Journal of System Simulation

Volume 35 | Issue 10 Article 15

10-30-2023

Design and Simulation of a Location Privacy Protection Scheme Based on Zero-knowledge Proof for Military IoT

Mingjie Shi
Sun Yat-Sen University, School of Systems Science and Engineering, Guangzhou 510000, China, shimj5@mail2.sysu.edu.cn

Chengyu Xie
Sun Yat-Sen University, School of Systems Science and Engineering, Guangzhou 510000, China

Chuanfu Zhang
Sun Yat-Sen University, School of Systems Science and Engineering, Guangzhou 510000, China, zhangchf9@mail.sysu.edu.cn

Design and Simulation of a Location Privacy Protection Scheme Based on Zero-knowledge Proof for Military IoT

Abstract

Abstract: In the military Internet of Things (IoT) combat environment, the location privacy issue becomes a key challenge. An innovative location privacy protection scheme based on zero-knowledge proof is proposed to ensure that in unreliable communication channels, the location information of combat units can be verified without revealing their specific coordinates, so as to achieve the goal of protecting sensitive location information. Based on the idea of cryptography, by using zero-knowledge proof, through algebraic circuit, rank-1 constraint system(R1CS), quadratic arithmetic programs(QAP), and other steps, the position coordinate information proof problem is transformed into a point verification problem on a polynomial curve, and the position verification is completed in one round of the challengeresponse process. The simulation experiment is carried out, and the results verify the effectiveness of the scheme, which significantly improves the security of position information and has broad practical application value. The research results provide an innovative solution for security positioning in future military operations and further strengthen the security guarantee of military IoT operations.

Keywords

location privacy, zero-knowledge proof, military IoT operation, location proof scheme

Recommended Citation

Shi Mingjie, Xie Chengyu, Zhang Chuanfu. Design and Simulation of a Location Privacy Protection Scheme Based on Zero-knowledge Proof for Military IoT[J]. Journal of System Simulation, 2023, 35(10): 2237-2248.

第 35 卷第 10 期 系统仿真学报© Vol. 35 No. 10
2023 年 10 月 Journal of System Simulation Oct. 2023

Design and Simulation of a Location Privacy Protection Scheme Based on Zero-knowledge Proof for Military IoT

Shi Mingjie，*Xie Chengyu*，*Zhang Chuanfu*[*]
(Sun Yat-Sen University, School of Systems Science and Engineering, Guangzhou 510000, China)

Abstract： In the military Internet of Things (IoT) combat environment, the location privacy issue becomes a key challenge. *An innovative location privacy protection scheme based on zero-knowledge proof is proposed to ensure that in unreliable communication channels*, *the location information of combat units can be verified without revealing their specific coordinates*, *so as to achieve the goal of protecting sensitive location information*. Based on the idea of cryptography, by using zero-knowledge proof, through algebraic circuit, rank-1 constraint system(R1CS), quadratic arithmetic programs(QAP), and other steps, the position coordinate information proof problem is transformed into a point verification problem on a polynomial curve, and the position verification is completed in one round of the challenge-response process. The simulation experiment is carried out, and the results verify the effectiveness of the scheme, which significantly improves the security of position information and has broad practical application value. The research results provide an innovative solution for security positioning in future military operations and further strengthen the security guarantee of military IoT operations.

Keywords： location privacy; zero-knowledge proof; military IoT operation; location proof scheme

一种基于零知识证明的军事物联网位置隐私保护方案设计与仿真

施明杰，解程宇，张传富[*]
(中山大学 系统科学与工程学院，广东 广州 510000)

摘要：*在军事物联网作战环境中，位置隐私问题成为关键挑战。提出了一种基于零知识证明的位置隐私保护方案，以确保在不可靠的通信信道中，作战单位的位置信息既得以验证，又无需暴露其具体坐标，达到保护敏感位置信息的目的。*基于密码学思想，利用零知识证明，通过代数电路、R1CS（rank-1 constraint system）、QAP（quadratic arithmetic programs）等步骤将位置坐标信息证明问题转换为多项式曲线上的点验证问题，在一轮挑战-响应过程中完成位置验证。仿真结果验证了该方案的有效性，提升了位置信息的安全性，有着广阔的实际应用价值。研究成果为未来军事作战中的安全定位提供了一种新的解决方案，进一步强化了军事物联网作战的安全保障。

关键词：位置隐私；零知识证明；军事物联网作战；位置证明方案
中图分类号：TP391 文献标志码：A 文章编号：1004-731X(2023)10-2237-12
DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E
引用格式: 施明杰, 解程宇, 张传富. 一种基于零知识证明的军事物联网位置隐私保护方案设计与仿真[J]. 系统仿真学报, 2023, 35(10): 2237-2248.

Received date: 2023-07-03 Revised date: 2023-08-03

First author: Shi Mingjie (1998-), male, master student, research areas: information security and zero-knowledge proof.
E-mail: shimj5@mail2.sysu.edu.cn
Corresponding author: Zhang Chuanfu (1973-), male, associate professor, doctor, research areas: information security modeling and simulation theory and technology. E-mail: zhangchf9@mail.sysu.edu.cn.

Reference format: Shi Mingjie, Xie Chengyu, Zhang Chuanfu. Design and Simulation of a Location Privacy Protection Scheme Based on Zero-knowledge Proof for Military IoT[J]. Journal of System Simulation, 2023, 35(10): 2237-2248.

0 Introduction

Military Internet of Things (IoT) [1] represents the practical application of IoT technology in various military fields, with an emphasis on the comprehensive processing of essential information such as personnel, equipment, resources, facilities, and environmental factors, thereby strengthening command capabilities and management coordination. Digitization, networking, and intelligence constitute the development direction of future warfare, while military IoT underpins the key technological support for future battlefields, enhancing situational awareness, command decision-making, logistical support, and overall combat efficiency [2].

