This is an electronic reprint of the original article.
This reprint may differ from the original in pagination and typographic detail.

Liu, Shushu; Yan, Zheng; Kantola, Raimo

Privacy-preserving D2D Cooperative Location Verification

Published in:
2021 IEEE Global Communications Conference, GLOBECOM 2021 - Proceedings

DOI:
[10.1109/GLOBECOM46510.2021.9685993](https://doi.org/10.1109/GLOBECOM46510.2021.9685993)

Published: 01/02/2022

Document Version
Peer reviewed version

Please cite the original version:
Liu, S., Yan, Z., & Kantola, R. (2022). Privacy-preserving D2D Cooperative Location Verification. In *2021 IEEE Global Communications Conference, GLOBECOM 2021 - Proceedings* IEEE.
<https://doi.org/10.1109/GLOBECOM46510.2021.9685993>

This material is protected by copyright and other intellectual property rights, and duplication or sale of all or part of any of the repository collections is not permitted, except that material may be duplicated by you for your research use or educational purposes in electronic or print form. You must obtain permission for any other use. Electronic or print copies may not be offered, whether for sale or otherwise to anyone who is not an authorised user.

Privacy-preserving D2D Cooperative Location Verification

Shushu Liu¹, Zheng Yan^{1,2}, Raimo Kantola¹

¹*Department of Communications and Networking, Aalto University, Espoo, Finland*

²*State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an, China*
liu.shushu@aalto.fi, zyan@xidian.edu.cn, raimo.kantola@aalto.fi

Abstract—Device-to-Device (D2D) cooperative location verification allows a device to verify its location with the help of neighbouring devices. It is especially handy in location-based services where location verification is essential. However, the exposure of device location during verification rises a big privacy risk for participants since they have to send their real-time locations to unknown verifiers holding anonymous identities. Thus, a privacy-preserving solution is urgently needed to provide verification without location disclosure. Traditional solutions based on Paillier and garbled circuits can solve the problem but also introduce high cost. Based on order-preserving encryption, we propose an efficient protocol with high-security guarantee to address this issue. Apart from rigorous security proof, complexity analysis and extensive experiments are also conducted to evaluate the proposed solution. The results compared with related work show that order-preserving encryption based mechanism achieves the best balance with regards to privacy, utility and performance requirements.

Index Terms—D2D cooperative location verification, security and privacy, order-preserving encryption, high efficiency

I. INTRODUCTION

The popularity of D2D communication stimulates its application in many fields, one of which is location verification. Location verification is an essential process to check the integrity and reliability of localization. It is an effective solution for spoofing attack in Global Positioning System (GPS) and noise interference detection in 5G base station localization. Khandker, Torres-Sospedra and Ristianiemi [1] presented a result with 44% reduction in positioning error by verifying the computed location with nearby devices.

The core concept of D2D cooperative location verification is straightforward. It compares measured distance and computed distance between a device with uncertain location and neighbouring devices. Specifically, when a device (known as UE) wants to check its location obtained from a localization service provider, it initials a query to nearby devices (known as A-UE). By measuring the time difference between query and response, it calculates the measured distance, supposing the message travels at the speed of light. At the same time, it calculates the Euclidean distance (known as computed distance) according

to their locations. The location verification can be confirmed once these two distance difference is under some threshold.

Although D2D cooperative location verification simplifies verification process substantially, the disclosure of location information during verification rises a big privacy risk for participating assistant devices (A-UEs) since they have to send their real-time locations to another device (UE) while the holder of this device is unknown and could be malicious. In this case, it threatens not only location privacy but also personal safety of assistants. Research shows that 46% of teen users and 35% of adults turn off location sharing due to privacy concern [2]. Thus, a privacy-preserving scheme for D2D cooperative location verification is highly needed.

Mainstream solutions to location privacy protection can be classified into three categories: access control, obfuscation and cryptography [3]. Here, we only focus on cryptography based solutions as it can meet the high-level privacy and accuracy demands at the same time. Paillier encryption and garbled circuit are two popular cryptographic tools that can be applied for this problem. The idea of Paillier based method [4] is easy to implement. By taking advantage of the homomorphic addition property of Paillier, we can compute distance (d_c) between UE and A-UE in the ciphertext and then compare it with measured distance (d_m). The design of garbled circuits [5] can be implemented with circuits modules which fulfill the multiply, add, comparison, and or operations. However, these solutions are not feasible in practice owing to their high overheads.

