Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

仮想化オーバレイネットワーク機構の設計

寺西裕一[†1,†4] 秋山豊和[†2] 岡村真吾[†3]
竹内亨[†4] 武本充治[†5,†4] 野本義弘[†6]

蓄積運搬転送型の送受信を含む P2P ネットワークにおいて，階層的に構成されるグループのメンバ同士で安全なメッセージ交換を行なうことを可能とする仮想化オーバレイネットワーク (VON) 機構の設計について述べる．

本稿では，メッセージに対する送信・中継ノードによる証明書の付与と，入れ子構造の暗号化により，階層構造をもつグループと蓄積運搬転送型の送受信に対応した上で，不正な挙動をするノードを排除する VON の実現法を示す．また，隣接ノード同士が直接接続可能，かつ，同一のグループに属している場合に，認証済みのセッションを構成することで，電子署名のための処理量とデータ転送量を削減する方法を提案する．

上記の各方法について，Android OS 向けのプロトタイプ実装によるフィージビリティ検証を行ない，VON 機構が携帯端末上でも動作可能であることを示した．

A Design of Virtual Overlay Network Mechanism

Yuuichi Teranishi,[†1,†4] Toyokazu Akiyama,[†2]
Shingo Okamura,[†3] Susumu Takeuchi,[†4]
Michiharu Takemoto[†5,†4] and Yoshihiro Nomoto [†6]

We propose a mechanism for *virtual overlay network* (VON) that enables message exchanges among authenticated members of hierarchical groups on P2P networks considering 'carry and forward' type message exchanges.

To enable carry and forward type message exchanges and hierarchical groups, we propose a design of VON that uses transfer certificates, which can prove the affiliated group of the message sender and forwarders, and recursive message encryptions. Moreover, our method makes authorized data sessions when adjacent nodes can directly connect to each other and both belong to the same group to reduce overhead for creating and verifying certificates and exchanging certificate data.

We also show the feasibility of above methods by implementing a prototype module on Android OS.

1. はじめに

特別なサーバ設備やインフラが無い環境であっても，利用者が持つ端末間での情報共有を低コストかつ容易に可能とする P2P ネットワークに関する研究が数多くなされている．近年では，山岳地帯等の分断された通信状況のもとであっても P2P ネットワークを構成可能とする手段として，遅延耐性ネットワーク DTN (Delay Tolerant Network) に注目が集まっている．DTN は，接続先と通信できない場合，中継地点でデータを蓄積し，通信可能となった時点で転送を行なう．これにより，従来よりもメッセージの配布率を向上させることができ，P2P ネットワークとしても適用範囲の広がりが期待できる．

P2P ネットワークが持つ利点を生かし，メッセージングやファイル交換等を行なうシステムが実用化されつつある一方で，データ漏洩等のセキュリティ上の懸念が，導入や普及における大きな障壁となっている．従来の P2P ネットワークにおけるセキュリティの研究は，改ざんやなりすましを防止する電子署名の構成方法や，情報発信元の特定を困難とする匿名化の実現法の検討が主であった．しかし，P2P ネットワークを日常の業務やサービスで利用する上では，複数のアプリケーションが同時に動作し，信頼度の異なる組織やグループの利用者が混在する状況のもと，承認された利用者やグループ内のみに閉じた情報共有ができることがより重要となる．

このような要求を満たすネットワークは，従来 VPN (Virtual Private Network) 等の下位レイヤのネットワークの枠組みによって実現されてきた．しかし，導入の敷居は高く，ネットワーク運用者による管理や設定が必要であり，アプリケーション利用者やサービス提供者が容易に導入できるものではない．また，互いに未知の端末が，外部と接続が無い状況で遭遇し，データの交換を行なう DTN のような環境は想定できない．

本研究では，こうした従来の課題を解決すべく，P2P ネットワークにおいて，アプリケーションや組織毎に専用の P2P ネットワークがあるかのようなふるまいを実現する **仮想化オーバレイネットワーク機構**を提案する．