In a military environment, IoT devices include vehicles, instruments, and weapons systems. The use of these devices introduces a higher level of complexity to battlefield systems, significantly improving operational efficiency. However, as an emerging military operational unit, IoT devices are not exempt from security and privacy issues. During mission execution, military IoT units [3] must comply with orders from the command center and perform tasks within defined areas. Traditional systems expose the potential risk of adversaries intercepting task lists or communications between the command center and military IoT units [4], thereby inferring the location of the operational units and initiating disruptive actions.

In this paper, we propose a zero-knowledge location verification scheme that focuses on addressing location privacy issues in the domain of military IoT operations. Through a round of challenge-response, location verification is achieved in complex channel environments. This scheme allows the command center to verify whether the operational units are located along a given trajectory without revealing the exact coordinates, thus ensuring location privacy while proving location coordinates.

1 Related Work

1.1 Location privacy schemes

Location privacy [5] refers to a distinct genre of information privacy that concerns the "when, where, and how" of sharing relevant information and content about individuals and organizations. Location privacy threats [6-7] refer to the acquisition of raw location data by attackers without proper authorization, followed by the execution of related attack activities based on this location information. Existing location privacy solutions [8] are analyzed for their respective strengths and weaknesses:

1.1.1 Trusted third-party schemes

Spatial cloaking techniques have been widely adopted to enhance the location privacy of users. These techniques rely entirely on a trusted entity [9], called a location anonymizer, introduced between the user and the center. The purpose of the location anonymizer is to implement k-anonymity [10], where a user becomes indistinguishable from $(k-1)$ users, rendering the control center unable to identify the true user and thus protecting the user's privacy. Zhang et al. [11] proposed a cached and spatial k-anonymity scheme to strengthen user privacy in continuous location queries, which used a caching mechanism to cache query results for future queries.

The primary problem of these schemes is that they rely entirely on a trusted third party. If an attacker compromises this trusted third party, the user's

DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E

location privacy could be violated. In addition, these trusted third parties remain tempting targets for attackers because they store large amounts of user location information. Therefore, including a trusted third party in the interaction is fraught with risk.

1.1.2 Virtual location generation schemes

In virtual location schemes [12], users construct fictitious or contrived locations that are congruent with their actual locations and transmit them to the control center to facilitate the provision of services. Kido et al. proposed a location privacy protection scheme [13] that allowed users to construct multiple fake locations in addition to their actual locations and transmit them to the center. Sun et al.[14] proposed an entropy-based fake location selection algorithm that greedily selected fake locations, thereby balancing privacy and computational cost.

While virtual location technologies ensure user location privacy, they do so at the expense of service accuracy. In addition, generating fake locations that mimic behavior under real-world conditions is challenging.

1.1.3 Encryption schemes

Encryption-based methods [15] fundamentally rely on encrypting location information, making it imperceptible to servers; consequently, even if attackers acquire encrypted data, they are unable to decipher the user's real data. By combining cryptographic principles with location privacy, these schemes ensure data usability and service precision [16]. However, they impose significant communication and computational overheads and complicate deployment.

1.2 Location privacy schemes in military IoT

He et al.[17] used NB-IoT communication module, Beidou positioning module, and buzzer to form positioning equipment. The NB-IoT SIM card on the device sent the real-time location information to the cloud platform to ensure real-time dynamic grasp and real-time data grasp. Utsav et al.[18] adopted the way of drone interconnection, and the entire network was monitored by the control unit through the IoT. Each drone had a GPS module which was used to get the current location of the drone. NATO STO IST-147 Research Task Group on Military Applications of the IoT [19] proposed a set of applicable methods and tools to protect data integrity and confidentiality using cryptography.

In general, existing military IoT devices generally rely on hardware modules to ensure location privacy, but Andras [20] used keyword analysis to examine the vulnerabilities of these IoT devices and pointed out that the main issue of IoT devices in the military field was privacy. Insufficient protection requires greater attention to data protection in military operations, as the success of operations depends to a large extent on achieving and maintaining information superiority.

In actual combat scenarios, sometimes it is only necessary to ensure that the combat unit is in a designated position, and there is no need to inform the exact position coordinates, which can effectively alleviate the problem of insufficient privacy protection. Cryptography can help prevent security and privacy issues as well as user impersonation attacks, and greater attention needs to be paid to such solutions in military settings.

2 Principles of Location Privacy Protection

2.1 Problem statement

Through our analytical study, we have identified

the inherent shortcomings of the previously mentioned location privacy proof strategies. In the military domain, relying on a trusted third party lacks comprehensive security guarantees; its compromise would render the entire system useless. Implementing a virtual location solution requires sacrificing quality of service to maintain location privacy.

In the context of the military IoT, the combat unit must follow a specific route, but the presence of unreliable channels makes real-time location reporting impossible. In this case, the command center only needs to ensure that the combat unit is following the prescribed path without worrying about the specific location. The combat unit can make a statement about its coordinates: “I am currently on the prescribed path”. The dilemma is how the combat unit can validate this claim without revealing its exact location.

The zero-knowledge proof [21], a cryptographic tool introduced by Goldwasser and others, allows the prover to prove the validity of a claim to a verifier without revealing any additional information. It satisfies three essential properties: ① completeness, If the prover provides a correct proof, the verifier will always pass the validation; ② soundness, if the prover concocts a false proof, the verifier will reject it with negligible probability; ③ zero-knowledge, the verifier only acknowledges the correctness of the assertion without acquiring any other knowledge.

