Wang, Pu; He, Limei; Yan, Zheng; Feng, Wei

AnonyTrust: An Anonymous Trust Authentication System for Pervasive Social Networking

Published in:
Security and Privacy in Digital Economy - 1st International Conference, SPDE 2020, Proceedings

DOI:
10.1007/978-981-15-9129-7_44

Published: 01/01/2020

Document Version
Peer-reviewed accepted author manuscript, also known as Final accepted manuscript or Post-print

Please cite the original version:
Wang, P., He, L., Yan, Z., & Feng, W. (2020). AnonyTrust: An Anonymous Trust Authentication System for Pervasive Social Networking. In S. Yu, P. Mueller, & J. Qian (Eds.), *Security and Privacy in Digital Economy - 1st International Conference, SPDE 2020, Proceedings* (pp. 643-660). (Communications in Computer and Information Science; Vol. 1268 CCIS). Springer. https://doi.org/10.1007/978-981-15-9129-7_44

AnonyTrust: an Anonymous Trust Authentication System for Pervasive Social Networking

Pu Wang[1], Limei He[1], Zheng Yan[1,2], and Wei Feng[1]

[1] Xidian University, Xi'an Shaanxi 710071, China
wangpu03@gmail.com
[2] Aalto University, Espoo 02150, Finland
zyan@xidian.edu.cn; zheng.yan@aalto.fi

Abstract. Pervasive social networking (PSN) is facilitating and enriching people's lives at any time and in any places with the heterogeneous networks. One of the most important issues in PSN is its security and privacy, since users hope their privacy not be disclosed in social activities. Trust relationship plays a crucial role in PSN system, and can be utilized to support trustworthy PSN system with anonymous authentication. Thus, this paper propose AnonyTtrust, an anonymous trust authentication scheme to authenticate identities and trust levels of users with privacy preservation. It also achieves conditional traceability with a trusted server (TS), as well as online and offline state switching with multiple authorized access points (APs). The security analysis, and performance evaluation of the scheme show that the scheme is efficient regarding to security, privacy preservation, computational complexity, and communication cost. In order to test the feasibility of the proposed scheme, a lightweight secret chat application called AnonyChat is developed in practice. The results show that AnonyChat performs well and efficiently in the Android system.

Keywords: Anonymous Authentication · Trust Management · Pervasive Social Networking.

1 Introduction

With the advent of the Internet era, pervasive social networking (PSN) is facilitating and enriching people's lives with all kinds of services [1–3]. One of the most important issues in PSN is its security, trust and privacy [4]. Thus, users want to perform identity authentication to ensure their personal and property security. Meanwhile, users also hope their privacy, such as identity information and geographical location, not be disclosed. Therefore, anonymous authentication has become an important technique to ensure the security and reliability of PSN systems. But anonymous authentication also brings risks to the network, that is, malicious users may abuse anonymity to do illegal and immoral things The existence of malicious users and unknown social relationships make it hard for users to verify the trust of other users and their messages in PSN. Therefore, how to authenticate the identity and trust of users while keeping anonymity to preserve privacy becomes an important issue in PSN systems.

However, few existing works studied this issue in the literature [5, 6]. Traditional anonymous authentication schemes mainly focus on protecting identities of users, such as pseudonyms-based [7], group signature [8, 9] and blind signature [10]. For example,

pseudonyms are applied in social networking to hide real identities and avoid privacy tracking [7]. The pseudonyms changed frequently will negatively influence the efficiency of authentication and pseudonyms management. Shao et al. proposed a protocol based on the group signature to achieve a threshold authentication for privacy preservation [11], but with the group revocation problem. Nevertheless, most of the existing schemes only realize the anonymous authentication, yet not considering to build the trust relationship among PSN users. They also fail to satisfy the security and performance requirements of PSN due to specific features of PSN, such as heterogeneous, high mobility and lacking trust in nature.

To address the above issue, Yan, and Feng et al. [12] proposed an anonymous authentication scheme based on trust value issued by a centralized TS. Users can authenticate each other about identity and trust without disclosing any private information. But the centralized structure cannot support the heterogeneous and complex PSN network topology, as well as the scalability and flexibility. Yan and Wang et al. [13] alleviate the dependence of the trusted central server in a distributed manner, but the computational and communication overhead still needs further improvement. Notable, it is necessary to apply and test such the anonymous trust authentication scheme in a practical system, especially for mobile devices with limited resources, such as computation, storage and network.

In this paper, we propose AnonyTrust, a semi-distributed anonymous trust authentication system to secure PSN and assist user social decisions. In such a PSN system, the trust value of each user is evaluated by TS and/or APs, which will issue up-to-date trust lists for anonymously authenticating the identity and trust of users and their message. The proposed scheme can flexibly support the online state with the help of TS and offline states with APs for users to authenticate each other, which is appropriate to PSN features. With trust value monitored by TS, APs and even PSN users, the malicious users can be rapidly detected and their message will be rejected, to avoid group revocation. Specifically, the contributions of this paper can be summarized as below:

- We propose an anonymous trust authentication scheme in the PSN system to preserve privacy along with anonymity, unforgeability, unlinkability and conditional traceability. It adopts semi-distributed architecture to support users with online and offline states.
- We confirm the security of the proposed scheme by extensive analysis and security proof, and validate the advantages through simulation-based evaluation and comparison.
- A lightweight secret chat application called AnonyChat is developed in Android devices to show efficiency performance, such as message delay, CPU utilization, memory usage and communication cost.

The remainder of the paper is organized as follows. A summarization of related work is given in Section 2. Section 3 briefly overviews the system model of AnonyTrust and details the anonymous trust authentication scheme. Section 4 gives the security analysis and performance evaluation. A secret chat APP developed based on AnonyTrust si presented in Section 5. Section 6 concludes the paper.