†1 大阪大学/Osaka University
†2 京都産業大学/Kyoto Sangyo University
†3 奈良工業高等専門学校/Nara National College of Technology
†4 情報通信研究機構/National Institute of Information and Communications Technology
†5 日本電信電話株式会社 未来ねっと研究所/NTT Network Innovation Laboratories, NTT Corporation
†6 日本電信電話株式会社 サービスインテグレーション基盤研究所/NTT Service Integration Laboratories, NTT Corporation

Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

2. VON: 仮想化オーバレイネットワーク

2.1 想定環境

まず，本稿で扱う仮想オーバレイネットワーク (Virtual Overlay Network; 以下，VON) を規定する．VON は，グループ毎に仮想的に存在する P2P ネットワークであり，グループのメンバ向けに専用の P2P ネットワークがあるかのようなふるまいを実現する．

1 つの VON には複数のノード (PC, デバイス, 端末等) が属し，共通の VON に属するノードへのメッセージの直接送信 (ユニキャスト) や同報送信 (マルチキャスト) を行なう．それぞれの VON は，独立した P2P ネットワークを構成するオーバレイネットワークであり，VON 毎に個別のルーティングプロトコルでメッセージを転送する．一つのノードが複数の VON に属することもあり，その場合，メッセージを作成して発信する発信元のノードにおいて，どの VON 宛にメッセージを送信するかを選択する．VON に属するノード集合は，全ノードの部分集合であり，多段の階層構造をとることもあり得る．その場合，ある VON に属することは，自動的に当該 VON を含む下位の VON にも属さなければならないことを意味する．例えば，会員制サービス A 上の情報配信サービス B を考えたとき，ノードが B に属するには A にも属している必要がある．また，ここでは，上位階層にある VON に属するノード集合は，必ず下位の VON に属するノード集合の部分集合になるものとする．

メッセージには，宛先となる VON やノードの情報が指定される．メッセージを受信できるのは，宛先となる VON に参加し，かつ，メッセージの宛先に指定されたノードのみである．ここでは，メッセージの宛先は，VON に属する一つのノード ID(ユニキャスト) か，VON に属するすべてのノード (マルチキャスト) のいずれかとする．メッセージを発信した発信元のノードを発信ノード，メッセージを中継するノードを中継ノード，メッセージに指定される VON を宛先 VON，ユニキャストメッセージの宛先を宛先ノードと呼ぶ．本研究では，与信・課金等を行なえるよう，VON の利用者や，利用者が所有するノードを承認する承認機関が存在するものとする．以下では，承認機関に承認された利用者が所有するノードを正規ノード，VON への所属が承認された正規ノードを正規メンバノードと呼ぶ．

ここでは，物理媒体をとくに規定せず，有線や無線が混在し，インターネット等の公衆網を経由することも考慮する．したがって，ノード間の通信において，メッセージの傍受や改ざんに対する対処が必要である．

各 VON は，中継ノードの自律的なメッセージ交換によりその構造が維持される．VON

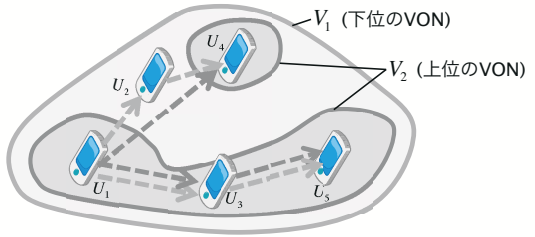


図 1 階層構造を持つ VON の例

が正しく動作するためには，VON に属するノードが中継ノードとしてメッセージ転送処理等を正しく行なう必要がある．階層構造を持つ VON では，全ての階層の VON において，中継ノードとして正しい動作をしなければならない．ここでは，正規メンバノードは，VON の中継ノードとしての動作を規定通り行なう前提とする．