Considering all aspects of the existing work in conjunction with the requirements of military applications, we design a location privacy proof scheme based on zero-knowledge proof. The combat unit can validate its assertion using the zero-knowledge proof; relying on the completeness, soundness, and zero-knowledge properties of the proof, the command center can verify that the combat unit is on the intended path without the need for specific location data.

2.2 Principles of proving location privacy protection

The location privacy protection scenario design is shown in Fig. 1. The command center issues operational tasks and target locations to the combat unit, which is obliged to follow the issued instructions, proceed along the pre-determined route, and immediately report its location to headquarters. Due to the existence of unreliable channels, specific locations must remain undisclosed. The combat unit makes a statement: “My coordinates are currently along the designated route”. The combat unit must substantiate this claim to headquarters.

In order to ensure the integral construction of the scheme proposed in this paper, several basic assumptions are made

(1) The communication process involves two parties, namely the combat units and the command center.

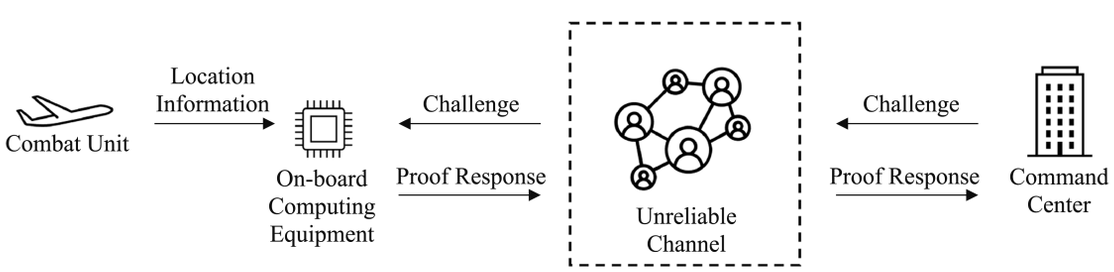

Fig. 1 Location privacy protection scenario design

DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E

(2) The communication unfolds over an unreliable channel, susceptible to interception by adversaries.

(3) The combat units, acting as honest provers, seek to validate the legitimacy of their locations by providing assertive evidence about them, while the command center, acting as a verifier, scrutinizes these assertions.

This paper utilizes the method of zero-knowledge proof to address the proof of assertion problem, namely, the location proof problem. In order to model the research question and describe it in mathematical language, a cubic curve $f(x)=ax^3+bx^2+cx+d$ represents the prescribed route, while the coordinate of the combat unit is (x,y). Without revealing the true values of (x,y), the unit must prove that (x,y) lies on the cubic curve, i.e., $f(x)=y$. The zero-knowledge proof involves two entities, namely the prover and the verifier. In the context of this paper, the combat unit is the prover, and the command center is the verifier.

3 Scheme Design

In response to the need for a combat unit to prove its location on a predetermined route without revealing its actual location, we consider a location proof scheme based on zero-knowledge proof. Our study incorporates zero-knowledge proof technology by transposing the dilemma to the verification of a point on a polynomial curve. Utilizing the mathematical properties of polynomials along with the security properties of zero-knowledge proof, we aim to accomplish the task of location verification. To facilitate explanation and exploration, we will delve into the matter using the example of a cubic polynomial. Fig. 2 shows the execution steps and information flow of the scheme.

3.1 Algebraic circuit

We reformulate the assertion verification problem as a computable dilemma. In other words, devising a zero-knowledge location proof protocol that outputs “true” when (x,y) rests on the curve, and conversely, it pronounces “false”'. First, the complex expression of the cubic curve is flattened, decomposed into a simple expression, and converted into a statement sequence with two forms, such as $x=y$or$x=y(op)z$; op includes $+-\times/$, and each A statement can be thought of as a logic gate in a circuit. Consequently, $f(x)$ can be broken down into the following five logical gate operations:

$$\begin{cases} sym_1=ax+b \\ sym_2=sym_1\times x \\ sym_3=sym_2+c \\ sym_4=sym_3\times x \\ y=sym_5+d \end{cases} \tag{1}$$

If (x,y) is on that particular curve, the above equations are universally satisfied; conversely, if (x,y) is not on that curve, the equations are not satisfied. Thus, the prover provides the input. According to the mathematical computational circuit, if the output testifies to be “true”, then it validates that the input conforms to expectations. By exploiting the circuit dilemma, the prover is allowed to hide the original data (input).

3.2 Rank-1 constraint system

The algebraic circuit fails to ensure that input, output, and the circuit itself correspond. Consequently, there is a need to connect these three entities to ensure that the output is indeed the result of the input passing through the algebraic circuit.