This paper is dedicated to providing an efficient solution with high-level privacy guarantee. Different from the traditional verification method which is based on distance comparison, we introduce an innovative coordinate based verification method. Besides, an efficient privacy-preserving protocol for interval query is designed based on order-preserving encryption. The privacy-preserving location verification can be easily achieved by applying the designed interval query on the coordinates based verification method. Apart from the security and complexity analysis, this paper also compares the proposed protocol with Paillier and garbled circuits based solutions. The results show that the order-preserving encryption based protocol achieves the best balance between privacy and efficiency. Paillier based protocol provides high privacy while presenting the highest online latency and the extensibility decreases drastically with the increasing of verification rounds. Garbled

This work is sponsored in part by the Academy of Finland under Grant 308087 and Grant 335262; in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Shaanxi Innovation Team Project under Grant 2018TD-007; and in part by the 111 Project under Grant B16037.

Fig. 1: Overview of D2D Cooperative Location Verification

circuits based scheme shows a fair performance with online latency while the high computation and communication cost limits its application in resource-constrained environments. To summarize, the contribution of this paper is as follows.

- To the best of our knowledge, this is the first work targeting privacy protection in D2D cooperative location verification.
- An efficient scheme based on order-preserving encryption is presented and implemented.
- Comprehensive analysis and extensive experiments are conducted to evaluate the performance of the proposed protocol. The comparison results show that the proposed protocol achieves the best balance with regards to privacy, utility and performance.

The rest of the paper is organized as follows. The problem definition and threat model of privacy-preserving D2D location verification are defined in Section II. Order-preserving encryption is briefly introduced in Section III. The solution based on order-preserving encryption is presented in Section IV. Complexity analysis and experiments compared with related work are illustrated in Section V. Section VI reviews the related work about location privacy. In the end, we wrap up with the conclusions and future work in Section VII.

II. PROBLEM STATEMENT

This section demonstrates the definition and security model of privacy-preserving D2D cooperative location verification.

A. Privacy-preserving D2D Cooperative Location Verification

D2D cooperative location verification has been extensively used in such scenarios as VANET and indoor positioning. Despite its variety, a general idea is to verify the distance with a nearby device by comparing the measured distance with computed distance based on known locations. Fig. 1 presents an overview of D2D cooperative location verification which happens between user equipment (UE) and assistant user equipment (A-UE). To do this, UE initiates a request to a nearby device (A-UE) for its location. Once A-UE accepts the request, it immediately responds with its location to UE and UE can easily calculate their distance (d_c) based on these two locations. At the same time, it also measures the distance between them by the time difference (ToA) between the query and response ($d_m = c \times ToA / 2$), supposing the signal travels at the speed of light c . If the difference between d_c and d_m is under a threshold θ , which is influenced by signal noise and request processing time, the verification is completed with success. Otherwise, the location should be recalculated.

Although this simplifies verification process substantially, it rises a big privacy risk for A-UEs with location disclosure since A-UEs have to send their real-time locations to another device (UE) while the holder of this device is unknown and could be malicious. Thus, a privacy-preserving scheme for D2D cooperative location verification is highly needed. For simplicity, a formal definition is given below.

Definition 1 (Privacy-preserving D2D Cooperative Location Verification). Given the measured distance d_m , UE verifies its location (x, y) with the assistance of A-UE with location (x_a, y_a) . Mutual privacy is required for both UE and A-UE during the verification which means the sensitive information should be revealed to nobody except the owner. The result fulfills the requirement of D2D cooperative location verification only if $|d_c - d_m| < \theta$, where $d_c = \sqrt{(x - x_a)^2 + (y - y_a)^2}$, $d_m = c \times ToA / 2$ and θ is an experience value related to signal noise and processing delay.

