Privacy-Enhanced Secure Neighbor Discovery for Wireless Networks

Ahmed Mohamed Hussain
Networked Systems Security (NSS) Group
KTH Royal Institute of Technology
Stockholm, Sweden
ahmed.hussain@ieee.org

Panos Papadimitratos
Networked Systems Security (NSS) Group
KTH Royal Institute of Technology
Stockholm, Sweden
papadim@kth.se

***Abstract*—We propose Privacy-Enhanced Secure Neighbor Discovery (PE-SND), a lightweight protocol that addresses the security and privacy needs of existing and emerging wireless networks. Traditional Secure Neighbor Discovery (SND) protocols effectively mitigate relay attacks but expose device identities and locations. Our protocol preserves SND security guarantees while enhancing privacy through pseudonymous authentication and encrypted location exchange. Formal verification confirms pseudonym unlinkability and location confidentiality against both external adversaries and honest-but-curious participants. Performance evaluation across security levels (96 to 256 bits) demonstrates feasibility with processing latencies of 14 to 75ms. Deployment of PE-SND using Ultra-Wide-Band (UWB) technology confirms sub-meter accuracy (15cm) in indoor Line-of-Sight (LoS) and 0.953m in Non-Line-of-Sight (NLoS) environments, with execution times up to 90ms. PE-SND provides a lightweight solution for privacy-demanding applications in the Internet of Things (IoT), Internet of Vehicles (IoV), and other emerging wireless ecosystems.**

***Index Terms*—Anonymity, Secure Neighbor Discovery, Security, Network Protocols, Privacy, Wireless Security**

I. Introduction

Wireless communications rely fundamentally on Neighbor Discovery (ND) protocols, which enable devices to identify peers they directly communicate with. These protocols are executed continuously across billions of devices in diverse applications, from healthcare monitoring systems to intelligent transportation networks. While 5G technologies [1] have significantly enhanced the capabilities of wireless networks, the underlying ND mechanisms present critical security-privacy concerns. This is particularly evident in Internet of Things (IoT) deployments, including Internet of Vehicles (IoV), Internet of Medical Things (IoMT), and Internet of Drones (IoD), where devices must establish secure connections while minimizing exposure of sensitive information about their identity, presence, and physical location.

Traditional ND protocols are vulnerable to various attacks, including eavesdropping, spoofing, Man-In-The-Middle (MITM), and relay or wormhole attacks ([2], [3]). While Secure Neighbor Discovery (SND) protocols effectively counter these threats through cryptographic primitives (i.e., authenticators) and precise distance measurements [3], they introduce significant privacy challenges: (i) Device identities and locations are exposed during discovery, possibly allowing participating devices tracking, (ii) Network topology becomes visible to observers, and (iii) Legitimate participants in the SND protocol can collect detailed location histories of their peers.

Current security frameworks, including IPsec, TLS, and cellular protocols, provide Authenticated ND (AND) with basic privacy features but fall short of proper SND, that is, the guarantee that a device is indeed a communication neighbor [4]–[6]. Recent privacy-enhancement proposals focus on MAC and IP address randomization ([7], [8]) yet fail to address fundamental SND requirements. The security-privacy gap in existing protocols becomes increasingly critical as networks permeate every aspect of our lives and location data grows more sensitive. We address these challenges by introducing Privacy-Enhanced SND (PE-SND), a lightweight protocol that preserves the security guarantees of SND while maintaining privacy by encrypting location information and using pseudonymous authentication, protecting against internal and external adversaries.

While there is the Privacy-Preserving SND (PP-SND) [6] that uses Homomorphic Encryption (HE), it introduces significant computational overhead, which is impractical for resource-constrained devices. For instance, implementing PP-SND on a typical IoT device increases protocol execution latency by a factor of 20 compared to plain/standard SND, severely impacting battery life and protocol responsiveness.