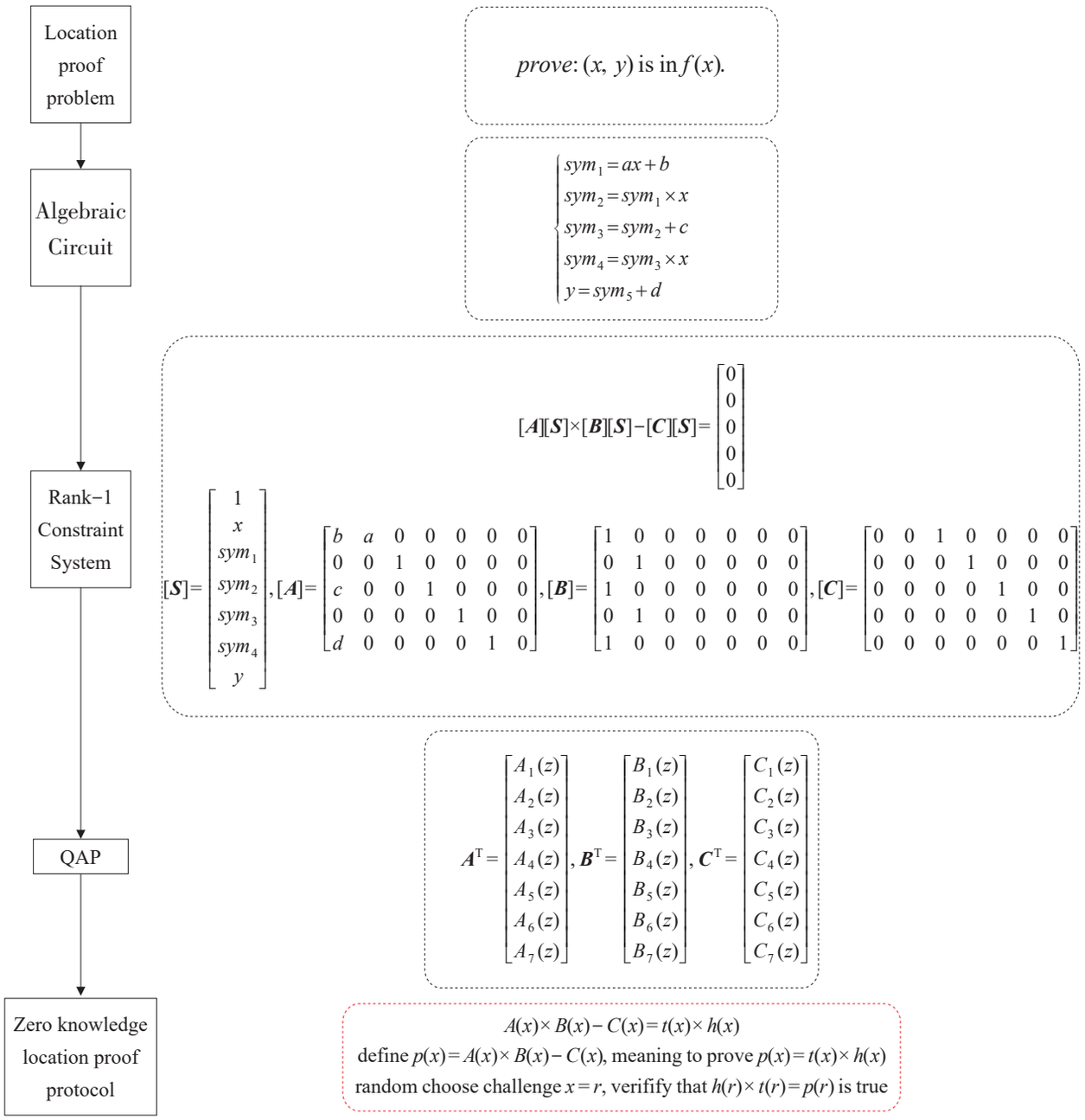

Fig. 2 Left is the execution steps of the scheme, and right is the information flow

The algebraic circuit is thus transformed into a rank-1 constraint system (R1CS). R1CS is a sequence composed of three vectors $(\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C})$. For the solution vector $\boldsymbol{s}$, it satisfies $\boldsymbol{sA}^{\mathrm{T}} \times \boldsymbol{sB}^{\mathrm{T}} = \boldsymbol{sC}^{\mathrm{T}}$, a constraint; × represents the multiplication of elements at the same position in the vector. Taking the first logical gate $ax + b - sym_1 = 0$ as an example, we convert this to R1CS constraints and get

$$\begin{aligned} \boldsymbol{A} &= [b, a, 0, 0, 0, 0, 0] \\ \boldsymbol{B} &= [1, 0, 0, 0, 0, 0, 0] \\ \boldsymbol{C} &= [0, 0, 1, 0, 0, 0, 0] \\ \boldsymbol{s} &= [1, x, sym_1, sym_2, sym_3, sym_4, y] \end{aligned} \tag{2}$$

At this point, $\boldsymbol{sA}^{\mathrm{T}} \times \boldsymbol{sB}^{\mathrm{T}} - \boldsymbol{sC}^{\mathrm{T}} = 0$ is satisfied. Each equation corresponds to a constraint, so there are five constraints in total. By repeating the same process for the remaining logic gates, the complete R1CS form is as follows:

DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E

$$[\boldsymbol{A}][\boldsymbol{S}]\times[\boldsymbol{B}][\boldsymbol{S}]-[\boldsymbol{C}][\boldsymbol{S}]=\begin{bmatrix}0\\0\\0\\0\\0\end{bmatrix} \tag{3}$$

To prove the validity of the polynomial $f(x)=y$, it is only necessary to prove the truth of $[\boldsymbol{A}][\boldsymbol{S}]\times[\boldsymbol{B}][\boldsymbol{S}]-[\boldsymbol{C}][\boldsymbol{S}]=0$.

3.3 Quadratic Arithmetic Programs

In the scenario of large-scale circuits with thousands upon thousands of circuit gates, the verification efficiency of R1CS becomes terribly low. Therefore, it is necessary to transform the calculation of vector inner products into a form of polynomial calculation. Unlike vector inner product computation, polynomial computation can verify the correctness of all constraints through a singular computation, thus avoiding heavy computational load. In other words, R1CS is transformed into the form of quadratic arithmetic programs (QAP). In this paper, five sets of seven vectors with a length of seven are converted into seven sets of polynomials, and each set of polynomials contains three fourth-order polynomials. Polynomials at each x coordinate represent a constraint condition, so there are five constraints in total, respectively. The set of five vectors is evaluated polynomially at $x = u_i$.

