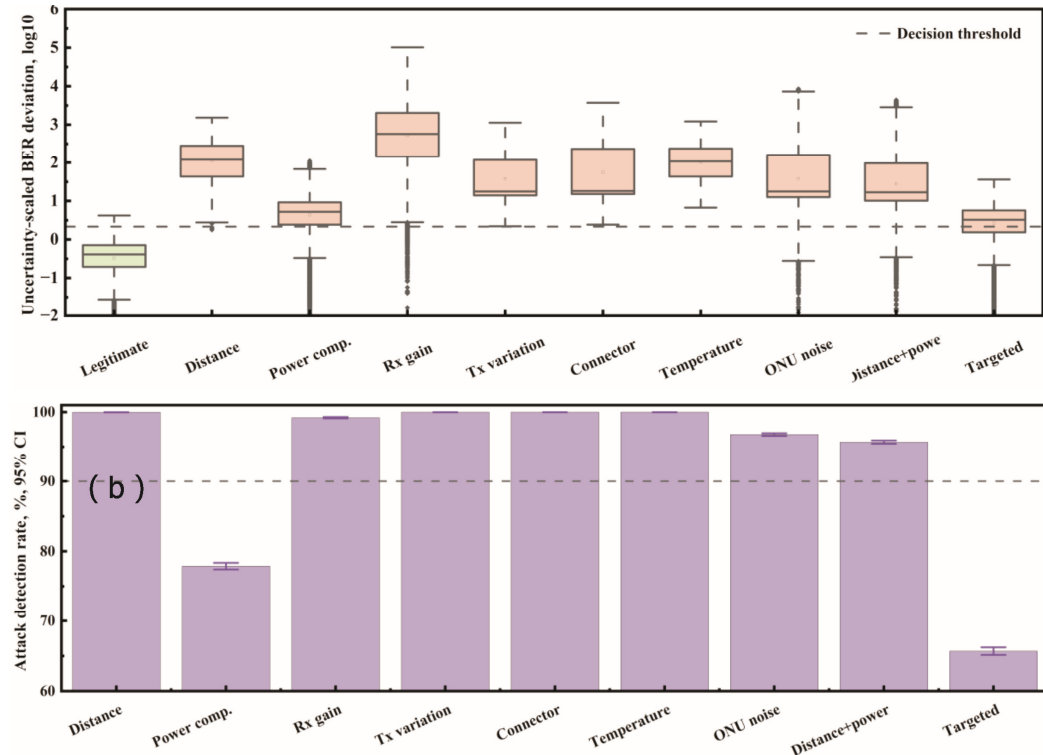


Fig. 9. Active-manipulation robustness: (a) legitimate and attack score distributions; (b) attack detection rates, $n=30,000$ per attack.

reference are the most difficult cases, with rejection rates of 77.88% and 65.68%, respectively. These results confirm that *BER* provides evidence of physical-path consistency but should remain combined with certificate, nonce, signature, and ledger verification in the complete scheme.

4.7. Consensus scalability

Fig. 10 compares PBFT and Raft using 4-25 consensus nodes. PBFT latency increases from approximately 6.6 to 12.2 ms, while throughput decreases from approximately 145 to 58 requests/s. Raft latency increases from approximately 4.5 to 5.8 ms, and throughput decreases from approximately 205 to 165 requests/s. The stronger dependence of PBFT on node count is

