分散型 SNS 基盤のための共通ランデブ・ポイント・インターフェースの提案

蛸井　博[†]　新城　靖[†]
佐藤　聡[†]　中井　央[†]

1. はじめに

現在、Social Networking Service (SNS)がコミュニケーションツールとして、広く利用されている。それらの多くは、中央サーバに依存する集中型 SNS である。ユーザは中央サーバを信頼し、プライバシに関わる情報を預けなければならない。また、SNS の運営が終了し、情報が失われることがある。

これに対し、分散型 SNS が提案されている。分散型 SNS は、サーバの連邦化や Distributed Hash Table (DHT)によって SNS を構築する[1]。相手と Peer-to-peer (P2P)で通信するには、何らかの手段を用いて、IP アドレスなどの接続情報を相手と交換する必要がある。このとき利用する場所を、ランデブ・ポイントと呼ぶ。

本研究室ではこれまで、ソーシャル VPN やソーシャルルータ、SocialSocket といった分散型 SNS の通信基盤を開発してきた。ランデブ・ポイントの実装には、集中型 SNS や eXtensible Messaging and Presence Protocol (XMPP)サーバを用いていた。しかし、それらの実装はそれぞれ独自に行っていたため、再利用性が低いという問題があった。

この問題に対し本研究では、分散型 SNS 基盤からランデブ・ポイントの実装を分離し、利用法を共通化するために、**共通ランデブ・ポイント・インターフェース**を実装する。本インターフェースは、通信対象とランデブ・ポイントの組合せを管理するコンタクトリストを持つ。分散型 SNS 基盤は、本インターフェースの Web API を通じて様々な種類のランデブ・ポイントを簡単に利用できる。

2. 共通ランデブ・ポイント・インターフェース

本研究では、共通ランデブ・ポイント・インターフェースを実装する。これにより、ランデブ・ポイントの実装の再利用が可能となる。また、特定のランデブ・ポイントを実装したサービスが終了しても、他のランデブ・ポイントに切り替えることが簡単になる。本研究の提案手法の全体図を図 1 に示す。各分散型 SNS 基盤は、共通ランデブ・ポイント・インターフェースを通して、ランデブ・ポイントを利用する。各分散型 SNS 基盤は共通ランデブ・ポイント・インターフェースにだけ対応すれば、複数のランデブ・ポイントが利用可能になる。

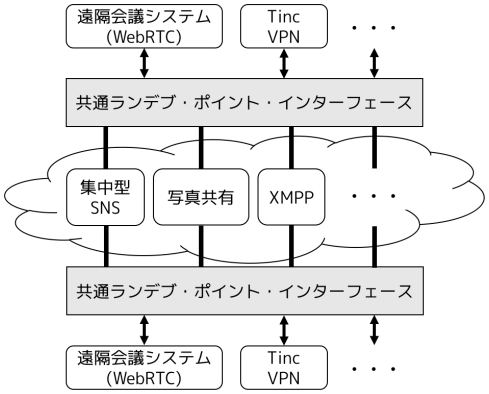

図 1 共通ランデブ・ポイント・インターフェース

共通ランデブ・ポイント・インターフェースは、Web Application Programming Interface (API)、Web User Interface (UI)、およびコンタクトリストを提供する。分散型 SNS 基盤は Web API と通信する。集中型 SNS の提供する API を利用して、ランデブ・ポイントを実装するために、集中型 SNS のユーザ認証で保護された Web アプリケーション、およびその Web UI も持つ。コンタクトリストは、分散型 SNS 基盤の通信対象(メンバ)とランデブ・ポイントの関係を管理する。

† 筑波大学

2.1 Web API

共通ランデブ・ポイント・インターフェースは分散型 SNS 基盤に、JavaScript Object Notation (JSON)形式を用いた次の Web API を提供する。

put: 接続情報の通信相手への通知を要求する。対象のメンバと通知する接続情報を指定する。共通ランデブ・ポイント・インターフェースは、指定されたランデブ・ポイントに、接続情報を設置する。

get: 通信相手の接続情報の取得を要求する。対象とするメンバと接続情報の種類を指定する。共通ランデブ・ポイント・インターフェースは、ランデブ・ポイントから接続情報を取得し、応答を返す。