The **research question** that we address in this paper is: *Can we develop a variant that maintains essential privacy-preservation properties while achieving significantly lower computational cost?* To address this, we introduce PE-SND that is designed with efficiency in mind, trading off privacy protection, revealing location information to curious peers. Employing lightweight cryptographic primitives and pseudonymous authentication, PE-SND achieves unlinkability and confidentiality along with stronger security guarantees compared to the standard SND. This is essential for practical deployment in resource-constrained devices.

Contributions. (i) Analysis of privacy requirements for SND, establishing formal criteria for privacy-enhancing ND protocol; (ii) PE-SND: A novel efficient protocol that enhances SND with pseudonymous authentication and encrypted location information, effectively protecting against both ex-

979-8-3503-9281-4/25/$31.00 ©2025 IEEE

ternal and internal (honest-but-curious) adversaries; and (iii) Practical validation through performance evaluation across multiple security levels and a proof-of-concept implementation using Ultra-Wide-Band (UWB) technology, demonstrating the PE-SND feasibility in real-world IoT deployments.

Paper Organization. We examine classical Two-Party SND and its variants in Section II, followed by the security and privacy requirements for the PE-SND in Section III, while Section V details the protocol design. We provide performance evaluation and security analysis in Section VI and conclude in Section VII.

II. Neighbor and Secure Neighbor Discovery

ND serves as a fundamental building block in wireless networks, enabling devices to identify peers within their direct communication range. While AND protocols implement cryptographic security mechanisms through digital signatures and HMACs, they cannot independently verify physical proximity between devices–a vulnerability that exposes networks to relay attacks, with the adversary relaying packets between two non-neighbors, misleading them that they are neighbors. The adversarial relaying introduces Δ_{relay} delay; the lower the value, the more effective the adversary. To address this security gap, SND protocols have emerged ([4], [5]), categorized primarily into *Time-based (T)* and *Time-and-Location-based (TL)* variants:

T-based protocols establish proximity by measuring message propagation time for distance estimation. However, this approach exhibits inherent vulnerabilities to fast relay attacks, where adversaries can forward messages with minimal delay. Their effectiveness notably diminishes in environments with physical obstacles, where signal propagation can distort time-based distance measurements and potentially compromise security guarantees.

TL protocols improve security by integrating both timing data and geographical coordinates in their verification process. This dual-verification approach enables robust proximity verification by comparing measured Time of Flight (ToF) against calculated geographical distances. Through this combination, *TL* protocols achieve resilience against relay attacks while maintaining effectiveness in Non-Line-of-Sight (NLoS) conditions. The two primary *TL* protocol variants have distinct operational characteristics:

Beaconing (B-TL). In this variant, node $\mathcal{A}$ initiates discovery by broadcasting a beacon containing timestamp t_1 and location coordinates. Upon reception, at time t_2, node $\mathcal{B}$ verifies proximity through two mechanisms: computing ToF $(t_2 - t_1)$ and comparing it against the expected geographical distance. While this approach enables efficient one-way proximity verification, it requires precise time synchronization between participating nodes.

Challenge-Response (CR-TL). This variant implements a rapid challenge-response exchange between nodes, eliminating the need for synchronized clocks. Node $\mathcal{A}$ initiates with a timed challenge to node $\mathcal{B}$, requiring a response within a minimal delay. The protocol maintains security through lightweight cryptographic operations that prevent adversaries from gaining timing advantages while ensuring message authenticity.

The operational advantages of *TL* protocols become particularly evident in challenging environments: (1) They maintain effectiveness even when Δ_{relay} values are below typical detection thresholds; (2) Their dual-verification mechanism provides robust defense against sophisticated relay attacks; (3) Location verification helps validate proximity even in NLoS conditions; (4) The protocols adapt well to environments with signal propagation irregularities.

These characteristics make *TL* protocols particularly suitable for SND in any network environment. However, existing SND protocols face these challenges: (i) location information is not encrypted, and (ii) node identity is known to all protocol participants and non-participants. Hence, there is a need for privacy enhancements in protocol design and implementation.