2 Related Work

Lindell [14] formally defined the requirement of anonymous authentication, which has been widely studied in Vehicular Ad Hoc Networks (VANETs) and Wireless Body Area Networks (WBANs) to preserve privacy without exposing real identities. But most anonymous authentication research mainly focused on security requirements and performance promotion. Pseudonym-based authentication, as one of the methods, has widely been studied in mobile networks to protect privacy while communicating without real identities [15,16]. Emura et al. [16] proposed a secure and anonymous communication protocol for user authentication with privacy preservation based on identity-based encryption solutions. Lin and Li [17] proposed a cooperative message authentication scheme for VANETs, in which vehicles can verify an evidence token from a Trusted Authority (TA) to check whether other vehicles truly verify the message their claimed with pseudonyms as their identities. However, both schemes face challenges of the computation cost and suffer from scalability and message loss problems.

On the other hand, group signature and blind signature are another most commonly used techniques of anonymous authentication [6], [18], [19]. Zhang and Cui [20] proposed an attribute encryption scheme for ciphertext based on the group signature, which can protect sensitive information to avoid privacy disclosure. Shao, et al. [11] presented an authentication protocol for VANETs with the group signature scheme to achieve a threshold authentication. An anonymous authentication scheme was proposed based on the group signature for authenticating trust levels rather than identities of nodes in order to avoid privacy leakage and guarantee secure communications in PSN [21]. These schemes can well resist selective plaintext attacks, but the revocation of group members is a difficult problem. Ren and Lou [10] combined the blind signature and hash chain to design an anonymity scheme with privacy preservation in pervasive computing environments. Users get blind signature certificates from service providers to prove their legitimacy, which is verified by service providers without knowing the real identity of users. Based on the blind signature, Huszti [22] proposed a multi-supplier that provides anonymity for the customers. In the micro-payment system, customers can be authenticated anonymously through blind signature by multiple vendors. However, these solutions mainly depend on a central server, which distributes and manages the key pairs and its certificate, for anonymous authentication. They cannot support decentralized authentication when the server is offline, as well as scalability and flexibility in PSN networks.

Trust plays an important role and can be applied to support anonymous authentication in PSN, such as the enhanced distributed reputation system in MANET [23], securing communication data [24], and cloud data access control [25,26] Zhao et al. [27] proposed a trust model of VANET to theorize the trust relationship in the dynamic traffic environment. In such a system, vehicles can perform verification through a trust chain with the evaluated vehicular trustworthiness in the trust model. However, this scheme only focuses on the design of the trust evaluation model, but does not provide anonymous authentication between users. Yan and Feng [12] propose an anonymous trust authentication scheme depending on a centralized TA to issue a list of trust values. It cannot support a distributed PSN topology where APs can play a role like TS to evaluate and issue the trust value. Besides, an anonymous authentication scheme in [13] can alleviate the dependence of the system on trusted central servers, but the

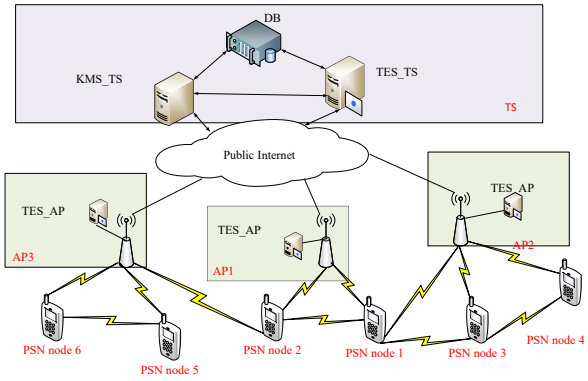


Fig. 1: System Model of AnonyTrust.

computational and communication overhead still needs further improvement. Also, all solutions above only mathematically analyzed the performance, without applying and testing in a real system, especially for mobile devices with limited resources, such as computation, storage and network.

3 Anonymous Trust Authentication Scheme

This section gives an overview of the system architecture, and details the proposed anonymous authentication scheme in which both users' identity and global trust level can be verified with preserving privacy.

3.1 Overview of AnonyTrust

As shown in Fig. 1, the entities in the model are divided into TS (Trusted Server), AP (Authorized Party) and PSN nodes (or users). This paper assumes that TS is trustworthy and will not reveal user privacy due to business motivation. Its functions are mainly divided into three parts: KMS_TS (Key Management Server of TS), TES_TS (Trust Evaluation Server of TS) and DB (DataBase).

KMS_TS handles registration requests from APs and PSN users and manages their identities and the corresponding long-term keys. For nodes whose trust value does not satisfy the condition, KMS_TS will not grant them access permission. TES_TS is responsible for collecting feedback from users, and evaluating and updating the trust of all users in the network. According to evaluation results, TES_TS publishes $token_{TS}$ and $list_{TS}$ related to trust values to trusted users. DB is responsible for storing the identity information, key information and user feedback of APs and PSN nodes.

AP is semi-trusted, a stable and reliable service device. Its main function is to evaluate and update the trust value of PSN nodes within its coverage. Similarly, it will issue $token_{AP}$ and trust value related $list_{AP}$. The purpose of this design is to enable users to authenticate each other when TS is not available, to achieve a semi-distributed effect. On the other hand, the introduction of AP can support users to authenticate

offline, thus reducing the dependence of users on TS. Although AP is responsible for the trust evaluation of PSN nodes, it does not know the real identity of users, but only the temporary identity.

PSN nodes will authenticate each other regarding the identity and trust value with $list_{TS}$ or $list_{AP}$ issued from TS or AP, correspondingly. Notably, nodes can switch between off-line only with help of APs and on-line state with both TS and APs according to their communication needs. To better understand the online and offline states of PSN nodes, we named and labeled PSN nodes in Fig. 1 where PSN node 1 connects AP1 and AP2 simultaneously. When it is online, it can anonymously authenticate with all online PSN nodes through TS. When it is offline, it can only anonymously authenticate with local user PSN node 2 through AP1, as well as PSN nodes 3 and 4 through AP2. It should be noted that in rare cases, PSN node 1 hopes to anonymously authenticate with PSN nodes 5 and 6, at which time it must adopt an online state with the assistance of TS.