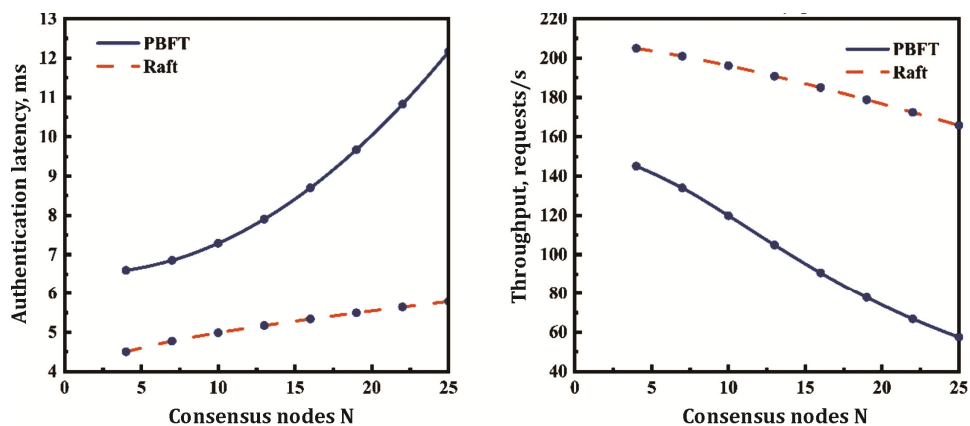


Fig. 10. Consensus scalability versus validator count: (a) end-to-end authentication latency; (b) throughput.

consistent with its multi-round broadcast process and approximately quadratic message complexity. Raft incurs less overhead but primarily tolerates crash failures and cannot address malicious validators. For a security-sensitive PON consortium with a limited validator set, PBFT provides Byzantine fault tolerance with millisecond-scale overhead.

5. Conclusions

This paper presents a trusted PON access authentication scheme that combines distance-conditioned *BER* channel fingerprinting with a permissioned blockchain. By anchoring authentication evidence, template digests, and authorization states on-chain via PBFT consensus, the proposed architecture links physical-path consistency assessment to auditable access control while retaining raw *BER* observations off-chain. On the independent simulated test set, the validation-selected threshold yields $FRR = 0.493\%$ and $FAR = 0.019\%$; the three *BER*-deviation scores yield AUC values of 0.99999, 0.99990, and 0.90524. The active-manipulation study identifies optical-power compensation and reference-forcing as the most difficult cases, with physical-layer *FAR* values of 22.12% and 34.32%, respectively. The *BER* fingerprint is therefore best viewed as a physical-path consistency factor that complements certificate-based authentication. Building on this simulation-based proof of concept, future work will validate the scheme on a physical OLT/ONU platform under device variability, burst-mode operation, temporal drift, and adaptive compensation attacks.

Funding. This research work was supported by the Special Fund of Advantageous and Characteristic Disciplines (Group) of Hubei Province. This work is supported by the Hubei Provincial Natural Science Foundation of China (Grant No. 2023AFB474, Grant No. 2024AFB881), the Anhui Provincial Special Project for Special Needs in Humanities and Social Sciences (Grant No. 2025AHGXSK50067), and the Postgraduate Quality Engineering Project of Anhui Province (Grant No. 2024jyxxggyjY232). Supported in part by the Scientific Research Project of Fuyang Normal University (Grant No. 2022KYQD0004). Supported by Special Project for Talent Development in Machinery Industry (Grant No. Cmitc2025087, Grant No. Cmitc2025066, Grant No. Cmitc2025090). This work is supported by the Jiangxi Provincial Natural Science Foundation (20232BAB212006). Supported by 2025 E-Commerce Research Project (No. CCPITCBEC-20251167) and 2025 Annual Project of the 14th Five-Year Plan for National Business Education Research (No. SKJYKT-2505186). This work is supported by the Anhui Provincial Quality Engineering Project (Grant No.: 2025xqhz041, 2025zytsai043).

Conflict of interest. Authors declare no conflict of interest.

Authors' contribution. Xiangqing Wang: Conceptualization, methodology, validation, and manuscript writing; Nannan Yu: Funding acquisition and project administration; Dongfei Wang: Software implementation and simulation; Xiaoling Cheng: Investigation and visualization; Nannan Yu: Resource support; Xiaokun Yang: Manuscript review and editing.