2.2 コンタクトリスト

コンタクトリストは JSON 形式で記述し、キーとしてメンバ名を、バリューとしてランデブ・ポイント名とそれにおける識別情報の組の配列を持つ。1 人のメンバに対し、複数のランデブ・ポイントを割り当てることができる。接続情報の交換は、すべてのランデブ・ポイントに対して行う方法、ランデブ・ポイントの優先度を定め、高い順番に行う方法などによって冗長化する。これにより、いずれかのランデブ・ポイントに障害が発生した場合でも、分散型 SNS 基盤は影響を受けずに通信が可能となる。

3. 分散型 SNS ソフトウェア

本研究では、複数の分散型 SNS ソフトウェアに共通ランデブ・ポイントを実装する。現在、本研究室で開発している遠隔会議システムと、P2P 型の Virtual Private Network (VPN)ソフトウェアである Tinc VPN に実装している。遠隔会議システムは通信に WebRTC を使用しており、接続情報として Session Discription Protocol (SDP) および Interactive Connection Establishment (ICE)が必要である。Tinc VPN では、同様に IP アドレスと公開鍵が必要である。これらの情報を共通ランデブ・ポイント・インターフェースを用いて交換するよう、変更を行っている。

4. ランデブ・ポイントの実装

本研究では、様々なランデブ・ポイントを実装する。現在、集中型 SNS と写真共有サービスを用いて実装を進めている。集中型 SNS については、特定の相手を指定した情報交換、および情報の全体公開が可能な SNS をランデブ・ポイントとして実装する。写真共有サービスでは、接続情報を画像に埋め込むことで、情報の存在を隠蔽する。実現する方法として、画像内への QR コードの埋め込みとステガノグラフィがある。これらの方法により、接続情報の存在を知る者のみが、画像から情報を抽出できる。その他に DHT や XMPP サーバ、クラウドストレージ、インスタントメッセンジャ、動画共有、Short Message Service (SMS)などでランデブ・ポイントを実装することを考えている。

5. 関 連 研 究

分散型 SNS 基盤の SocialVPN[2]では、Facebook および XMPP サーバをランデブ・ポイントとして、ソフトウェアに統合する方法で実装している。また、Lorenz らの調査[1]によれば、分散型 SNS では連邦化されたサーバや DHT をランデブ・ポイントに用いている。

本研究では、共通ランデブ・ポイント・インターフェースを実装することで、分散型 SNS 基盤におけるランデブ・ポイントの個別実装が不要となる。また、通信相手に複数のランデブ・ポイントを割り当てる冗長化が可能である。

6. お わ り に

本研究では、分散型 SNS 基盤のための、共通ランデブ・ポイント・インターフェースを実装する。これにより、ランデブ・ポイントの再利用と冗長化を可能にする。現在、ランデブ・ポイントとして、集中型 SNS と写真共有サービスによる方法の実装を進めている。これまでに、遠隔会議システムと Tinc VPN から、共通ランデブ・ポイント・インターフェースを利用可能にした。

今後は、さらに多くのサービスに対してランデブ・ポイントを実装する。また、暗号化および秘密分散法による、接続情報の秘匿を実装する。メンバのグループ管理機能も実装する。

参 考 文 献

[1] L. Schwittmann, M. Wander, C. Boelmann, and T. Weis, “Privacy preservation in decentralized online social networks,” IEEE Internet Computing, No.2, pp.16-23, 2014.

[2] P. S. Juste, D. Woinsky, P. O. Boykin, M. J. Covington, and R. Figueiredo, “SocialVPN: Enabling wide-area collaboration with integrated social and overlay networks,” Computer Networks, Vol.54, No.12, pp.1926-1938, 2010.