B. Security Model

1) *Assumptions*: We take the localization service provider (LSP) as a *trusted party* providing localization services for its users. Because LSP is normally endorsed by big organizations or governments, it is against its benefit cheating its users as a service provider. However, the service provided by LSP could be inaccurate and influenced by many factors such as spoofing attacks or Non-Line-of-Sight (NLOS) interference. Also, we suppose there is a reliable communication channel between LSP and its end users which can be easily set up by encrypted channel. Therefore, the communication between LSP and its end-user is secure and trusted. In contrast, as an open network, the participants in D2D location verification are random and anonymous, the communication channel is vulnerable and easily under attacks. Therefore, it is essential to provide privacy protection mechanisms while preserving smooth location verification.

2) *Threat model*: We assume that both UE and A-UE are *semi-honest*, which means that they follow the verification scheme exactly, but may try to infer as much as possible about the other party's personal information. *From UE's perspective, the verification should proceed without compromising its information like location, the measured distance and threshold. From A-UE's perspective, its location is sensitive and should be kept secret. It is also noteworthy that intermediate values generated from the computation should be kept secret from both sides, for example, the computed distance, while the verification result can be revealed to UE.*

Just to highlight, this paper focuses on privacy protection and we suppose UE and A-UE are both semi-honest. A-UE sending a fake location is considered as a malicious active attack and is out of scope of this paper. It can be considered in the future, but would probably require more A-UE's interactions.

III. ORDER PRESERVING ENCRYPTION

Order preserving encryption (OPE) is a symmetric-key algorithm with order-preserving property, where the orders of

Fig. 2: Coordinates based Location Verification

ciphertexts are the same as the orders of their plaintexts. This property enables sorting and ranking on encrypted data without revealing plaintexts. This paper adopts the implementation proposed in [6]. It encrypts the values with linear computation so that the values can be disguised while the order of the values can still be preserved. It consists of three main parts: key generation, encryption and decryption, as described below.

Key Generation (KG): It generates a key pair (k, r) , where k and r are both random integers with $k \in \mathbb{Z}$ and $0 \leq r < k$. As a symmetric-key algorithm, the key is used for both encryption and decryption.

Encryption (EN): For value m , the encryption function is defined as $E(m) = k \times m + r$. The security of OPE is defined with indistinguishability under Ordered Chosen-Plaintext Attacks (IND-OCPA), an adversary cannot deduce any information about the plaintexts except the order when ciphertext space is at least three times bigger than the plaintext space [6].

Decryption (DE): For ciphertext c , the decryption function is defined as $D(c) = (c - r)/k$.

IV. ORDER-PRESERVING ENCRYPTION BASED LOCATION VERIFICATION

We first introduce our innovated coordinates based location verification. Based on it, an efficient privacy-preserving location verification can be implemented.

A. Coordinates Based Location Verification

Intuitively, instead of computing the distance, we focus on the coordinates directly, as shown in Fig 2. Likewise, UE is in possession of uncertain location (x, y) , measured distance d_m and noise effect θ , while A-UE is in possession of (x_a, y_a) . A-UE must locate in the grey area to valid a successful location verification. A formal definition is presented below.

Definition 2 (Coordinates Based Location Verification). Given measured distance d_m and θ , UE verifies its location (x, y) successfully with A-UE (x_a, y_a) once

$$x_a \in (x - d_m - \theta, x - d_m + \theta) \cup (x + d_m - \theta, x + d_m + \theta)$$

and

$$y_a \in (y - d_m - \theta, y - d_m + \theta) \cup (y + d_m - \theta, y + d_m + \theta).$$

Observing the definition, the problem can be dissolved into four Interval Query (IQ) problems when a value is from A-UE and the interval is set by UE. The tricky point is how

to proceed with the IQ without any information leakage from both sides.

Algorithm 1: Privacy-preserving Interval Query (IQ)

Result: True or False

Input: UE: (a, b) A-UE: c ;

Init: UE generates (k_u, r_u) ; A-UE generates (k_a, r_a) ;

Step1: (UE)

1.1: $E_1 = k_u * a + r_u, E_2 = k_u * b + r_u$;

1.2: send E_1, E_2 to A-UE;

Step2: (A-UE)

2.1: accept E_1, E_2 ;

2.2: $E_3 = k_a * E_1 + r_a, E_4 = k_a * E_2 + r_a$;

2.3: $E_5 = k_a * c + r_a$;

2.4: send E_5 to UE ;

Step3: (UE)

3.1: accept E_5 ;