Privacy-Preserving SND (PP-SND) addresses these privacy concerns through the use of public key authentication and Homomorphic Encryption (HE). Although the public key authentication and its overhead cannot be avoided in open dynamic networks, the use of HE introduces significant computational overhead, impractical for resource-constrained devices. As demonstrated in [6], implementing homomorphic operations increases protocol execution time by up to 20x compared to standard SND protocols. This processing overhead is particularly problematic for wireless sensors, IoT devices, and other constrained platforms, especially those where energy efficiency and response time are critical. The complexity of homomorphic operations required for encryption/decryption and secure distance calculation exceeds the practical limitations of many deployment scenarios, necessitating more lightweight approaches that balance privacy protection with implementation efficiency.

III. Security and Privacy Requirements for Privacy-Enhanced SND

This section discusses the core requirements for PE-SND protocol and examines their implementation challenges, reusing or differentiating from PP-SND requirements [6].

Fundamental Security Requirements. An effective SND protocol must satisfy two essential properties [5]:

P1 – Correctness: A device declared as a neighbor at time t must be a genuine communication neighbor at that moment. This ensures that devices $\mathcal{A}$ and $\mathcal{B}$ are identified as neighbors and are within communication range and capable of direct message exchange, guaranteeing that the discovered network topology accurately reflects actual communication capabilities.

P2 – Availability: The protocol must establish neighbor relationships for all distances within the specified network discovery range $\mathcal{R}_{\text{SND}}$, where $\mathcal{R}_{\text{SND}} \leq R$. Here, R represents the maximum theoretical communication range of the underlying radio or data link technology.

Privacy Enhancement Requirements. Beyond security, PE-SND protocol must additionally satisfy the following privacy requirements:

P3 – Pseudonymity: Devices must conceal their real identities during protocol execution, preventing both external adversaries and legitimate participants from determining true identities. This can be achieved through pseudonymity, utilizing temporary unlinkable identifiers for protocol interactions.

P4 – Confidentiality: The protocol must protect sensitive information, particularly location data, from unauthorized access and eavesdropping.

P5 – Unlinkability: Device participation in multiple discovery sessions must not be linkable, effectively preventing adversaries from tracking devices across different protocol executions.

IV. Adversarial Model

We consider both internal and external adversaries, following the model established in [6], with sophisticated yet realistic capabilities. The fundamental adversary is a relay attacker deploying one or two devices to compromise SND protocols executed between honest nodes. We extend this model to address adversaries that target privacy and availability, categorizing them based on their capabilities and objectives.

A. External Adversaries

External adversaries lack legitimate cryptographic credentials and attempt to extract or infer information about network participants through:

1) **Passive eavesdropping**: Collecting and analyzing SND protocol messages to extract neighbor relationships, node identities, and, in *TL* protocols, node locations.
2) **Active protocol initiation**: Initiating the SND protocol to measure distances (in *CR* protocols) or force location disclosure (in *CR-TL* protocols) from legitimate nodes.
3) **Session repetition**: Repeatedly initiating legitimate protocol sessions to accumulate fine-grained location and distance information about nodes within the network.
4) **Cross-session linking**: Analyzing information across multiple protocol executions to track specific nodes over time.

These adversaries may also target protocol availability by:

5) **Topology mapping**: Monitoring protocol executions to construct detailed maps of network topology and node movement patterns.

B. Internal (Honest-but-Curious) Adversaries

Beyond traditional adversaries, we consider *honest-but-curious* nodes that possess legitimate cryptographic credentials and execute the SND protocol, yet attempt to compromise privacy through:

6) **Protocol monitoring**: Eavesdropping on SND protocol executions between other nodes to extract sensitive information.
7) **High-rate protocol initiation**: Executing the SND protocol at a higher rate to accumulate fine-grained distance (*CR-T* protocols) and location (*CR-TL* protocols) data about peer nodes.