The Lagrange interpolation formula is used to generate the QAP. With $[\boldsymbol{A}]$ as an example, there are a total of five constraints, each of which is a vector $\boldsymbol{A}_i$, $i=1,2,\cdots,5$. The Lagrange interpolation method transforms these five vectors into seven polynomials. Specifically, the polynomial of the first value of each vector A_i corresponding to the five constraints is calculated. In other words, the Lagrange interpolation theorem is used to obtain a polynomial over the five points (u_i, A_{i1}), $i=1,2,\cdots,5$. The Lagrange interpolation formula appears as follows. With the first column value A_{i1} as an example, the polynomial over the five points (u_i, A_{i1}), $i=1,2,\cdots,5$ is

$$A_1(z)=\sum_{i=1}^{5}A_{i1}\times\prod_{j\neq i}^{1\leqslant j\leqslant 5}\frac{(z-u_j)}{(u_i-u_j)} \tag{4}$$

Performing the same operation on B and C yields twenty-one quartic polynomials. Thus, the proof, $[\boldsymbol{A}][\boldsymbol{S}]\times[\boldsymbol{B}][\boldsymbol{S}]-[\boldsymbol{C}][\boldsymbol{S}]=0$, transforms into the proof, $A(x)\times B(x)-C(x)=0$ when $x=u_i$, $i=1,2,\cdots,5$, where $A(x)=\boldsymbol{A}\boldsymbol{s}^{\mathrm{T}}$, $B(x)=\boldsymbol{B}\boldsymbol{s}^{\mathrm{T}}$ and $C(x)=\boldsymbol{C}\boldsymbol{s}^{\mathrm{T}}$.

If there are n R1CS constraints, it is necessary to verify that $A(x)\times B(x)-C(x)$ equals zero n times. For large-scale polynomials, multiple verifications are not pragmatic, so it is necessary to convert multiple verifications into a single one that ensures equivalent conversion. Let $t(x)=(x-u_1)(x-u_2)\cdots(x-u_n)$, where $t(x)$ necessarily equals zero at $x=u_1$, $x=u_2,\cdots$, $x=u_n$. If there exists a polynomial $h(x)$ such that $A(x)\times B(x)-C(x)=t(x)\times h(x)$, it implies that the polynomial $A(x)\times B(x)-C(x)$ can be divided by $t(x)$, and this polynomial will necessarily equal zero at $x=u_1$, $x=u_2,\cdots$, $x=u_n$. Verifying $A(x)\times B(x)-C(x)=t(x)\times h(x)$ allows for the completion of all R1CS constraints' verification at once; once this verification passes, the input can be trusted to be truthful.

Specifically, the verifier chooses a random number x to initiate a challenge, and the prover proves that $A(x)\times B(x)-C(x)=t(x)\times h(x)$. If it is satisfied, the proof can be considered valid.

3.4 Zero-knowledge location proof protocol

An analysis of the formula $A(x)\times B(x)-C(x)=t(x)\times h(x)$ that needs verification unveils the following contents.

(1) $t(x)$ is a polynomial known to both the verifier and the prover, $t(x)=(x-u_1)(x-u_2)\cdots(x-u_n)$;

(2) Only the prover knows$A(x)\times B(x)-C(x)$, and its coefficients contain knowledge;

(3) $h(x)$ is also known only to the prover and is computed by dividing $A(x)\times B(x)-C(x)$ by $t(x)$; the verifier should not know $h(x)$, as $A(x)\times B(x)-C(x)$ can be computed through $t(x)$ and $h(x)$.

The public verifiability of the polynomials is illustrated in Table 1. If $p(x)=A(x)\times B(x)-C(x)$, we need to prove that $p(x)=t(x)\times h(x)$. The verification process is divided into the following three steps:

(1) Challenge phase: The verifier selects a random challenge point, $x=r$, which is subsequently conveyed to the prover.

(2) Response phase: Upon receipt, the prover calculates $p(r)$, $h(r)$ and dispatches these values back to the verifier as a response.

(3) Verification phase: The verifier calculates $t(r)$ and ascertains the validity of the equality $h(r)\times t(r)=p(r)$ based on the received $p(r)$ and $h(r)$. If this holds, it substantiates that the prover's location aligns with the anticipated outcome.

Table 1 Public verifiability of polynomials

	$A(x)\times B(x)-C(x)$	$t(x)$	$h(x)$
Prover	√	√	√
Verifier	×	√	×

Note: √ denotes known values; × represents the unknown.

4 Simulation Experiment and Analysis

4.1 Experimental design

In accordance with the milieu of military IoT operations, operational units must confirm their locational alignment with the command center's directives during mission execution. Owing to the unreliability of communication channels, it is untenable for units to directly relay their coordinates (x,y). Therefore, in order to fortify the locational confidentiality of military IoT units, we resort to zero-knowledge proof technology, utilizing the scheme delineated in Section 3 for our simulation experiment design. The overall flow chart of ZKLP scheme design is illustrated in Fig. 3.

As shown in Fig. 4, the cubic trajectory curve$y=x^3+4x^2-20x+6$ is considered and hypothetically precalculated by the command center based on the battlefield environment. If an operational unit diverges from this curve, it may incur the risk of enemy fire. Hence, the command center (verifier) requires the operational unit (prover) to demonstrate its adherence to the predetermined trajectory without compromising coordinate information. We shall validate this by using the coordinates (2, −10) and (2.5, −6) as examples.

As illustrated in Fig. 5, the coordinates (x,y) of the prover (operational unit) are (2 , − 10), situated accurately on the curve$y=x^3+4x^2-20x+6$. The verifier (command center) poses a challenge value $r=6.2$. The prover responds with computed $p(r)$ and $h(r)$, upon receipt of which the verifier computes $\left|p(r)/h(r)-t(r)\right|$. If this value is less than a predefined verification threshold (such as 1×10^{-3}), it is deemed within permissible error margins, thus successfully confirming the prover's location on the designated curve.