また，階層構造を持つ VON では，同一の VON に属さないノードを介するメッセージ転送も想定する．図 1 は，階層構造を持つ VON におけるマルチキャストメッセージの転送処理の例である．図において，V_2 は，V_1 を下位とする ($V_2 \subset V_1$) 階層構造を持つ VON である．この例では，ノード U_1〜U_5 は，VON V_1 に属しており，ノード U_2 以外は VON V_2 に属している．図において，$U_1 \rightarrow U_3 \rightarrow U_5$ の経路は，V_1，V_2 ともに属しているノード間のやりとりとなるため同じとなる．一方，$U_1 \rightarrow U_2 \rightarrow U_4$ の経路では，V_2 のメンバではない U_2 を経由しており，V_1 と V_2 でそれぞれ経路が異なる．すなわち，U_2 は，自ノードが属していない上位の VON である V_2 が宛先に設定されたメッセージを V_1 によって転送している．このように，下位の VON に属するノード群の中継ノードとしての動作を許容すれば，同一グループに属するノード群のみではネットワーク的に分断されてしまうノードであってもメッセージを配布できる．

また，VON は DTN 環境でも動作する前提とする．DTN 環境では，end-to-end のメッセージ送受信において，複数のノード間で通信が分断されながらもメッセージが転送されるため，各ノードと承認機関の間，および，end-to-end のノード間での常時接続は存在しない．したがって，任意のノード間，および，承認機関と任意のノード間で，任意のタイミングで暗号化や署名に必要な鍵情報等の交換を行なうことはできない．

VON の正規メンバノードの管理は，承認機関で一元的に行なうことを基本とするが，既に正規メンバノードとなっているノードに申請し，承認を得る紹介制の形態をとる VON の

Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

運用も可能とする．この場合，承認機関との間の接続がオフライン状態となっているときに新規のメンバが増える可能性がある．すなわち，VON に属する正規メンバノードの集合は，メッセージ発信時点で確定しない．

一方，各ノードは初期状態，および，定期的または不定期に，利用者のアカウントによる認証のもと承認機関から直接承認を受けることが可能であるものとする．また，各ノードは NTP 等で内部時計をあわせる動作をする想定とし，ある程度時刻が同期している前提とする．また，ノードとして，動作の違反が観測された場合には，次回以降，承認機関が承認を拒否することで排除される運用が行なわれるものとする．

上記前提のもと，VON が正しく動作するには，以下の要件を満たす必要がある．

要件 1) メッセージを送信する発信ノードは，正規ノードでなければならない．また，宛先 VON を持つメッセージの発信ノードは，VON の正規メンバノードでなければならない．

要件 2) 宛先 VON の正規メンバノード以外はメッセージを中継してはならない．ただし，自ノードが属する VON の上位の VON を宛先 VON とするメッセージの中継を許容する選択を可能とする．

要件 3) メッセージの宛先である場合以外はメッセージを読み出せない，秘匿通信の選択を可能とする．すなわち，以下を実現できる必要がある．

要件 3-1) マルチキャストメッセージの場合，正規メンバノードのみが内容を読み出せる．

要件 3-2) ユニキャストメッセージの場合，宛先ノードのみが内容を読み出せる．

2.2 関 連 研 究

これまでの P2P ネットワークや DTN におけるセキュリティ実現の取り組みは，主に改ざんやなりすましを防止するための電子署名の構成方法や ID ベース暗号に基づく効率化手法[1)]，匿名性を実現するための方法[2)] 等に注力されてきた．

文献 3) 等では，DTN において，利用者認証を行った後に，承認機関から各ノードに対して公開鍵証明書を発行し，中継ノード毎にメッセージへの署名付与と検証を行なう方法が示されている．しかし，この方法は，メッセージが経路したノードが正規ノードであることを確認できるのみであり，複数のグループが混在する状況，複数の包含関係のあるグループが存在する状況を想定していない．また，この方法は事前に転送先のノードへ公開鍵証明書を送付し，メッセージ受信時に署名を検証できる状態とする．本研究では，隣接ノードは同一グループに属しているとは限らない想定であり，この方法では，自ノードが属する VON 以外が宛先 VON に設定されたメッセージを転送する挙動に対応できない．