C. Protocol-Specific Security Considerations

SND protocols exhibit distinct security and privacy characteristics based on their design principles. **B** protocols offer complementary security and privacy advantages: temporally constrained operation imposes fundamental limitations on adversarial capabilities by requiring beacon transmission at predetermined intervals, while their broadcast-based communication model inherently protects privacy by complicating the identification of communication relationships. These temporal constraints render relay attacks technically infeasible when implementations employ sufficiently short transmission intervals. However, B protocols require precise clock synchronization between participating nodes, introducing both implementation complexity and potential vulnerabilities to synchronization manipulation attacks. Physical-layer distance-decreasing attacks ([9], [10]) present additional security considerations, beyond the scope here to be addressed in future work.

In contrast, **CR-TL** protocols offer security guarantees with more flexible implementation requirements. Combining challenge-response mechanisms with location verification effectively mitigates relay attacks even with minimal adversarial delay ($\Delta_{\text{relay}} > 0$). This is due to the dual-verification approach: measuring the ToF while simultaneously verifying location coordinates creates two independent verification vectors that an adversary must simultaneously compromise. Additionally, it eliminates the need for synchronized clocks, reducing deployment complexity and removing vulnerabilities associated with time synchronization attacks.

CR-TL protocols present a more adaptable base for privacy-enhanced implementation as they facilitate granular control over information disclosure. Through encryption of location data and incorporation of pseudonymous authentication, CR-TL protocols can be extended to satisfy both robust security requirements and comprehensive privacy protections. This flexibility enables them to be particularly suitable for privacy-demanding applications in dynamic network environments where both security and privacy guarantees must be simultaneously maintained.

These protocol-specific security considerations guide our PE-SND design (Section V). Specifically, our protocol adopts the CR-TL approach while incorporating pseudonymous authentication and encrypted location exchange to address the vulnerabilities identified in our adversarial model. This design protects against both external adversaries (attacks 1-5) and honest-but-curious participants (attacks 6-7), while maintaining the essential security properties of traditional SND.

V. Privacy-Enhanced Secure Neighbor Discovery Protocol

As mentioned earlier, traditional SND protocols lack confidentiality and are vulnerable to availability attacks. Adversaries can initiate the protocol without legitimate credentials, compromising both security and privacy. Our PE-SND protocol addresses the confidentiality and authentication vulnerabilities through two primary enhancements: pseudonymous authentication [11], [12] and encrypted location exchange.

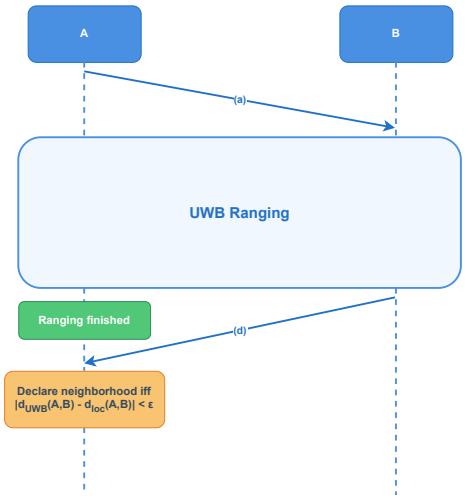

Fig. 1: Privacy-Enhanced *CR* TL-based SND protocol variant with UWB ranging.

The protocol initiates with an additional preliminary message from $\mathcal{A}$ containing its pseudonym, hashed nonce $h(n_1)$, and digital signature, providing pseudonymous authentication. Node $\mathcal{B}$ verifies the initial message signature using $pk_{\mathcal{A}}$ extracted from $\mathcal{A}$'s pseudonym. Following this, $\mathcal{A}$ initiates the ranging phase: using the UWB, it performs distance estimation based on ToF measurements. Fig. 1 illustrates the protocol, with the following messages:

(a) $\mathcal{A} \rightarrow * : \langle \mathcal{A}, h(n_1), auth_{\mathcal{A}}(n_1), PNYM(\mathcal{A}) \rangle$

(b) $\mathcal{A} \rightarrow \mathcal{B}$: UWB Ranging Message (includes n_1)

(c) $\mathcal{B} \rightarrow \mathcal{A}$: UWB Ranging Message (includes n_2)