3.2: $E_6 = k_u * E_5 + r_u$;

3.3: send E_6 to A-UE;

Step4: (A-UE)

4.1: accept E_6 ;

4.1: if $E_6 \in (E_3, E_4)$: True else: False;

4.2: send result to UE;

Step3: (UE)

5.1: accept result;

Algorithm 2: OPE based Privacy-preserving Location Verification

Result: True or False (UE)

Input: UE: $(x, y), d_m, \theta$ A-UE: (x_a, y_a) ;

Init: UE generates (k_u, r_u) ; A-UE generates (k_a, r_a) ;

1: $R_1 = IQ$ (UE: $(x - d_m - \theta, x - d_m + \theta)$, A-UE: x_a);

2: $R_2 = IQ$ (UE: $(x + d_m - \theta, x + d_m + \theta)$, A-UE: x_a);

Init: UE generates (k'_u, r'_u) ; A-UE generates (k'_a, r'_a) ;

3: $R_3 = IQ$ (UE: $(y - d_m - \theta, y - d_m + \theta)$, A-UE: y_a);

4: $R_4 = IQ$ (UE: $(y + d_m - \theta, y + d_m + \theta)$, A-UE: y_a);

5: if $(R_1 \vee R_2) \wedge (R_3 \vee R_4)$: True else: False;

B. Order-preserving Encryption Based Location Verification

Alg. 1 is the process of privacy-preserving interval query, which plays as a fundamental algorithm to realize coordinates based location verification. We suppose that interval (a, b) is held by UE, and value c is held by A-UE, the result is True when $c \in (a, b)$, otherwise False. The process is easy to understand. UE and A-UE start with initializing their key pairs according to order preserving encryption. Then, both parties will encrypt their messages with their keys and send them to the other party for double encryption. For example, UE first encrypts its interval (a, b) with its own key (k_u, r_u) and sends ciphertexts $E_u(a, b)$ to A-UE. A-UE double encrypts it with (k_a, r_a) and sends the ciphertext $E_a(E_u(a, b))$ to UE. At the same time, A-UE encrypts its value c with its key and sends to UE for double encryption. The result is True only if

the double encrypted c is located in double encrypted interval (a, b) , which is $E_a(E_u(a)) < E_u(E_a(c)) < E_a(E_u(b))$ as shown in the correctness proof below.

With interval query, it is straightforward to implement privacy-preserving location verification based on coordinates comparison. We achieve it by simply calling Alg. 1 four times and combining the results. We present the algorithm in Alg. 2. Note that IQ is the abbreviation of interval query and the key needs to be updated every time for x_a and y_a .

C. Correctness Analysis

The correctness of privacy-preserving location verification can be proved by the correctness of interval query since location verification is just repeating calling of interval query. Thus, we just need to prove the correctness of Alg. 1. The proof is presented in the following theorem.

Theorem 1. *Given (a, b) and c , if $c \in (a, b)$, there is always $E_u(E_a(c)) \in (E_a(E_u(a)), E_a(E_u(b)))$, where E_a and E_u are OPE encryption function with key pair (k_a, r_a) and (k_u, r_u) .*

Proof. We first prove that if $c > a$, then $E_u(E_a(c)) > E_a(E_u(a))$. By substituting E with its encryption function, we have

$$\begin{aligned} E_u(E_a(c)) - E_a(E_u(a)) &= k_u(k_a c + r_a) + r_u - (k_a(k_u a + r_u) + r_a) \\ &= k_u k_a (c - a) + k_u r_a - k_a r_u + r_u - r_a \end{aligned}$$

Since $c > a, 0 < r_a < k_a, 0 < r_u \leq (k_u - 1)$, it is easy to prove that

$$\begin{aligned} k_u k_a (c - a) + k_u r_a - k_a r_u + r_u - r_a &> k_u k_a - k_a (k_u - 1) - k_a = 0 \end{aligned}$$

Thus, $E_u(E_a(c)) > E_a(E_u(a))$ is proved.

Similarly, we can prove that if $b > c$, then $E_a(E_u(b)) > E_u(E_a(c))$. Thus if $a < c < b$, then $E_a(E_u(a)) < E_u(E_a(c)) < E_a(E_u(b))$. $\square$

D. Security Analysis

The security of location privacy is also guaranteed by the security of interval query which is presented in the following.