文献 5) では，DTN において送信先ノードがマルチキャストのメンバかどうかを判定し，メンバ以外へ送信しない方法が提案されている．この方法も階層構造を持つグループは考慮しておらず，自ノードが属する VON 以外が宛先 VON に設定されたメッセージを転送する挙動に対応できない．

一方，グループに対する秘匿通信を行なう方式として，放送型暗号[4)] がある．この方法は，送信者があらかじめグループに属しているメンバを全て把握している必要がある．したがって，オフライン状態でのメンバの増減を想定する VON には適用できない．また，前節で示した要件 3 では暗号化をしない選択も可能であり，暗号化せずとも，承認されたグループのメンバからのメッセージのみをグループ内に流通させる機能が必要である．

3. VON の実現

3.1 実 現 方 針

VON 実現の基本方針として，メッセージに始点ノード，中継ノードで，メッセージ送信の正当性を示す証明書を付与し，各中継ノードで証明書を検証することで，不正ノードを介在したメッセージを排除する．また，マルチキャストでは有効期限つきの共通鍵による暗号化を，ユニキャストでは有効期限つきの公開鍵による暗号化を用いて秘匿通信を実現する．

以下，2.1 節の要件に対応した VON の実現方針を示す．

方針 1) 正規ノードであることを証明する**ノード証明書**，正規メンバノードであることを証明する **VON 証明書**を，承認機関が生成する．これらの証明書には，ノードの公開鍵に対する承認機関の署名を含み，公開鍵証明書としての役割も持たせる．正規メンバノードが別のノードをメンバノードとして承認できる VON では，正規メンバノードが，VON 証明書を中間証明書相当として新たな VON 証明書を生成することを許容する．

方針 2) 各ノードは，送信するメッセージ毎に，正規ノード，および，VON の正規メンバノードとしてメッセージを送信したことを示す**送信証明書**を生成し，メッセージに付与する．送信証明書は，ノード証明書，または，VON 証明書を含み，正規ノードとして承認された，または，VON の正規メンバノードとして承認されたノードが送信したメッセージであることを示す．メッセージに付与された送信証明書を検証し，検証に成功した場合に VON の中継処理を行なう．また，メッセージの VON 送信証明書を中継ノードが生成したものに置換する．階層構造を持つ VON では，依存する VON 全てについて，送信証明書の検証と置換を行なう．

方針 3) 秘匿通信のために，共通鍵，公開鍵による暗号化を行なう．

方針 3-1) 正規メンバノードには VON 毎に決まる共通鍵を配布し，マルチキャストメッ

Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

セージを秘匿通信により送信する場合，共通鍵でメッセージを暗号化する．階層構造を持つ VON では階層毎に入れ子構造の暗号化を施す．

方針 3-2) ユニキャストメッセージを秘匿通信により送信する場合，宛先ノードの公開鍵でメッセージに暗号化を施す．

方針 1) のノード証明書，VON 証明書は，方針 2) の送信証明書に含まれ，メッセージに付与されるため，メッセージの送信元のノードが正規ノード，正規メンバノードであるかどうかが検証可能となる．

メッセージの中継ノードが全て正規メンバノードであることを示すには，全ての中継ノードが送信証明書をメッセージに付与することが考えられるが，経路が長い場合にメッセージのサイズが増大してしまう．ここでは，正規メンバノードが不正な動作をしない想定であるため，方針 2) で示した中継ノードで証明書を置換する挙動により，正規メンバノードのみを流通してきたメッセージであることを保証する．正規メンバノードではない中継ノードを経由したメッセージは中継しないようにすることで，DoS 攻撃や不正な動作をする不正なノードの介在を防ぐ．各証明書には有効期限を設け，オフライン状態が有効期限を過ぎるまで継続した場合に，メッセージの発信や中継はできなくする．