(d) $\mathcal{B} \rightarrow \mathcal{A} : \langle \mathcal{B}, \mathcal{A}, n_1, n_2, auth_{\mathcal{B}}(\mathcal{A}, n_1, n_2, loc(\mathcal{B})), Enc_{pk_{\mathcal{A}}}(loc(\mathcal{B})), PNYM(\mathcal{B}) \rangle$

Final Step $\mathcal{A}$: Declare neighborhood iff $|d_{\text{UWB}}(\mathcal{A}, \mathcal{B}) - d_{\text{loc}}(\mathcal{A}, \mathcal{B})| < \epsilon$

After confirming that $\mathcal{A}$ is within communication range, $\mathcal{B}$ responds by transmitting its location encrypted with $pk_{\mathcal{A}}$, nonce, its own pseudonym, alongside an authentication token $auth_{\mathcal{B}}(\mathcal{A}, n_1, n_2, \text{location}(\mathcal{B}))$. Once $\mathcal{A}$ verifies the legitimacy of this message, it decrypts $\mathcal{B}$'s coordinates and establishes neighborhood only if the distance discrepancy satisfies $|d_{\text{UWB}}(\mathcal{A}, \mathcal{B}) - d_{\text{loc}}(\mathcal{A}, \mathcal{B})| < \epsilon$.

A. Privacy and Security Analysis

The security properties of PE-SND are fulfilled, inherited from the proven secure SND [5]. Here, we consider the protocol privacy properties using ProVerif [13] with an automated cryptographic protocol verifier: (i) location data confidentiality and (ii) cross-session unlinkability. Message exchange and cryptographic operations were modeled within the symbolic framework, considering a Dolev-Yao adversary model.

Verification summary:
Query event(linkPseudonyms(p1, p2)) ==> p1 = p2 is **true**.
Query not attacker(loc_B[]) is **true**.

The first property demonstrates pseudonym unlinkability across multiple protocol sessions, effectively preventing tracking attacks. The second property confirms that $\mathcal{B}$'s location (sent to $\mathcal{A}$ to compute $\text{d}_{\text{loc}}(\mathcal{A}, \mathcal{B})$) remains confidential against both passive and active adversaries, even those capable of message interception and manipulation.

We address the attacks identified in Section IV. For external adversaries, the pseudonymous authentication prevents unauthorized mapping of node relationships by passive eavesdropping (attack 1). The pseudonymous authentication of the initial message mitigates active protocol initiation attacks (attack 2) by rejecting participation requests from entities without valid credentials.

For session repetition and cross-session linking (attacks 3-4), the protocol can facilitate authentication token freshness verification and pseudonym rotation mechanisms, ensuring that distinct protocol executions cannot be linked. For topology mapping (attack 5), PE-SND encrypts location data using the recipient's public key ($\text{Enc}_{pk_{\mathcal{A}}}(\text{loc}(\mathcal{B}))$), preventing adversaries from constructing network topology maps.

Regarding honest-but-curious adversaries engaging in protocol monitoring (attack 6), our formal verification confirms that encrypted location information remains confidential even to legitimate participants of other protocol sessions. As for the high-rate protocol initiation (attack 7), the implementation of session-specific nonces and authentication tokens prevents information reuse across sessions, while pseudonym unlinkability thwarts attempts to build movement profiles.

VI. Implementation and Performance Evaluation

We implemented PE-SND using Python 3.11 with Elliptic Curve Cryptography (ECC) optimized for resource-constrained environments. Our implementation supports four security levels through distinct elliptic curves: SECP192R1 (96-bit), SECP256K1 (128-bit), SECP384R1 (192-bit), and SECP521R1 (256-bit). For secure message exchange, we employed Elliptic Curve Digital Signature Algorithm (ECDSA) with SHA-256 for digital signatures and ECC for message encryption.