Besides, the behavior of PSN nodes is uncertain, and there may be malicious behavior, such as eavesdropping other people's private information, spreading rumors. PSN nodes hope that their identity will not be disclosed in the communication, meanwhile authenticating the trust and identity of others Thus, TS is responsible for trust evaluation and distribution with all feedback from PSN nodes and APs, which can be utilized for authentication at PSN nodes. In some scenarios, PSN nodes only can obtain incomplete trust information from multiple APs without TS, they will verify the trust level of the sender after receiving anonymous messages. On the other hand, the PSN nodes can evaluate the trust value of senders according to the content of the anonymous message and their behavior, which is finally uploaded to TES_AP or TES_TS as feedback for trust evaluation. Therefore, the trust value of PSN nodes will be periodically updated with all new feedback.

In the proposed network architecture, nodes can choose their network state, i.e. online state and offline state, to communicate with other users. The offline state can support anonymous authentication between users within the coverage of the same APs. On the one hand, it enhances the stability of the system and prevents users from being unable to authenticate each other, when they cannot connect to the TS. On the other hand, it reduces the communication and computing overhead between users and the TS.

This paper only focuses on the secure and reliable anonymous authentication and communication between PSN nodes with the assistance of TS and APs. The communication between TS and PSN nodes, AP and PSN nodes, and between AP and TS is assumed to be based on secure channels, such as Diffie-Hellman protocol.

3.2 Preliminaries

Bilinear pair is a powerful tool for constructing digital signatures. Assume q is a large prime number related to a given security constant k, G is a cyclic additive group generated by P, GT is a cyclic multiplicative group, $|G| = |GT| = q$. bilinear map $e : G \times G \to GT$ satisfies the following properties:

- **Bilinear:** For $\forall P, Q \in G$, $a, b \in Z_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$.
- **Non-degenerate:** There exist $P, Q \in G$ that $e(P, Q) \neq 1_{GT}$.
- **Computable:** For $\forall P, Q \in G$, $e(P, Q)$ can be computed by polynomial-time algorithm.

Table 1: Notations

Notation	Description
sk_{TS}, pk_{TS}	Secrete and public key of TS
ID_i, ID_{ap}	Identity of user i and ap
sk_{ap}, pk_{ap}	Private and public key of ap
$cert_{ap}$	Public key certificate of ap
$tempID_i$	Temp identity of i
$info_i$	Personal information of i
sk_i, pk_i	Long-term private and public key of i
$cert_i$	Long-term public key certificate of i
s_i	Secret between i and TS
Q_i	Multi-scalar multiplication of s_i and P
tv_i_TS, tv_i_ap	Trust value of i from TS and ap
$token_i$	Token of i's trust value
$secre\_token_i$	Token of $token_i$
$list$	Trust related list
$\boldsymbol{P}_i$	Short-term public key vector of i
$\boldsymbol{temp\_sk_i}$	Short-term private key vector of i

The following cryptographic problems ensure that bilinear pairings can be used to construct digital signatures safely:

- **Discrete Logarithm Problem (DLP Problem):** Given $P, Q \in G$, compute $a \in Z_q^*$ that $Q = aP$.
- **Computational Diffie-Hellman Problem (CDH Problem):** Given $P, aP, bP \in G$, in which $a, b \in Z_q^*$, compute $abP \in G$.

The notations that are usually used in this paper are summarized in Table 1.

3.3 The Proposed Scheme

Each step of this anonymous trust authentication scheme is described in detail below. Assuming that the sender i requires anonymous communication, and its corresponding authorized access point is ap (i may connect with multiple AP but with the same operation), the receiver j will verify i's trust level and authenticate the message.

System setup: Give security parameter k and generate q, group G, GT, Z_q^*, $|G| = |GT| = q$, P is the generator, and bilinear map $e : G \times G \to GT$. TS chooses master private key $sk_{TS} \in Z_q^*$ and computes the corresponding public key $pk_{TS} = sk_{TS} \cdot P$. In addition, it also chooses $H_1 : \{0,1\}^* \to \{0,1\}^n$, $H_2 : G \to \{0,1\}^n$, $H_3 : \{0,1\}^n \to G, H_4 : \{0,1\}^* \to G$. The system parameters contains $\{q, G, GT, e, P, pk_{TS}, H_1, H_2, H_3, H_4\}$.

AP Registration: ap uses its own ID_{ap} to register to TS. TS generates private key $sk_{ap} \in Z_q^*$, public key $pk_{ap} = sk_{ap} \cdot P$ and the certificate $cert_{ap} = pk_{ap} \cdot sk_{TS}$ for ap.

User registration:

- User i registers TS with his real ID (such as phone number or mailbox) and sends his necessary information $info_i$ that defined by TS.
- TES_TS uses $info_i$ and previous information to generate the trust value tv_i_TS for user i. If tv_i_TS reaches the desired threshold, TS generates the unique temporary

identification $tempID_i$. Then it chooses private key $sk_i \in Z_q^*$, public key $pk_i = sk_i \cdot P$ and public key certificate $cert_i = pk_i \cdot sk_{TS}$ for user i.
– TS sends $\{tempID_i, sk_i, pk_i, cert_i\}$ to user i through a secure channel.