また，階層構造を持つ宛先 VON では，始点ノードや中継ノードは，全ての下位階層の VON でも正規メンバノードであることを示す必要がある．上位階層の VON の正規メンバノードであっても，下位階層の VON の正規メンバノードではない場合があるため，宛先 VON が依存するすべての下位の VON 送信証明書を付与する．自ノードが属する VON を下位に持つ宛先 VON が設定されたメッセージを受信した中継ノードは，自ノードより上位の VON 送信証明書はそのままとし，自ノードが属する VON 以下の階層の VON 送信証明書を置き換える．これにより各階層が正規メンバノードのみで中継された状態が保たれていることを保証する．

方針 3) の暗号化を行なうことで，VON の正規メンバノード以外はメッセージを読み取れなくする．VON の共通鍵は VON 証明書同様に一定期間毎に承認機関を介して更新する想定とし，VON を脱退したノードが，一定期間を越えて VON のメッセージを読めないようにする．また，暗号化を宛先 VON の階層毎に行なうことにより，宛先 VON が依存する全ての下位 VON の正規メンバノードではないノードが，メッセージの内容を読み出すことを防ぐ．ユニキャストメッセージでは，発信ノードが，何らかの手段で宛先ノードの公開鍵を取得する必要がある．受信メッセージに対する返信をユニキャストで行なう場合は，メッセージに付与された発信ノードのノード証明書に含まれる公開鍵を用いれば良い．

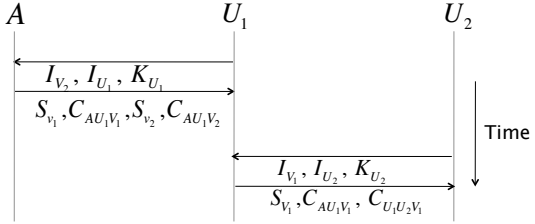


図 2 VON 証明書取得シーケンスの例

3.2 ノードと VON の承認

主体 X の ID を I_X, 公開鍵暗号における公開鍵を K_X, 秘密鍵を k_X, 共通鍵暗号における共通鍵を S_X と表記する．また，鍵 k による m に対する署名を $< m >_k$，暗号化されたメッセージ m を $\{m\}_k$ と表記する．A は承認機関，$U_i(i = 1, 2..)$ は，利用者のノードを表わす．

A が U を承認したことは，ノード証明書 C_{AU}，A が U に対して VON V への参加を承認したことは，VON 証明書 C_{AUV} の検証により確認できるようにする．

ノード証明書 C_{AU}，および，VON 証明書 C_{AUV} を，以下の通り定義する．

$$C_{AU} = I_A, I_U, K_U, t, < I_A, I_U, K_U, t >_{k_A}$$
$$C_{AUV} = I_A, I_U, I_V, K_U, t, < I_A, I_U, I_V, S_V, K_U, t >_{k_A}$$

t は証明書の有効期限を表す．C_{AU} は,「A, U の各 ID」,「U の公開鍵」,「有効期限」と，それらを秘密鍵 k_A により署名したデータである．C_{AUV} は,「A, V, U の各 ID」,「U の公開鍵」,「有効期限」，および，それらと「V の 共通鍵 S_V 」を秘密鍵 k_A により署名したデータである．各証明書は安全ではない通信路上で，メッセージに付与されてやりとりされるため，共通鍵 S_V そのものは，VON 証明書には含まない．

各証明書は，A を認証局とする公開鍵証明書としての役割も担っている．ノードが不正な振舞いをしない前提であるとき，承認機関の秘密の共通鍵を安全に配布できれば，k_A の替わりに秘密の共通鍵を用いる実装もあり得る．