Theorem 2. *Based on order-preserving encryption, privacy-preserving interval query is secure against semi-honest adversary attack.*

Proof. From the point view of UE, A-UE can be an adversary who is interested in inferring UE's interval set (a, b) . In Alg. 1, UE sends E_1 and E_2 to A-UE where $E_1 = k_u * a + r_u, E_2 = k_u * b + r_u$. Since the values obtained by A-UE are actually masked by random number (k_u, r_u) generated from a sufficiently large domain, the data reveals no information about a or b . Besides, A-UE is also unable to guess (k_u, r_u) by solving a linear system which is $E_1 = k_u * a + r_u, E_2 = k_u * b + r_u$, when there are more variables than equations.

When UE is an adversary device, it tries to extract any information about A-UE's value c . In the algorithm, UE

obtains E_5 from A-UE where $E_5 = k_a c + r_a$. However, without key (k_a, r_a) , UE is unable to reveal c from E_5 either and it is also unable for UE to guess (k_a, r_a) by solving the linear system. $\square$

TABLE I: Security Strength and Recommended Key Size

Security Strength	Paillier	OPE	Garbled Circuits
Short	1024	112	112
Medium	2048	128	128
Long	3072	196	196

TABLE II: Complexity Analysis of Three Schemes

	Computation Cost		Communication Cost
	UE	A-UE	
PAI	2EN, 2MUL, 4ADD	3EN, 1DE	5L
OPE	10EN	10EN	14L
GCC	8CMP, 6AND, 1OR	8CMP	(96t+21)L

PAI: EN, MUL, ADD and DE refer to Paillier encryption, homomorphic multiplication, homomorphic addition and decryption; OPE: EN refers to OPE encryption; GCC: CMP, AND and OR refer to two party computation circuit block CMP, AND and OR; L is the bitlength of ciphertext according to the security strength; t is the bitlength of location values.

V. PERFORMANCE EVALUATION

This section presents the performance evaluation both theoretically and experimentally. The comparison methods are implemented based on Paillier encryption and garbled circuit respectively. The idea of Paillier based method is to compute distance (d_c) between UE and A-UE in the ciphertext and then compare it with measured distance (d_m). The design of garbled circuits is also based on coordinates comparison with three circuits modules which fulfill the Comparison, AND and OR operation. With these modules, we can easily implement the corresponding garbled circuits for location verification. For simplicity, PAI, OPE and GCC are referring to Paillier based, order-preserving encryption based and garbled circuits based location verification, respectively.

A. Security Strength And Recommended Key Size

A *security strength* is a number associated with the amount of work that is required to break a cryptographic algorithm or a system [7]. Cryptographic algorithms provide different "strength" of security, depending on the algorithm and the key size used. Throughout the experiment, we divide the security strength into three levels: short, medium and long. Table I lists the usage time for different keys of corresponding cryptographic algorithms.

B. Evaluation Metrics

Based on the threat model, we list the following evaluation metrics to assess protection schemes.

- *privacy*: The confidentiality of spatial data is the priority of privacy. Besides, a qualified scheme should be able to defend against attacks from both inside and outside.
- *utility*: The utility refers to the service usability. In this paper, it is reflected by location verification accuracy.

TABLE III: Operations Comparison of Different Cryptographic Algorithms

Security Strength	Paillier				Order-preserving Encryption		Garbled Circuits		
	EN	DE	ADD	MUL	EN	DE	CMP	AND	OR
Short	$1.6 * 10^3 T$	$1.7 * 10^3 T$	$10 T$	$0.6 * 10^3 T$	T	$3 T$	$7.5 * 10^4 T$	$9.5 * 10^4 T$	$1.1 * 10^5 T$
Medium	$7 * 10^3 T$	$6.7 * 10^3 T$	$50 T$	$3.2 * 10^3 T$	$1.3 T$	$5.7 T$	$1 * 10^5 T$	$1.1 * 10^5 T$	$1.1 * 10^5 T$
Long	$4.7 * 10^4 T$	$4.7 * 10^4 T$	$70 T$	$2.3 * 10^4 T$	$2.5 T$	$14 T$	$1.4 * 10^5 T$	$9.5 * 10^4 T$	$1.1 * 10^5 T$

Fig. 3: Performance Comparison Under Different Security Strength

If the verification accuracy remains as the original one without privacy protection, the utility is preserved.