Trust evaluation: When the user swicths to the offline state, TS will not serve the user, only the APs connected by user work; when the user selects online, TS and all APs connected by the user will conduct trust evaluation with its $tempID_i$.
– TS choose s_i as its secret with i, and calculate $Q_i = s_i \cdot P$. Both of the two will be sent to user i.
– TS/ap periodly updates tv_i, and generates $token_i = H_1(tv_i||tempID_i)$. Users will provide the Q_i to ap for trust evaluation services.
– TS/ap first calculates $secret\_token_i = H_1(Q_i||H_1(token_i))$ and puts it into the $list = \{secret\_token_i, ...secret\_token_j\}$. Secret tokens are arranged in ascending order of the corresponding trust values.
– TS sends $\{token_i\_TS, s_i, Q_i\}$ to i, and publishes $list_{TS}$ to all nodes of the network; ap sends $token_i\_ap$ to i and publishes $list_{ap}$ to local nodes.

Short-term key pair generation: Users will generate its short-term public and private keys based on $token_i$ and $token_i\_ap$ issued by TS and AP. Table 2 shows the short-term key pair generation algorithm with the token $token_i$ from TS (if with AP, replacing with $token_i\_ap$ in algorithm). It should be noticed that user i will choose either online or offline mode, it will connect to TS and multiple APs for receiving several tokens. Accordingly, i's public key is a vector $\boldsymbol{P_i}$ with several elements $temp\_pk_i$, composed of $temp\_pk_i\_1$ and $temp\_pk_i\_2$. User i's secret key is $temp\_sk_i$. $|\boldsymbol{P_i}\_\boldsymbol{2}|$ is the XOR result of all $temp\_pk_i\_2$.

Table 2: Short-term Key Generation

Input: $token_i$, s_i, Q_i
Output: $temp\_pk_i$, $temp\_sk_i$
a) compute $temp\_pk_i$ $temp\_pk_i\_1 = H_1(a \oplus H_2(Q_i))$ $temp\_pk_i\_2 = temp\_pk_i\_1 \oplus H_1(token_i)$ b) compute $temp\_sk_i$ $temp\_sk_i = s_i \cdot H_3(temp\_pk_i\_1) + s_i \cdot H_3(\|\boldsymbol{P}_i\_2\|)$

Signature generation: User i uses $temp\_sk_i$ to generate the signature of message m, $sig(m) = temp\_sk_i + H_4(m) \cdot s_i$. The user i sends $\{m, sig, \boldsymbol{P_i}, Q_i\}$.

Signature verification: The whole process of message verification is shown in Table 3.

Table 3: Signature Verification

Input: $temp\_pk_i$, Q_i, m, sig
Output: true, false
1) if (at least one $secret\_token$ was found) goto 2); else return false;
2) if ($e(sig, P) = e(H_3(temp\_pk_i\_1) + H_3(\|\boldsymbol{P}_i\_2\|) + H_4(m), Q_i)$) goto 3); else return false;
3) if ($tv_i > threshold$) return true; else return false;

– a) Verify the identity legitimacy of message signers. First calculate $H_1(token) = temp\_pk_i\_2 \oplus temp\_pk_i\_1$, and calculate $secret\_token = H_1(Q_i||H_1(token))$. Then

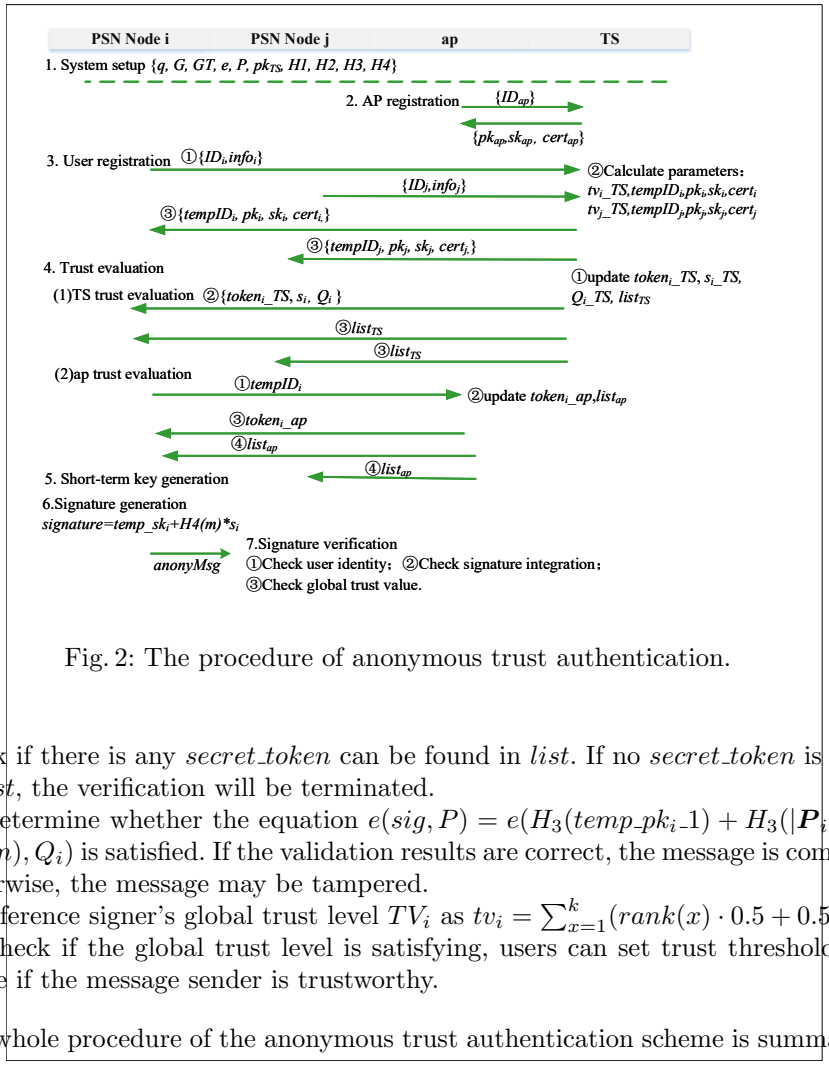


Fig. 2: The procedure of anonymous trust authentication.

check if there is any *secret_token* can be found in *list*. If no *secret_token* is found in *list*, the verification will be terminated.