In Fig. 6 above, the coordinates (x,y) of the prover (operational unit) are (2.5, −6), which do not correspond with the curve$y=x^3+4x^2-20x+6$. Under such coordinate deviation, the verifier's final computation of $\left|p(r)/h(r)-t(r)\right|$ approximates 37.67, markedly exceeding the preset verification threshold. Consequently, it is determined that the prover is not on the specified curve, necessitating further directive adjustments.

DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E

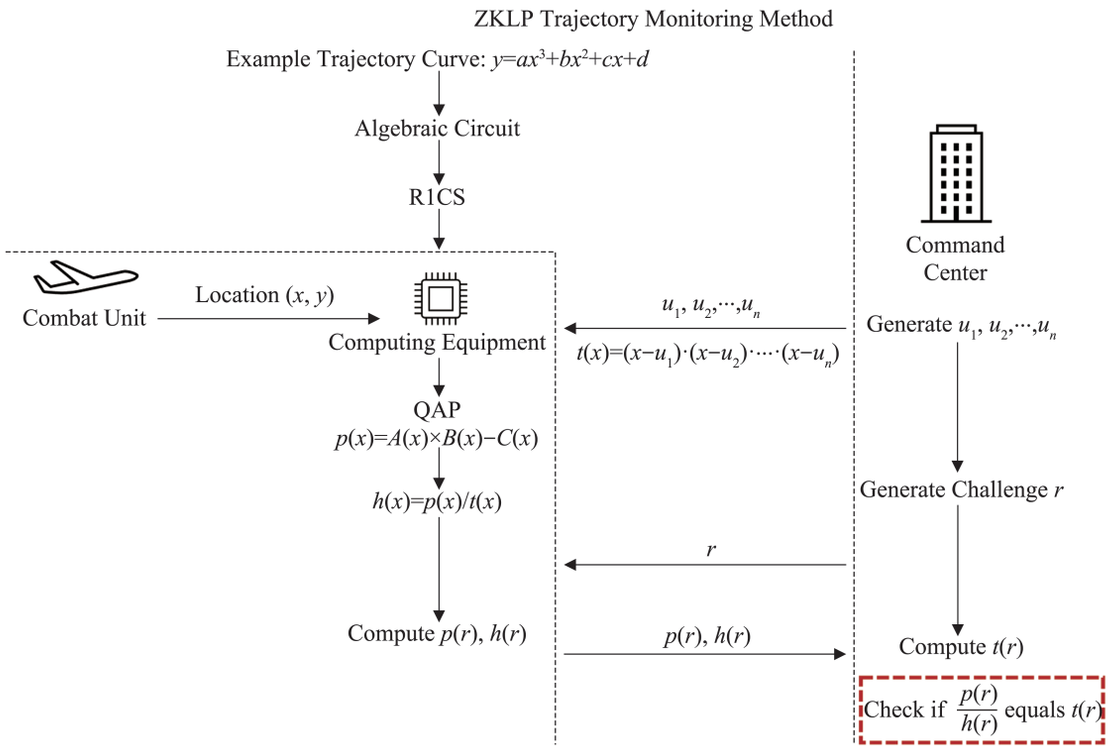

Fig. 3 ZKLP scheme flow

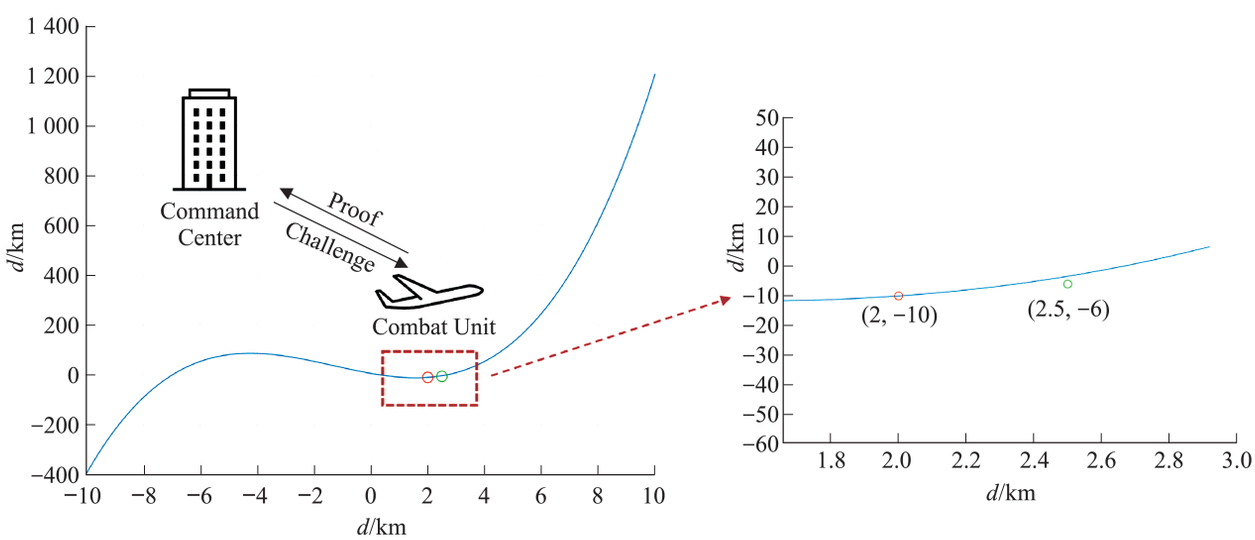

Fig. 4 ZKLP scheme simulation experiment

```
*************ZKLP*************
the location of verifier is:
(2, -10)
Challenge value r given by the challenger is: 6.20
Prover provide p(r)/h(r): 2.95679666
Verifier compute t(r) is: 2.95680000
|p(r)/h(r) - t(r)| is: -0.00000334, less than 10^(-3)
*************Successfully verified!*************
```