図 2 は，VON 証明書取得シーケンスの例を示している．V_2 は，V_1 を下位に持つ VON である．ノード U_1 が，V_2 へ参加する際は，A へ安全な経路で接続し，自身の ID, 公開鍵とともに参加したい VON の ID を送信する．A は，必要に応じて利用者の認証を行ない，承認する場合に，要求された VON が依存するすべての VON の共通鍵と，VON 証明書を

Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

配布する．この例の場合，S_{V_1}, S_{V_2} および，VON 証明書 $C_{AU_1V_1}$，$C_{AU_1V_2}$ を送信する．VON 証明書に付与された署名を K_A により検証することで，証明書に記載された I_V を ID として持つ VON の正規メンバノードとして承認されたことを確認できる．

また，図 2 は，メンバを紹介制で追加する VON の運用がなされる例となっており，U_2 が，V_1 への参加を U_1 に要求している．U_1 は，入手した V_1 の VON 証明書に加えて，$C_{U_1U_2V_1}$ を生成し，S_{V_1} とともに送信している．VON 証明書の検証の際，$C_{AU_1V_1}$，$C_{U1U_2V_1}$ によって，V_1 の承認機関である A まで承認者を遡ることができるため，これらを $C_{AU_2V_1}$ とみなせる．よって，この例では，次節で示すメッセージ送受信の際，$C_{AU_2V_1}$ 相当として $C_{AU_1V_1}$ と $C_{U1U_2V_1}$ を用いる．

3.3 メッセージの送受信

宛先 VON V_n の m を V_i 向けに暗号化したデータ $E_{mV_nV_i}$ を，次の通り定義する．

$$E_{mV_nV_i} = \{\{\{m\}_{S_{V_n}}\}_{S_{V_{n-1}}}...\}_{S_{V_i}}$$

$E_{mV_nV_1}$ は，$V_{n-1}, V_{n-2}, ..., V_1$ を下位 VON を持つ V_n が読み出せるよう，m を階層的に暗号化したデータに相当する．暗号が不要な VON では，暗号化せず元のデータを用いる．

$C^m_{AU}, C^m_{AUV_nV_i}$ を，次の通り定義する．

$$C^m_{AU} = C_{AU}, < m >_{k_U}$$

$$C^m_{AUV_nV_i} = C_{AUV_i}, < E_{mV_nV_i}, I_{V_i} >_{k_U}$$

C^m_{AU} は，「U のノード証明書」，および，「m をノードの秘密鍵 k_U で署名したデータ」に相当する．C^m_{AU} の署名データを，C_{AU} が含む K_U により検証することで，U が，m の始点ノードであること，また，C_{AU} を検証することで，U が正規ノードであることが確認できる．

$C^m_{AUV_nV_i}$ は，「V_i の VON 証明書」，および，「『送信先 VON V_n の m を V_i 向けに暗号化したデータ』，『V_i の ID I_{V_i}』を，ノードの秘密鍵 k_U で署名したデータ」に相当する．$C^m_{AUV_nV_i}$ の署名データを C_{AUV_i} が含む K_U により検証することで，U が，V_i の VON 証明書を保持する正規メンバノードであり，V_i 向けに暗号化された m を送信したことを示せる．

これらが方針 2) に従った送信証明書に相当する．以下では，C^m_{AU} をノード U による m の**ノード送信証明書**，$C^m_{AUV_nV_i}$ をノード U による V_n を宛先に持つ m の V_i に対応する **VON 送信証明書**と呼ぶ．このとき，本文 m を持ち，A より V_n への参加を承認された U から送信される V_n を宛先 VON とするメッセージ M_{mAUV_n} は次の定義に従うものとする．

$$M_{mAUV_n} = E_{mV_n}, C^m_{AU}, C^m_{AUV_nV_n}, C^m_{AUV_nV_{n-1}}, ..., C^m_{AUV_nV_1}$$

M_{mAUV_n} は，V_n 向けに階層的に暗号化されたデータ，ノード送信証明書，および，V_n 以下の各階層の VON 送信証明書から構成されるデータである．