- b) Determine whether the equation $e(sig, P) = e(H_3(temp\_pk_i\_1) + H_3(|\boldsymbol{P}_i\_2|) + H_4(m), Q_i)$ is satisfied. If the validation results are correct, the message is complete; otherwise, the message may be tampered.
- c) Inference signer's global trust level TV_i as $tv_i = \sum_{x=1}^{k}(rank(x) \cdot 0.5 + 0.5)/k$.
- d) Check if the global trust level is satisfying, users can set trust threshold, and judge if the message sender is trustworthy.

The whole procedure of the anonymous trust authentication scheme is summarized in Fig. 2.

4 Security Analysis & Performance Evaluation

In this section, the security of the proposed scheme is proved theoretically and analyzed in order to show the correctness, anonymity, unforgeability, traceability and nonrepudiation. Then, we analyze and evaluate its performance about computation and communication cost.

4.1 Security Analysis

1) Correctness: the correctness of the signature verification can be proved as follows:

$$e(sig, P) = e(temp\_sk_i + H_4(m) \cdot s_i, P) \tag{1}$$

$$= e(s_i \cdot H_3(temp\_pk_i\_1) + s_i \cdot H_3(|\boldsymbol{P}_i\_2|) + H_4(m) \cdot s_i, P)$$
$$= e(H_3(temp\_pk_i\_1) + H_3(|\boldsymbol{P}_i\_2|) + H_4(m), P \cdot s_i)$$
$$= e(H_3(temp\_pk_i\_1) + H_3(|\boldsymbol{P}_i\_2|) + H_4(m), Q_i)$$

2) Anonymity: The receiver can get are Q_i, $temp\_pk_i\_1$, $temp\_pk_i\_2$, $list_{ap}$, $list_{TS}$, m, sig, and compute $H1(token_i)$ and $secret\_token_i$. Q_i is an element on G and has nothing to do with real identity because of DLP problem. $temp\_pk_i\_1$ and $temp\_pk_i\_2$ generated by $token_i$, random number a and Q_i, are hash value that seems to be a random value for receiver. Also, $H_1(token_i)$, $secret\_token_i$, $list_{ap}$ and $list_{TS}$ are only related to the hash value of $token_i$, so a receiver can not determine the identity of the sender.

3) Unforgeability: the commonly used definition of digital signature security is Existence Unforgebility under Adaptive Selective Message Attacks (EUF-CMA) [28]. EUF-CMA of AnonyTrust can be proved under the random oracle model. The prove is as follows,

Theorem 1. *For a given security parameter k, the anonymous trust authentication scheme (TAS) is secure under a random oracle model if the CDH problem holds.*

Proof. If there is a probability that attacker A can break through the scheme in time t, there is a challenger $\mathcal{C}$ that can solve the CDH problem in time t'. We assume Attacker $\mathcal{A}$ and Challenger $\mathcal{C}$ interact as follows:

Step 1: $\mathcal{C}$ choose parameters $\{q, P, G, GT, e, H_1, H_2, H_3, H_4\}$ and calculates public-private key pairs (pk, sk), where pk consists of pk_1 and pk_2, and calculates $H_3(pk_1)$ and $H_3(pk_2)$.

Step 2: $\mathcal{C}$ sends pk, $H_3(pk_1)$ and $H_3(pk_2)$ to $\mathcal{A}$;

Step 3: $\mathcal{A}$ queries $\mathcal{C}$ with $H_4(x)$.

a) $\mathcal{C}$ maintains a list of $(n, x, H_4(x))$ as H_4_List which is empty at the beginning.

b) When input $x*$ appears in H_4_List, return $H_4(x*)$. If not, $rand* \in 0, 1$ is randomly generated, where $Pr[rand* = 1] = \delta$. If $rand* = 0$, return $H_4(x*) = nP$; else, $rand* = 1$, $H_4(x*) = nP + bP$, $n \in Z_q^*$.

c) Return $H_4(x*)$ to $\mathcal{A}$, and add $(n, x*, H_4(x*)$ to H_4_List.

Step 4: $\mathcal{A}$ queries to $\mathcal{C}$ with $sig(m)$

a) $\mathcal{C}$ maintains a list of $(m*, H_4(m*), sig(m*))$ as $signList$ which is empty at the beginning.

b) $\mathcal{A}$ should ask for $H4(m*)$ before inquiring for $sig(m*)$ from $\mathcal{C}$. If $H4(m*)$ is not inquired before, the $\mathcal{C}$ will answer generate $(m*, H_4(m*))$.

c) When the input $m*$ appears in the list $signList$, it returns $sig(m*)$; when the input $m*$ is not in the list, if $rand* = 0$, it calculates $\sigma = a \cdot H_3(pk_1) + a \cdot H_3(pk_2) + a \cdot H_4(m*)$; else, terminates the response.

d) Returns $sig(m*)$ to $\mathcal{A}$ and adds $(m*, H_4(m*), sig(m*))$ to the list.

Step 5: $\mathcal{A}$ forges signatures, if $\mathcal{A}$ forges $sig(m')$, then $rand* = 1$, the following equation holds: $\sigma' = a \cdot H_3(pk\_1) + a \cdot H_3(pk\_2) + abp + anp$.