Fig. 5 Proof result for location coordinates (2, −10)

```
*************ZKLP*************
the location of verifier is:
(2.5, -6)
Challenge value r given by the challenger is: 6.20
Prover provide p(r)/h(r): 37.67145169
Verifier compute t(r) is: 2.95680000
|p(r)/h(r) - t(r)| is: 34.714652, more than 10^(-3)
*****Failed to verify! please give the right (x,y)*****
```

Fig. 6 Proof result for location coordinates (2.5, −6)

Following extensive experiment validation, it is confirmed that this design scheme successfully enables the prover (operational unit) to verify its position on the pre-set curve to the verifier (command center) without disclosing its coordinates (x, y). It is crucial to note that this experimental design aims to validate the feasibility of the scheme, and hence a simplified cubic polynomial situation is adopted. However, in reality, trajectory curves can be exceedingly complex, necessitating segmenting and approximating the trajectory into lower order polynomial curves for validation. Therefore, the ZKLP scheme proposed in this paper has significant practical value.

4.2 Further discussion

In this section, we will explore the verification accuracy and computation time of this algorithm. Firstly, regarding the verification accuracy of coordinate points, we take the scenario in Fig. 5 of Section 4.1 as an example. We introduced a bias of 1×10^{-3} to the x-axis and the verification results are illustrated in Fig. 7. Our tests show that any deviation above 1×10^{-3} will result in the computation of the term $\left|p(r)/h(r)-t(r)\right|$ significantly exceeding our set error tolerance threshold, and it will be judged as deviating from the preset trajectory. Additionally, we have tested a large number of computation cases, all of which support this conclusion.

```
*************ZKLP*************
the location of verifier is:
(2.001, -10)
Challenge value r given by the challenger is: 6.20
Prover provide p(r)/h(r): 2.98431773
Verifier compute t(r) is: 2.95680000
|p(r)/h(r) - t(r)| is: 0.027518, more than 10^(-3)
*****Failed to verify! please give the right (x,y)*****
```

Fig. 7 Proof result for location coordinates (2.001, −10)

Secondly, we have conducted further statistical analysis on the running time of the algorithm. Again, taking the scenario in Fig. 5 as an example, we have recorded the running times of different algorithm steps (refer to Fig. 2 in Section 3) on the laptop. The runtime for each step is presented in Table 2. We have found that over 90% of the time is consumed in the QAP step. The analysis suggests that this might be due to the need for multiple Lagrange interpolation computations in calculating the QAP constraint matrix. In contrast, our core algorithm step, the ZKLP proof, only takes about 0.02 s, demonstrating the lightweight characteristic of the algorithm. This conclusion is also supported by the computation of a large number of other test cases.

Table 2 Runtime statistics

Step	Algeria circuit & R1Cs	QAP	ZKLP	Overall
Time/s	0.000 3	0.263 8	0.021 5	0.285 6

4.3 Experimental analysis

Upon empirical validation, the ZKLP trajectory monitoring scheme proposed in this study exhibits zero knowledge, completeness, and soundness, fulfilling the privacy requirements for typical operational scenarios.

Zero knowledge: The zero-knowledge location proof scheme ensures that the verifier can only ascertain the veracity of the assertion without gaining any other useful information. In the context of military IoT operations, this implies that the command center can verify whether the operational unit is on the specified route without knowing the exact location information. This zero-knowledge property safeguards the location privacy of the operational units, precluding any useful location information acquisition even in the face of malevolent eavesdropping.

Completeness: The completeness of the zero-

DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E

knowledge location proof scheme guarantees that if the prover provides correct proof, the verifier will definitely pass the verification. In military IoT operations, the operational unit provides an assertion and executes a zero-knowledge proof to demonstrate its position on the specified route. The command center verifies the proof via a challenge-response approach, only accepting the verification if the assertion and corresponding proof are accurate, thus ensuring the positional accuracy of the operational units.

Soundness: The soundness of the zero-knowledge location proof scheme ensures that if the prover fabricates a false proof, the verifier will reject it with negligible probability. In military IoT operations, if an operational unit provides false assertions or fabricated proofs, the command center will reject the verification with negligible probability, effectively precluding the possibility of arbitrary location information forgery. This ensures the authenticity and trustworthiness of the operational units' positional information.

In addition, we compare the proposed scheme with existing technological solutions. The comparison results can be seen in Table 3. The scheme presented in this paper demonstrates improvements in terms of accuracy, privacy, and computational efficiency and can meet the requirements of military IoT warfare scenarios.

Table 3 Comparison

Scheme	Trusted settings	Accuracy	Privacy	Efficiency
TTP	Yes	High	Medium	High
VLG	No	Low	High	Medium
ENC	No	High	High	Low
ZKLP(ours)	**No**	**High**	**High**	**High**

Note：TTP(trusted third party schemes); VLG(virtual location generation schemes); ENC(encryption schemes).

5 Conclusion

This paper presents a location privacy solution based on zero-knowledge proof, specifically designed to address the privacy concerns inherent in military IoT warfare scenarios. By developing a verification scheme capable of confirming the location of a combat unit along a predetermined route without revealing the exact coordinates, it adeptly addresses the need for location validation without revealing specific location data. In our experimental evaluation, this strategy ensures a high level of verification accuracy and efficiency while maintaining the integrity of location privacy.