メッセージを受信したノードは，ノード送信証明書，および，VON 送信証明書を検証する．V_n まで VON 送信証明書を検証でき，復号できた場合，U はメッセージ m が V_n を正しく宛先 VON とするメッセージであることを確認できる．マルチキャストメッセージの場合はこの時点で受信する．また，VON で決められた挙動にしたがってメッセージの中継を行なう．

U が正規メンバノードではない VON が含まれていた場合，検証できた VON 送信者証明書の最上位の VON において転送を行なう．すなわち，U は，V_n が宛先 VON のメッセージに対し，所属する最上位 VON が p $(p < n)$ であったとき，V_p より上位の VON 送信証明書および暗号化データはそのままに，$V_p, V_{p-1}, ..., V_1$ の順で各 VON 向けの暗号化を行なった上で VON 送信証明書を付与し，V_p の動作に従いメッセージを転送する．上記により，発信ノードが VON の正規メンバノードであり，中継ノードが，下位で用いる VON を含め，宛先 VON の正規メンバノードである状態が保たれる．

ユニキャストの場合は，宛先ノードの公開鍵で暗号化を施したメッセージを用いる．例えば U_r が宛先ノードのメッセージでは，$\{m\}_{K_{U_r}}$ を m として指定する．

図 3 a) は，VON によるメッセージ送受信の例である．例では，$V_3 \subset V_2 \subset V_1$ であり，U_1 と U_3 が V_3 の正規メンバノード，U_2 は V_2, の正規メンバノードである．図では，V_3 を宛先 VON とする 'message' を U_1 が送信している．最初に，ノード送信証明書が付与されたのち，V_3, V_2, V_1 の順に暗号化と VON 送信証明書の付与がなされている．U_2 は，V_3 に所属していないため，V_2 まで復号化と証明書の検証をしたあと，V_2 以下で U_2 により VON 送信証明書が再度付与されている．中継の際，受信した各階層の暗号化データは再利用できる．

3.4 VON セッション

前節で示した VON の実現方法は，隣接ノードが同一の VON に属していない場合に対応できるよう，毎メッセージに VON 送信証明書を付与している．この方法は，ノードの VON への所属を厳密に検証できるが，階層構造を持つ VON では，全ての階層について VON 送信証明書を付与する必要があり，階層構造が深い場合にトラヒックが大きくなってしまう．