Thus, $abp = \sigma' - a \cdot H_3(pk\_1) - a \cdot H_3(pk\_2) - anp$. So $\mathcal{C}$ can obtain abp as a solution of CDH problems. If $\mathcal{A}$ breaks through the scheme with a non-negligible probability ϵ in time t, then $\mathcal{C}$ can solve the probability of CDH with probability $\epsilon' >= \delta(1-\delta)^{q_S}\epsilon >= \epsilon/(q_S e)$, e is a natural number. Then, $\epsilon <= q_S \cdot e \cdot \epsilon'$. □

4) Conditional traceability: TS can determine the signer of a message through the corresponding relationship between temporary ID and user's real ID, so the scheme achieves conditional traceability, which is one of the acceptable and desired properties in PSN. But if TS is not involved in the PSN, such a dispute cannot be solved. Thus, we suggest that for crucial PSN communications, TS should be involved in order to guarantee system safety and at the same time preserve node privacy.

4.2 Performance Analysis

1) Computation cost

We mainly focus on the computation cost of key algorithms, such as short-term key generation, signature generation and signature verification. By comparing our scheme with [5] and [29], the analysis results are summarized as shown in Table 4. We de-

Table 4: Analysis and Comparison of Computation Cost

Scheme	Short-term key	signature	verification
AnonyTrust	$2C_{GZ} + C_G$	$C_{GZ} + C_G$	$2C_G + 2C_e$
[5]	$2C_{GZ}$	$C_{GZ} + C_G$	$C_{GT} + 3C_e$
[29]		$3C_{GZ}$	$2C_{GZ} + C_G + C_e$

fine cost of pairing as C_e, as well C_G, C_{GZ}, C_{GT} is the cost of add and multiplication operation of G and multiplication operation of GT, correspondly. $\oplus$, $|\cdot|$ and other operations are not considered here because they are simple operation in groups compared operations above. According to implementation in next subsection, we obtain that the C_{GZ} and C_e are most time-consuming operations. The compared result will be given with the evaluation results

2) Communication cost

The data frequently transmitted in this scheme are *token*, *list* and *anonymsg*. With n users and k APs, we can obtain the communication cost as Table 5. Only data length of *list* is linear with the number user, but it is distributed by TS while registering and only updated when needing. Besides, the number of APs is not large. Thus, communication cost in the proposed scheme is reasonable.

Table 5: Communication Data Length

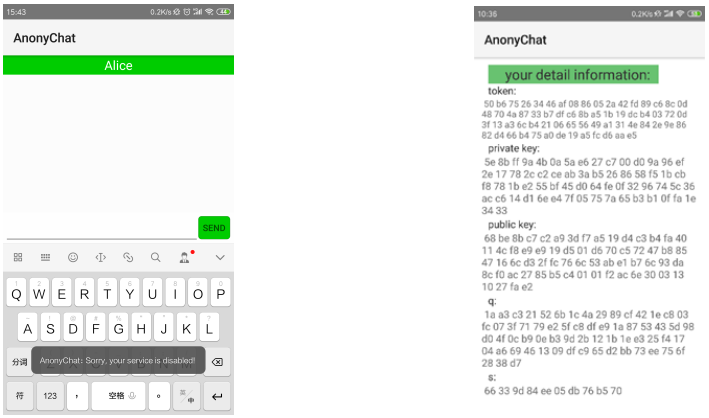
Data type	Content	Data length
token	MD5	16
list	$\{secret\_token_1, ...,\}$	$16n$
anonymsg	$\boldsymbol{P}_i, Q_i, sig, m$	$16 + 16k + 64 + m + 64$

Table 6: Operation Time Comparison (ms))

Scheme	short-term key	signature	verification
1 token	14.724	3.268	46.402
5 token	16.981	3.275	47.453
[5]	14.127	3.142	65.051
[29]	8.045	9.076	27.029

4.3 Performance Evaluation

We implemented the proposed scheme in Java language using a JPBC library on a desktop (running 64-bit Windows OS, equipped with Intel Core i5-3230M @2.60GHz).



(a) (b)

Fig. 3: Access control based on user trust

We mainly focus on the computational performance of short-term key generation, signature generation and signature verification.

We assume that users use $num = 1$ (only TS) or $num = 5$ tokens (for TS and 4 APs) to authenticate anonymously, and then test their performance compared with [5] and [29]. The average computational time for each stage is shown in Table 6. The time of short-term key generation of 5 tokens is a little longer than that in 1 token, but the computing time of other stages is very close. Thus, multiple tokens do not affect the computing performance of the scheme very much. Besides, compared with [5] and [29], the short-term key generation time of our scheme is the longest. This is because the public key is generated in two parts to realize anonymity, message verification and trust value authentication. The signature generation is the same as [5], but more efficient than [29] because of more C_{GZ} operations shown in Table 4. For signature verification, our scheme is faster than [5], but longer than [29]. That is because the proposed scheme realizes both authenticating the identity and integrity of the message at the same time, as well as verify its trust level. As can be seen from the above analysis and evaluation results, the proposed scheme can achieve trust authentication at a low computational cost.

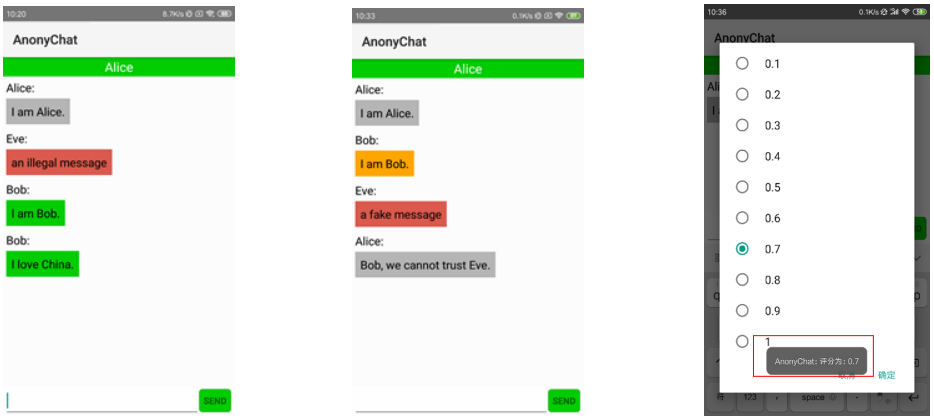
5 Application and Experimental Results

This section presents a secret chat APP: AnonyChat on Android devices and then gives the experimental results, such as running efficiency, message delay, CPU occupancy, memory occupancy and communication overhead.