References

1. Li, J., Fan, R., He, Q., Luo, M., & Li, X. (2024). Bidirectional TFDM 200 G coherent PON with a simplified receiver at the ONU side. *Optics Letters*, 49(18), 5127–5130.
2. Moon, S.-R., & Bae, S. (2024). Coherent-lite PON with repetition code and single polarization receiver. *Optics Communications*, 557, Article 130331.
3. Zhou, J., Liu, Z., Guo, M., Wang, H., Liu, W., & Yu, C. (2024). Burst-mode digital signal processing for passive optical networks based on discrete multi-tone. *Optics Express*, 32(21), 37148–37154.
4. Furdek, M., Natalino, C., Di Giglio, A., & Schiano, M. (2021). Optical network security management: Requirements, architecture, and efficient machine learning models for detection of evolving threats. *Journal of Optical Communications and Networking*, 13(2), A144–A155.

5. Niu, Z., Xie, Y., Xu, G., Dai, C., Yang, H., Zeng, C., Shi, M., Li, L., Pu, G., Hu, W., & Yi, L. (2025). Experimental demonstration of integrated encryption and communication over optical fiber. *National Science Review*, 12(7), Article nwaf112.
6. Wu, Y., Zhang, Z., Luo, H., Deng, L., Yang, Q., Dai, X., Liu, D., Gao, X., Yu, Y., & Cheng, M. (2023). 100Gb/s coherent optical secure communication over 1000 km based on analog-digital hybrid chaos. *Optics Express*, 31(20), 33200–33211.
7. Huang, D., Deng, L., Yang, Q., Dai, X., Liu, D., Gao, X., Yu, Y., & Cheng, M. (2024). Hardware fingerprint authentication based on Siamese neural networks in PON. *IEEE Photonics Technology Letters*, 36(7), 508–511.
8. Wang, X., Zhang, H., Ren, L., Wu, Z., Wang, D., & Yang, X. (2024). Enhanced authentication technology based on deep neural network in the physical layer of optical communication. *Optical Fiber Technology*, 84, Article 103703.
9. Wu, K., Wang, H., & Ji, Y. (2022). Channel characteristics based adjustable fingerprint for identity authentication in WDM-PON with deep neural networks. *IEEE Photonics Journal*, 14(2), 1–11.
10. Tang, C., Zhang, Y., Liu, K., Yao, Y., Deng, L., Yang, Q., Liu, D., & Cheng, M. (2026). Delayed self-homodyne detection enabled optical fingerprint identification of ONUs in IMDD passive optical networks. *Optics Letters*, 51(7), 1828–1831.
11. Yao, Z., Mauldin, T., Heffernan, G., Xu, Z., Liu, M., & Wei, T. (2019). Low-cost optical fiber physical unclonable function reader based on a digitally integrated semiconductor LiDAR. *Applied Optics*, 58(23), 6211–6216.
12. Cao, B., Wang, Z., Zhang, L., Feng, D., Peng, M., Zhang, L., & Han, Z. (2023). Blockchain systems, technologies, and applications: A methodology perspective. *IEEE Communications Surveys & Tutorials*, 25(1), 353–385.
13. Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, 22(2), 1432–1465.
14. Afraz, N., & Ruffini, M. (2022). Trusted distributed marketplace for virtual passive optical network sharing. *Journal of Optical Communications and Networking*, 14(5), B22–B29.
15. Alemany, P., Muñoz, R., Martrat, J., Pastor, A., Díaz, R., Lopez, D., Casellas, R., Martínez, R., & Vilalta, R. (2023). Blockchain-based trust management collaborative system for transport multi-stakeholder scenarios. *Journal of Optical Communications and Networking*, 15(8), 488–496.
16. Fichera, S., Sgambelluri, A., Paolucci, F., Giorgetti, A., Sambo, N., Castoldi, P., & Cugini, F. (2021). Blockchain-anchored disaggregated optical networks. *Journal of Lightwave Technology*, 39(20), 6357–6365.
17. Pang, Y., Zhang, M., Wang, Y., Tang, M., Zhang, Y., Wu, Y., Zhang, C., Zhang, L., & Wang, D. (2024). Blockchain-enabled secure and reliable management for digital components in digital twin optical network. *Journal of Lightwave Technology*, 42(19), 6647–6661.
18. Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access*, 8, 18207–18218.
19. Novo, O. (2018). Blockchain meets IoT: An architecture for scalable access management in IoT. *IEEE Internet of Things Journal*, 5(2), 1184–1195.
20. Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy blockchain oracles: Review, comparison, and open research challenges. *IEEE Access*, 8, 85675–85685.
21. Wang, X., Li, Y., Zhao, Y., Lei, C., Zhang, H., & Zhang, J. (2020). Physical layer authentication based on BER measurement of optical fiber channel. *IEEE Access*, 8, 101812–101823.
22. Elfaki, A. A. A., Elobaid, R. A., Elamin, A. A., & Abd-Alla, M. D. (2017). The effect of temperature and laser type on optical fiber temperature coefficient. *American Journal of Optics and Photonics*, 5(1), 1–5.
23. Keiser, G. (2000). *Optical fiber communications* (3rd ed.). McGraw-Hill.
24. Agrawal, G. P. (2002). *Fiber-optic communication systems* (3rd ed.). Wiley-Interscience.
25. Montgomery, D. C., & Runger, G. C. (2019). *Applied statistics and probability for engineers* (7th ed.). John Wiley & Sons.
26. Venkatesan, C., Jeevanantham, S., & Rebekka, B. (2024). A lightweight physical layer authentication-based blockchain consensus mechanism for edge networks. *IEEE Transactions on Network and Service Management*, 22(2), 1594–1607.
27. Luo, H., Yang, X., Yu, H., Sun, G., Lei, B., & Guizani, M. (2023). Performance analysis and comparison of nonideal wireless PBFT and RAFT consensus networks in 6G communications. *IEEE Internet of Things Journal*, 11(6), 9752–9765.