A. Simulation Analysis

We evaluated the protocol through extensive simulations comprising 10,000 executions per security level, measuring processing latency for both protocol participants through the complete discovery process. Fig. 3 illustrates the execution times across all security levels. At 96-bit security, $\mathcal{A}$'s operations required $14.07 \pm 0.02ms$ while $\mathcal{B}$'s completed in $8.13 \pm 0.01ms$. The 128-bit security configuration demonstrated moderate increases to $18.57 \pm 0.03ms$ and $11.97 \pm 0.02ms$ for $\mathcal{A}$ and $\mathcal{B}$, respectively. Higher security

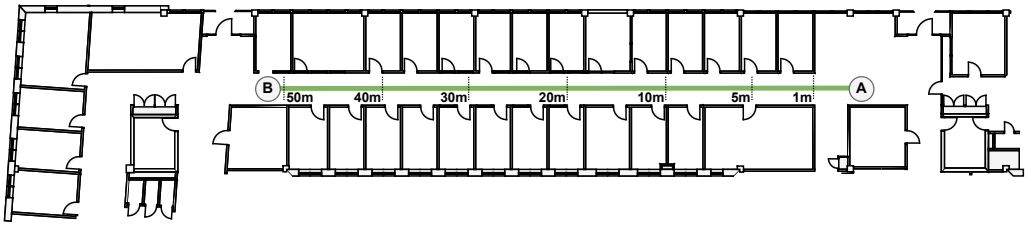

Fig. 2: Experimental setup for Line of Sight (LoS) performance evaluation. Devices A and B are positioned at measured intervals ($1m$ to $50m$) along a corridor to assess ranging accuracy and protocol execution under controlled conditions. The setup enables precise distance verification and timing measurements for protocol validation.

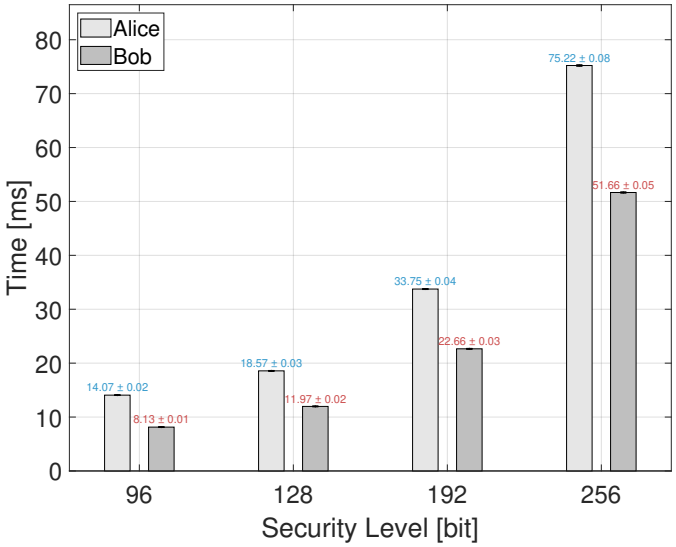

Fig. 3: Average execution time of the PE-SND protocol for Alice ($\mathcal{A}$) and Bob ($\mathcal{B}$) across four different security levels (96, 128, 192, and 256-bit).

levels exhibited expected computational trade-offs, with 256-bit security requiring $75.22\pm0.08ms$ for $\mathcal{A}$ and $51.66\pm0.05ms$ for $\mathcal{B}$.

The results demonstrate consistent asymmetry between $\mathcal{A}$'s and $\mathcal{B}$'s execution profiles, with $\mathcal{A}$'s operations incurring approximately 45% higher latency. This asymmetry arises from their distinct protocol roles: as the initiator, $\mathcal{A}$ performs additional message processing operations. The implementation maintains practical feasibility across all security levels, with execution times below $80ms$ even at the maximum security, 256-bit setting, indicating suitability for diverse IoT applications. For our proof-of-concept, we selected the 128-bit security level, which balances security requirements with performance constraints.