5.1 Function Design

1) Access control based on user trust

As shown in Fig. (3a), when a user sends a login request, the server will verify his/her trust value. If the user's trust value is lower than the threshold (set to 0.56),



(a) (b) (c)

Fig. 4: (a)(b) Anonymous chat interface, (c) Trust rating feedback interface

a pop-up window will prompt the user that he/she has been denied. As shown in Fig. (3b), a user can check his/her detailed information like the token, short-term key.

2) Anonymous chat

Fig. (4a) and Fig. (4b) shows the chat interface. After receiving a message, a user first verifies the identity of the sender by checking whether its *secret_token* is in the trust-related list. If it does not exist, the message bubble is red and "an illegal message" is displayed. Then the correctness of the signature is verified. If it fails, the bubbles are shown in red and "a fake message" is displayed. Finally, the trust value of the sender is computed. If lower than the threshold (0.6), the bubble of the message is yellow, and the normal content of the message is displayed. Otherwise, the bubble of the message is green.

3) Rating feedback

As shown in Fig. (4c), when a user clicks on a certain message, AnonyChat will pop up the scoring dialog box for users to score the corresponding message. The score results will be sent as feedback to TS or APs for updating the trust value related list.

5.2 Experimental Results

1) Message delay

In this paper, AnonyChat is tested on Xiaomi 6, 6G RAM, 835 2.45GHz CPU. When the density of messages is 2/sec - 10/sec, the average delay of messages changes with time as shown in Fig. 5. When the message density is less than 8/sec, the delay keeps stable as 150 ms. When reaching 8/sec, the message delay will increase slightly, but the delay lasting for 5 seconds is only 240 ms. When reaching 10/sec, the message delay can rise to 800 ms in 5 seconds, which is unfriendly for users. Thus, 10/sec can be viewed as the limit of AnonyChat's message density. This is because the time interval between messages transmission is less than the time needed for encryption and decryption, so there is a blockage of message processing in the client. In practice, sending and receiving messages at a density of 8/sec can already meet the actual needs of users for most of the time, but it is necessary to improve it in the future.

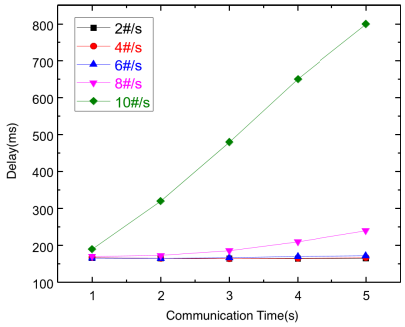


Fig. 5: Performance evaluation on message delay

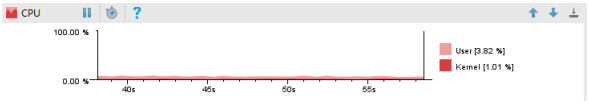


Fig. 6: Performance evaluation on CPU usage

2) CPU usage, memory usage and communication consumption

CPU usage, memory usage and communication consumption are three commonly used performance indicators for mobile applications. This paper will assume an extreme situation is the density of messages is 10/s to test performance. From Fig. 6, AnonyChat occupies lower than 4% of the CPU even in extreme cases, so it does not consume too much system resources of Android devices. As shown in Fig. 7, AnonyChat generally occupies about 4M-5M of memory even in extreme cases, so it is very lightweight. For communication cost, the traffic consumption of AnonyChat is less than 5KB/s, very little traffic even in extreme cases, as shown in Fig. 8. Therefore, the resource usage of AnonyChat can be neglected to present smartphones.

6 Conclusion

This paper proposed an anonymous trust authentication scheme, which can ensure the security of user messages and the anonymity of identity, while helping users verify the trust level of anonymous sources. In the proposed scheme, TS is responsible for the management of all PSN entities, evaluates and issues the trust value of PSN users along with APs. Based on the token of trust value, cryptographic algorithms and the authentication protocol were constructed to realize anonymous trust authentication for PSN users. This scheme adapted a semi-distributed architecture and introduced authorized APs to overcomes the problem of over-reliance on central TS. Thus, PSN users can switch online and offline states to authenticate with each other. Through security analysis and performance evaluation, the scheme realized secure and trusted anonymous authentication among users with high computational efficiency. Then, AnonyChat was developed to verify in Android devices. The results demonstrated that the application is very lightweight and performs well about message delay, CPU usage, memory usage and communication cost.

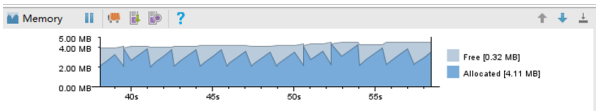


Fig. 7: Performance evaluation on memory

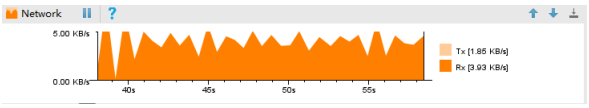


Fig. 8: Performance evaluation on communication

Acknowledgement

The work is supported in part by the National Natural Science Foundation of China under Grants 61672410 and 61802293, the Academy of Finland under Grants 308087 and 314203, the Key Lab of Information Network Security, Ministry of Public Security under grant No. C18614, the open grant of the Tactical Data Link Lab of the 20th Research Institute of China Electronics Technology Group Corporation, P.R. China under grant CLDL-20182119, the Shaanxi Innovation Team project under grant 2018TD-007, and the 111 project under grant B16037.