- *performance*: The performance of mechanisms refers to the execution time and communication overhead which is normally the biggest obstacle for cryptography-based solutions.

C. Theoretical Analysis

Table II lists the time-consuming operations and communication cost of each party in three schemes. For the communication cost, L is the bitlength of ciphertext according to the security strength and t is the bitlength of coordinate values. Since a 32-bit integer can present the location precisely at a centimetre level, we assume $t \leq 32$. However, it is hard to have a direct comparison between solutions with different operations as shown in Table II. It is necessary to standardize operation cost into the same unit. To obtain the ratio between different operations, we measure the running time of each operation under the same setting. With the running time of OPE encryption T as a base unit, the results of each operation under different security strength are shown in Table III. From the result, it is easy to see that the OPE presents a big advantage in computation cost.

D. Experimental Analysis

We implemented both UE and A-UE on a macOS platform with 3.1GHz Intel Core i5 CPU and 8G RAM to evaluate the performance of the proposed protocols. Specifically, we generate random location pairs and distribute them to UE and A-UE, separately. The measured distance is Euclidean distance of a location pair with random values. The threshold is set to a random value. Both measured distance and threshold are held by UE. The experimental results are the average for 10 rounds.

According to the algorithm, all schemes can be divided into initialization and online process. Noted that initialization

is an offline process of key generation and can be operated alone without any information dependence or cooperation requirements. Online latency is composed of three parts: the computation of UE, the computation of A-UE and the communication delay between them. Fig. 3 is the results of two processes respectively. From the results, we can see that (1) OPE outperforms PAI and GCC in online latency, which makes it more practical in reality; (2) both OPE and GCC show a stable performance with regard to different security strength; (3) although GCC shows a fair performance in online latency, its heavy computation cost in initialization limits its usage in resource constraints platform.

For more insights, we also study the detail of online latency. The results are presented in Table IV. From the results, we can see that (1) compared with UE, all schemes put more computation on A-UE; (2) thanks to the fast data transmission, the communication cost of GCC does not delay its online response. As a conclusion, OPE outperforms both PAI and GCC in both utility and performance.

VI. RELATED WORK

Location privacy has been widely studied in the literature. According to adopted strategies, solutions can be classified into three categories: access control, obfuscation and cryptography [3].

Access control grants users with the right to perform actions on the location information of another user according to policies or defined trust [8]. Access control enhances system security by filtering participants involved. Nevertheless, it assumes that all the passed participants are trusted. Thus, it is unable to prevent attacks when compromised participants try to obtain the location information of other users and could hazard the system in the long term.

TABLE IV: Details of Online Latency in Location Verification

	Short			Medium			Long		
	PAI	OPE	GCC	PAI	OPE	GCC	PAI	OPE	GCC
UE (ms)	13	3	22	26	4	21	77	7	35
A-UE (ms)	13	8	27	44	9	26	100	14	46
comm. (kb)	1	3.5	47	2	7	47	4.1	14	47

K -anonymity, dummy location and mix zone are three representative obfuscation strategies for location privacy. K -anonymity obfuscates a user's location related query with at least $K - 1$ similar queries so that the service provider cannot infer the user's location from the query [9], the construction of K -anonymity protected query is normally processed by a trusted local server. In contrast, dummy location shares the same idea with K -anonymity without any constraints like a trusted third party or key sharing. But, it also suffers from spatiotemporal correlation issues when users submit consecutive requests [10], [11]. Mix zone is a popular solution for location privacy-preserving in VANET. For any vehicle entering a mix zone, it immediately gets a pseudonym that will be used for communications in the zone. It protects the vehicle privacy by disconnecting the link between vehicles and pseudonyms employed by the vehicles. In general, obfuscation based solutions protect user identity by disguising it with random generalized fake information. However, they are limited by the requirement of a central gateway for data obfuscation or key generation which makes them not suitable for decentralized D2D scenarios.