B. Hardware Implementation and Validation

To validate real-world applicability, we developed a proof-of-concept implementation using commercially available hardware, combining precise ranging with resource-constrained processing. Our experimental platform integrated a DWM1000 UWB module with a Raspberry Pi 4. The DWM1000 module, based on Decawave's DW1000 chip and operating in the 6.5 GHz band, delivers ranging accuracy within 10cm through precise ToF measurements, maintaining robust performance even in challenging indoor multipath environments. Our implementation executes PE-SND with: (i) **Ranging** (messages (b) and (c)): The DWM1000 module performs ToF-based measurements via SPI interface with the Raspberry Pi, incorporating multiple readings with environmental parameter compensation for reliable proximity verification; and (ii) **Cryptographic operations** (messages (a) and (d)): Pseudonymous authentication, pseudonym exchange, location encryption, and message nonces.

We evaluated protocol performance in two deployment scenarios, particularly LoS and NLoS conditions. Tests along a 50-meter corridor, depicted in Fig. 2, demonstrated excellent precision in LoS environments, with measured distances close to reference values, with maximum deviations below $15cm$ (Fig. 4). NLoS experiments showed predictably increased variation, with a maximum observed error of $0.953m$ (Fig. 5).

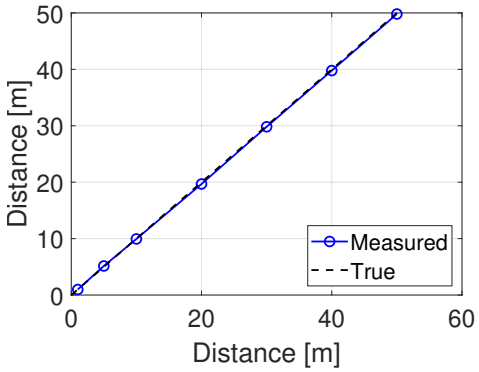

Fig. 4: LoS ranging performance analysis showing measured versus true distances across the $50m$ test range.

Fig. 6 presents the complete protocol execution times, including all cryptographic operations, message processing, and network communication overhead. The initiator ($\mathcal{A}$) demonstrated a mean execution time of $80.6\pm7.6ms$, while the responder ($\mathcal{B}$) exhibited a better performance at $49.2\pm2.6ms$. The notable difference in the 95% CI ($7.6ms$ for $\mathcal{A}$ versus $2.6ms$ for $\mathcal{B}$) indicates that the initiator additional processing is more susceptible to performance variations.

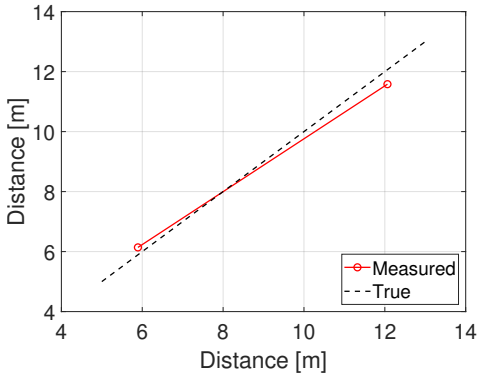

Fig. 5: NLoS performance characterization comparing measured and true distances in challenging environments.

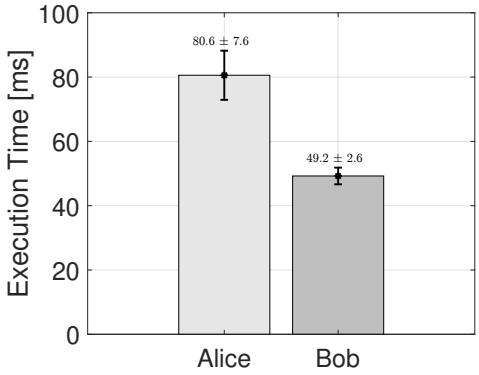

Fig. 6: PE-SND protocol execution time including network transmission overhead with 95% Confidence Interval (CI) for two Raspberry Pi's (each representing $\mathcal{A}$ and $\mathcal{B}$) executing PE-SND with 128-bit security level in real-world network conditions.