References

1. Z. Yan, K. Zeng, Y. Xiao, P. Samarati, et al. Guest editorial special issue on trust, security, and privacy in crowdsourcing. *IEEE Internet of Things Journal*, 5(4):2880–2883, 2018.
2. A. Ahtiainen, K. Kalliojarvi, M. Kasslin, K. Leppanen, A. Richter, P. Ruuska, and C. Wijting. Awareness networking in wireless environments. *IEEE Vehicular Technology Magazine*, 4(3):48–54, 2009.
3. Shen X, H. Yu, J. Buford, and M. Akon. *Handbook of peer-to-peer networking*, volume 34. Springer Science & Business Media, 2010.
4. Z. Yan, Y. Chen, and Y. Shen. A practical reputation system for pervasive social chatting. *Journal of Computer and System Sciences*, 79(5):556–572, 2013.
5. C. Zhang, R. Lu, X. Lin, P. Ho, and X. Shen. An efficient identity-based batch verification scheme for vehicular sensor networks. In *IEEE INFOCOM 2008-The 27th Conference on Computer Communications*, pages 246–250. IEEE, 2008.
6. A. Wasef and X. Shen. Efficient group signature scheme supporting batch verification for securing vehicular networks. In *2010 IEEE International Conference on Communications*, pages 1–5. IEEE, 2010.
7. J. Liu, Z. Zhang, X. Chen, and K. Kwak. Certificateless remote anonymous authentication schemes for wirelessbody area networks. *IEEE Transactions on parallel and distributed systems*, 25(2):332–342, 2013.
8. D. Boneh, X. Boyen, and H. Shacham. Short group signatures. In *Annual international cryptology conference*, pages 41–55. Springer, 2004.
9. Y. Lee, S. Han, S. Lee, B. Chung, and D. Lee. Anonymous authentication system using group signature. In *2009 International Conference on Complex, Intelligent and Software Intensive Systems*, pages 1235–1239. IEEE, 2009.

10. K. Ren, W. Lou, K. Kim, and R. Deng. A novel privacy preserving authentication and access control scheme for pervasive computing environments. *IEEE Transactions on Vehicular technology*, 55(4):1373–1384, 2006.
11. J. Shao, X. Lin, R. Lu, and C. Zuo. A threshold anonymous authentication protocol for vanets. *IEEE Transactions on vehicular technology*, 65(3):1711–1720, 2015.
12. Z. Yan, W. Feng, and P. Wang. Anonymous authentication for trustworthy pervasive social networking. *IEEE Transactions on Computational Social Systems*, 2(3):88–98, 2015.
13. Z. Yan, P. Wang, and W. Feng. A novel scheme of anonymous authentication on trust in pervasive social networking. *Information Sciences*, 445:79–96, 2018.
14. Y. Lindell. Anonymous authentication. *Journal of Privacy and Confidentiality*, 2(2), 2011.
15. X. Lin, X. Sun, X. Wang, C. Zhang, P. Ho, and X. Shen. Tsvc: Timed efficient and secure vehicular communications with privacy preserving. *IEEE Transactions on Wireless Communications*, 7(12):4987–4998, 2008.
16. F. Sato, H. Takahira, and T. Mizuno. Message authentication scheme for mobile ad hoc networks. In *11th International Conference on Parallel and Distributed Systems (ICPADS'05)*, volume 1, pages 50–56 Vol. 1, 2005.
17. X. Lin and X. Li. Achieving efficient cooperative message authentication in vehicular ad hoc networks. *IEEE Transactions on Vehicular Technology*, 62(7):3339–3348, 2013.
18. L. Zhang, Q. Wu, A. Solanas, and J. Domingo-Ferrer. A scalable robust authentication protocol for secure vehicular communications. *IEEE Transactions on vehicular Technology*, 59(4):1606–1617, 2009.
19. Y. Hao, Y. Cheng, C. Zhou, and W. Song. A distributed key management framework with cooperative message authentication in vanets. *IEEE Journal on selected areas in communications*, 29(3):616–629, 2011.
20. X. Zhang and Y. Cui. Attribute-based encryption schema with group signatures. *Chinese Journal of Network and Information Security*, 5(1):15–21, 2019.
21. W. Feng, Z. Yan, and H. Xie. Anonymous authentication on trust in pervasive social networking based on group signature. *IEEE Access*, 5:6236–6246, 2017.
22. A. Huszti. Anonymous multi-vendor micropayment scheme based on bilinear maps. In *International Conference on Information Society (i-Society 2014)*, pages 25–30. IEEE, 2014.
23. Z. Yan, P. Zhang, and A. Vasilakos. A survey on trust management for internet of things. *Journal of network and computer applications*, 42:120–134, 2014.
24. N. Li, Z. Yan, M. Wang, and L. Yang. Securing communication data in pervasive social networking based on trust with kp-abe. *ACM Transactions on Cyber-Physical Systems*, 3(1):1–23, 2018.
25. Z. Yan and W. Shi. Cloudfile: A cloud data access control system based on mobile social trust. *Journal of Network and Computer Applications*, 86:46–58, 2017.
26. Z. Yan and M. Wang. Protect pervasive social networking based on two-dimensional trust levels. *IEEE Systems Journal*, 11(1):207–218, 2014.
27. H. Zhao, D. Sun, H. Yue, M. Zhao, and S. Cheng. Dynamic trust model for vehicular cyber-physical systems. *IJ Network Security*, 20(1):157–167, 2018.
28. S. Goldwasser, S. Micali, and R. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on Computing*, 17(2):281–308, 1988.
29. X. Cao, X. Zeng, W. Kou, and L. Hu. Identity-based anonymous remote authentication for value-added services in mobile networks. *IEEE Transactions on Vehicular Technology*, 58(7):3508–3517, 2009.