Wang, X., Cheng, X., Wang, D., Yang, X., Yu, N. (2027). Trusted Passive Optical Networks Access Authentication Using Distance Conditioned Bit Error Rate Fingerprinting and a Permissioned Blockchain. *Ukrainian Journal of Physical Optics*, 28(1), 01063 – 01076.
doi: 0.3116/16091833/Ukr.J.Phys.Opt.2027.0163

Анотація. Щоб вирішити проблему клонування облікових даних та обмежених можливостей аудиту в пасивних оптичних мережах (PON), ми представляємо концепцію автентифікації доступу на основі моделювання. Вона інтегрує відбитки бітової частоти помилок (BER), обумовлені відстанню, з блокчейном із розмежуванням прав доступу. Шаблон залежності BER від відстані створюється в умовах зареєстрованого з'єднання. Під час автентифікації нормалізовані відхилення між BER у реальному часі до прямої корекції помилок та

зареєстрованими еталонними значеннями служать відбитками каналу для автентифікації фізичного рівня. Водночас адаптивний поріг, калібрований на основі змодельованих легітимних спостережень, оцінює узгодженість фізичного шляху. Непов'язувані підписані дані вимірювань підтверджують можливість аудиту авторизації через консенсус практичної візантійської відмовостійкості. На незалежному змодельованому тестовому наборі поріг, вибраний для перевірки, забезпечує коефіцієнт помилкового відхилення 0,493% та коефіцієнт помилкового прийняття 0,019%; показники відхилення BER, масштабовані з урахуванням невизначеності, дають значення площі під кривою 0,99999, 0,99990 та 0,90524 відповідно. Результати підтверджують доцільність методу в умовах моделювання; водночас апаратна валідація залишається необхідною, а компенсаційні атаки обмежують можливості розрізнення на основі BER.

Ключові слова: пасивна оптична мережа, автентифікація фізичного рівня, відбиток каналу, блокчейн із розмежуванням прав доступу, практична візантійська відмовостійкість.