These experimental results validate PE-SND's practicality, with significantly reduced overhead compared to PP-SND trading off privacy protection. It demonstrates consistent submeter accuracy in LoS conditions and reliable performance even in challenging NLoS environments. With execution times compatible with IoT application requirements, PE-SND effectively balances security and privacy requirements with practical implementation constraints in diverse wireless network environments.

VII. Conclusion

This paper introduced Privacy-Enhanced SND (PE-SND), a lightweight, Secure Neighbor Discovery (SND) protocol that addresses essential confidentiality and availability limitations in existing SND protocols. We demonstrated that privacy enhancement can be effectively integrated with SND without compromising protocol performance or security guarantees. Our experimental validation confirms the protocol efficiency across multiple security levels (96 to 256 bit), with execution times remaining within practical bounds (up to 90ms) even for resource-constrained environments. The protocol maintains all the needed security and privacy properties (formally verified) while introducing minimal computational overhead, making it suitable for deployment in emerging wireless ecosystems, including IoT, IoV, and various other wireless networks. Implementation results from both simulation and hardware-based proof-of-concept demonstrate the protocol's resilience in both LoS and NLoS deployment scenarios, maintaining submeter accuracy and acceptable performance. For future work, we aim to evaluate the protocol reliability, and scalability in a larger setting where multiple nodes are deployed in the network

Acknowledgment

This work is supported in parts by the Swedish Research Council (VR) and the Knut and Alice Wallenberg (KAW) Foundation. The authors would like to thank Hongshuo Yi for his assistance with conducting the experiments.

References

[1] U. Pingle, "5G Means Big Changes for Large Public Venues in 2023 and Beyond." https://www.commscope.com/blog/2023/5g-means-big-changes-for-large-public-venues-in-2023-and-beyond/, Jan 2023.

[2] A. AlSa'deh and C. Meinel, "Secure Neighbor Discovery: Review, Challenges, Perspectives, and Recommendations," *IEEE Security & Privacy*, vol. 10, no. 4, pp. 26–34, 2012.

[3] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Čapkun, and J.-P. Hubaux, "Secure Neighborhood Discovery: A Fundamental Element for Mobile Ad Hoc Networking," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 132–139, 2008.

[4] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Secure Neighbor Discovery in Wireless Networks: Formal Investigation of Possibility," in *Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security*, pp. 189–200, 2008.

[5] M. Poturalski, P. Papadimitratos, and J.-P. Hubaux, "Formal Analysis of Secure Neighbor Discovery in Wireless Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 10, no. 6, pp. 355–367, 2013.

[6] A. M. Hussain and P. Papadimitratos, "Privacy-Preserving Secure Neighbor Discovery for Wireless Networks," in *IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, (Sanya, China), December 2024.

[7] J. Hugon, M. Cunche, and T. Begin, "RoMA: Rotating MAC Address for privacy protection," in *Proceedings of the SIGCOMM'22 Poster and Demo Sessions*, pp. 31–33, 2022.

[8] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A study of MAC address randomization in mobile devices and when it fails," *arXiv preprint arXiv:1703.02874*, 2017.

[9] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks," in *Security and Privacy in Ad-Hoc and Sensor Networks: Third European Workshop, ESAS 2006*, pp. 83–97, Springer, 2006.

[10] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures," *IEEE Transactions on Wireless Communications (IEEE TWC)*, vol. 10, pp. 1334–1344, April 2011.

[11] P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure Vehicular Communication Systems: Design and Architecture," *IEEE Communications Magazine*, vol. 46, pp. 100–109, November 2008.

[12] M. Khodaei, H. Noroozi, and P. Papadimitratos, "Scaling Pseudonymous Authentication for Large Mobile Systems," in *ACM Conference on Security & Privacy in Wireless and Mobile Networks (ACM WiSec)*, (Miami, FL, USA), pp. 174–185, May 2019.

[13] B. Blanchet, "ProVerif: Cryptographic protocol verifier in the formal model," 2001–2025. Software tool and documentation available online.