The proposed scheme significantly reduces the risk of sensitive information leakage. In real military IoT wars, the control center and the combat units agree on the trajectory in advance. The scheme in this paper can prove that the combat unit is at the specified location on the trajectory, thereby protecting the unit's location privacy. This solution has important practical value for military IoT wars, providing a secure and reliable means of location verification for strategic military decision-making.

Future research could further explore the potential application of this approach in the area of military IoT. The zero-knowledge proof technology has shown broad applicability beyond the field of location privacy, such as communication security, location sharing, and secure navigation. In addition, performance enhancements and improvements to the solution can be explored to improve verification efficiency and scalability.

References：

[1] 张萌, 杨志伟, 姜江, 等. 军事物联网体系试验初探[J]. 军事运筹与评估, 2023, 38(1): 67-72.
Zhang Meng, Yang Zhiwei, Jiang Jiang, et al.

Preliminary Study on the Military Internet of Things System Tests[J]. Military Operations Research and Assessment, 2023, 38(1): 67-72.

[2] Yu Juan. Design of Location Security Protection System Based on Internet of Things[C]//2022 4th International Conference on Applied Machine Learning (ICAML). Piscataway, NJ, USA: IEEE, 2022: 273-276.

[3] Calcara A, Gilli A, Gilli M, et al. Why Drones Have Not Revolutionized War: the Enduring Hider-finder Competition in Air Warfare[J]. International Security, 2022, 46(4): 130-171.

[4] Asada M, Yoshikawa M, Cao Yang. "When and Where Do You Want to Hide?" - Recommendation of Location Privacy Preferences With Local Differential Privacy[C]// Data and Applications Security and Privacy XXXIII. Cham: Springer International Publishing, 2019: 164-176.

[5] 李沛谕, 张治学. 基于安全区域的汇聚节点位置隐私保护协议算法设计[J]. 系统仿真学报, 2015, 27(12): 2973-2980.
Li Peiyu, Zhang Zhixue. Protocol Algorithm Design of Location Privacy Preserving for Sink Node Based on Security Area[J]. Journal of System Simulation, 2015, 27 (12): 2973-2980.

[6] Zhu Liang, Liu Xiaowei, Jing Zhiyong, et al. Knowledge-driven Location Privacy Preserving Scheme for Location-based Social Networks[J]. Electronics, 2023, 12(1): 70.

[7] Naher N, Hashem T. Loukas G. Think Ahead: Enabling Continuous Sharing of Location Data in Real-time With Privacy Guarantee[J]. The Computer Journal, 2019, 62 (1): 1-19.

[8] Zhang Shiwen, Li Mengling, Liang Wei, et al. A Survey of Dummy-based Location Privacy Protection Techniques for Location-based Services[J]. Sensors, 2022, 22(16): 6141.

[9] Nisha N, Natgunanathan I, Gao Shang, et al. A Novel Privacy Protection Scheme for Location-based Services Using Collaborative Caching[J]. Computer Networks, 2022, 213: 109107.

[10] Tian Cenxi, Xu Hongyun, Lu Tao, et al. Semantic and Trade-off Aware Location Privacy Protection in Road Networks Via Improved Multi-objective Particle Swarm Optimization[J]. IEEE Access, 2021, 9: 54264-54275.

[11] Zhang Shaobo, Li Xiong, Tan Zhiyuan, et al. A Caching and Spatial *K*-anonymity Driven Privacy Enhancement Scheme in Continuous Location-based Services[J]. Future Generation Computer Systems, 2019, 94: 40-50.

[12] Chen Guobin, Li Shijin. Markov and Improved Particle Swarm Optimization-based Privacy Preservation Algorithm for User Space Geographical Location[J]. European Journal of Remote Sensing, 2020, 53(S1): 31-40.

[13] Kido H, Yanagisawa Y, Satoh T. An Anonymous Communication Technique Using Dummies for Location-based Services[C]//ICPS '05. Proceedings. International Conference on Pervasive Services, 2005. Piscataway, NJ, USA: IEEE, 2005: 88-97.

[14] Sun Gang, Chang V, Ramachandran M, et al. Efficient Location Privacy Algorithm for Internet of Things (IoT) Services and Applications[J]. Journal of Network and Computer Applications, 2017, 89: 3-13.

[15] Dua A, Singh P, Bapat J. Location Privacy-preserving Mechanism - A Data-driven Approach[C]//2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT). Piscataway, NJ, USA: IEEE, 2021: 1-6.

[16] 叶清, 李默洮, 宋莹莹, 等. 基于噪声加密机制的WSN差分位置隐私保护[J]. 传感技术学报, 2019, 32(12): 1904-1910.
Ye Qing, Li Moqian, Song Yingying, et al. Noise Encrypted Based Differential Location Privacy Protection in Wireless Sensors Network[J]. Chinese Journal of Sensors and Actuators, 2019, 32(12): 1904-1910.

[17] He Weixin, Cong Linhu. Intelligent Security System Based on Location Information[C]//2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE). Piscataway, NJ, USA: IEEE, 2020: 985-989.

[18] Utsav A, Abhishek A, Suraj P, et al. An IoT Based UAV Network for Military Applications[C]//2021 Sixth International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). Piscataway, NJ, USA: IEEE, 2021: 122-125.

[19] Tortonesi M, Wrona K, Suri N. Secured Distributed Processing and Dissemination of Information in Smart City Environments[J]. IEEE Internet of Things Magazine, 2019, 2(2): 38-43.

[20] Toth A. Internet of Things Vulnerabilities in Military Environments[J]. Vojenské Rozhledy, 2021, 30(3): 45-58.

[21] Goldwasser S, Micali S, Rackoff C. The Knowledge Complexity of Interactive Proof Systems[J]. SIAM Journal on Computing, 1989, 18(1): 186-208.

DOI: 10.16182/j.issn1004731x.joss.23-FZ0813E