Schemes relying on cryptography have been extensively studied to offer high-level privacy and security guarantee. A privacy-preserving proximity notification that provides a complete privacy-concerning service was proposed by Mascetti et al. [12]. Based on private information retrieval (PIR), Ghinita et al. [13] implemented privacy-preserving nearest neighbour search in LBS. A similar work that also aims to solve the location comparison is presented by Narayanan et al. in [14], they solved the problem with a private equality testing protocol based on Decision Diffie-Hellman (DDH) problem. However, their solution is not applicable to our target problem since they treated a location as a value, not coordinates and they only support an equality test. As a conclusion, the schemes relying on cryptography normally meet high-level privacy and security demands even though their design is challenging and problem-oriented. Given the sensitivity and precision requirement of location verification, we only focus on cryptography-based schemes for privacy-preserving D2D cooperative location verification.

VII. CONCLUSION

This paper addresses the privacy issues in D2D cooperative location verification so that devices involved in location verification are not required to share their location information anymore. Specifically, three solutions based on state-of-the-art cryptographic techniques are designed and implemented. Extensive theoretical analysis and experimental tests were conducted to evaluate the proposed solutions. The results show

that OPE based scheme achieves the best balance with regards to privacy, utility and performance. Although this paper can solve the privacy issues in D2D location verification efficiently, it is still unable to defend malicious attacks when A-UE sending fake locations. Future work will focus on this issue.

ACKNOWLEDGMENT

This work is supported in part by the Academy of Finland under Grant 308087, Grant 335262 and Grant 345072; and in part by the National Natural Science Foundation of China under Grant 62072351.

REFERENCES

- [1] S. Khandker, J. Torres-Sospedra, and T. Ristaniemi, "Improving rf fingerprinting methods by means of d2d communication protocol," *Electronics*, vol. 8, no. 1, p. 97, 2019.
- [2] K. Zickuhr, "Location-based services," *Pew Research*, vol. 679, p. 695, 2013.
- [3] M. Haus, M. Waqas, A. Y. Ding, Y. Li, S. Tarkoma, and J. Ott, "Security and privacy in device-to-device (d2d) communication: A review," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 2, pp. 1054–1079, 2017.
- [4] Z. Yang and K. Järvinen, "The death and rebirth of privacy-preserving wifi fingerprint localization with paillier encryption," in *IEEE INFOCOM 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 1223–1231.
- [5] M. Dehghan, B. Sadeghiyan, and E. Khosravian, "Private trajectory intersection testing: Is garbled circuit better than custom protocols?" *International Journal of Engineering*, vol. 34, no. 4, pp. 863–872, 2021.
- [6] F. Kerschbaum, "Commutative order-preserving encryption," May 17 2012, uS Patent App. 12/944,672.
- [7] E. Barker, W. Barker, W. Burr, W. Polk, M. Smid et al., *Recommendation for key management: Part 1: General*. National Institute of Standards and Technology, Technology Administration, 2006.
- [8] G. Xu, H. Li, Y. Dai, K. Yang, and X. Lin, "Enabling efficient and geometric range query with access control over encrypted spatial data," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 870–885, 2018.
- [9] B. Niu, Q. Li, X. Zhu, G. Cao, and H. Li, "Achieving k-anonymity in privacy-aware location-based services," in *IEEE INFOCOM 2014-IEEE Conference on Computer Communications*. IEEE, 2014, pp. 754–762.
- [10] H. Liu, X. Li, H. Li, J. Ma, and X. Ma, "Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services," in *IEEE INFOCOM 2017-IEEE Conference on Computer Communications*. IEEE, 2017, pp. 1–9.
- [11] M. R. Nosouhi, V. V. H. Pham, S. Yu, Y. Xiang, and M. Warren, "A hybrid location privacy protection scheme in big data environment," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*. IEEE, 2017, pp. 1–6.
- [12] S. Mascetti, D. Freni, C. Bettini, X. S. Wang, and S. Jajodia, "Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies," *The VLDB journal*, vol. 20, no. 4, pp. 541–566, 2011.
- [13] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan, "Private queries in location based services: anonymizers are not necessary," in *Proceedings of the 2008 ACM SIGMOD international conference on Management of data*, 2008, pp. 121–132.
- [14] A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, D. Boneh et al., "Location privacy via private proximity testing," in *NDSS*, vol. 11, 2011.