そこで，あらかじめ隣接ノードが同一 VON に所属していることが確認できた場合に，隣

Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

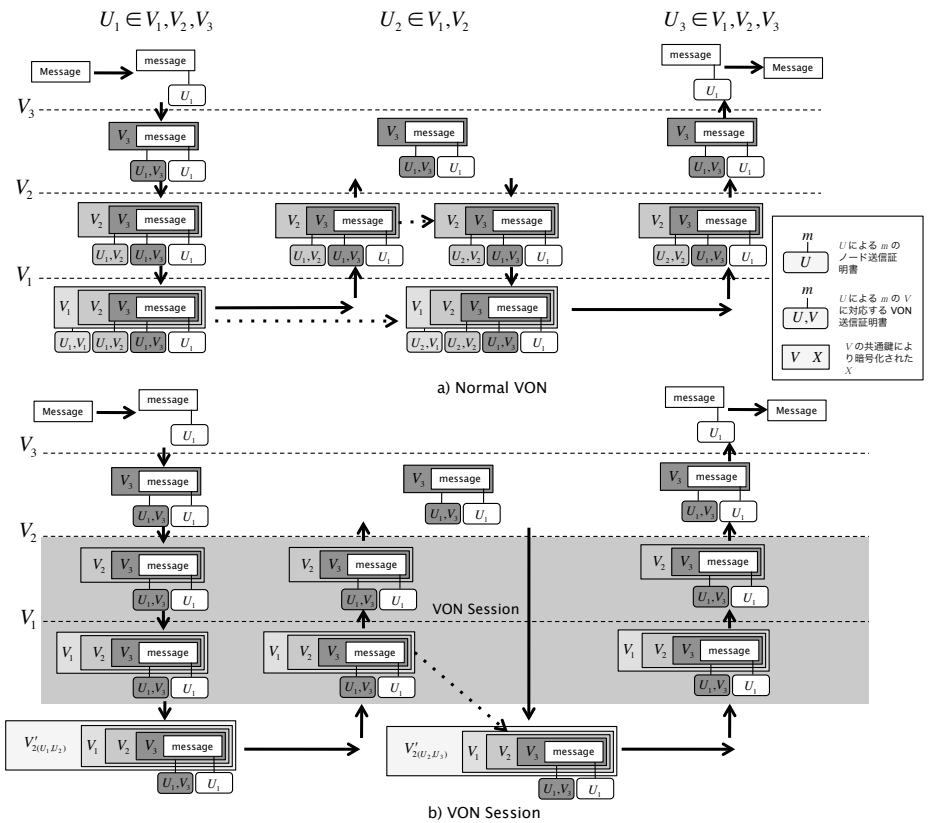


図 3 メッセージの中継処理

接ノードとの間で，当該 VON について認証済みのセッションを生成する方法を提案する．これにより，メッセージ毎に VON 送信証明書の付与と検証をせずとも，互いに正規メンバノードであることを確認可能とする．ここでは，隣接ノード間で共通の VON について構成する認証済みのセッションを **VON セッション**と呼ぶ．

以下では，隣接ノード間で VON セッションを構成する手順を示す．まず，各ノードは隣接ノードから送信されるメッセージの宛先 VON を記録しておく．送信先 VON，または，その下位階層の VON が，ノードが所属している VON であり，かつ，一定数以上のメッセージを送受信できる状態が続く場合に VON セッション構成要求を当該ノードへ送信する．一定数以上のメッセージを送受信できる状態が続くかどうかの判定は，ノードのモビリティや，VON のプロトコル，物理ネットワークの状態等に依存して判定することになると考えられ，その判定方法は本稿の範疇外とする．

VON セッション構成要求は，要求先ノードを宛先ノードとするユニキャストメッセージとする．また，このメッセージの宛先 VON をセッションを要求する VON とする．VON セッション構成要求を受けたノードは，VON 送信証明書を検証して隣接ノードが共通の VON の正規メンバノードであることを確認した上で，VON セッション用の秘密の共通鍵を生成し，要求元ノードに VON 指定のユニキャストメッセージで返信する．この VON セッション用の秘密の共通鍵を有していることが，当該 VON に両ノードが属していることを示す．共通鍵には有効期限を設け，有効期限が切れた時点で VON セッションを終了させる．

ノード U_s と U_r の間で，V_p 向けに構成される VON セッションを $V'_{p(U_s,U_r)}$ と表記する．

ノード U_s は，U_r との間で VON セッションが存在する VON については，$E_{mV_pV_1}$ を共通鍵 $S_{V'_{p(U_s,U_r)}}$ で暗号化した $\{E_{mV_pV_1}\}_{S_{V'_{p(U_s,U_r)}}}$ を送信し，VON セッションに属している場合のみ復号できるようにするとともに，VON セッションが存在する VON 以下は VON 送信証明書の付与を省略する．

すなわち，本文 m を持ち，A より V_n への参加を承認された U から送信される V_n を宛先 VON とするメッセージを，$V_p(p \leq n)$ の VON セッションが存在する U_s，U_r 間で送信する場合の M'_{mAUV_n} は，

$$M'_{mAUV_n} = \{E_{mV_pV_1}\}_{S_{V'_{p(U_s,U_r)}}}, C^m_{AU}, C^m_{R_UAUV_nV_n}, C^m_{AUV_nV_{n-1}}, ..., C^m_{AUV_nV_p}$$

となる．

図 3 b) は，VON セッションによるメッセージ送受信の例である．各ノードが所属する VON は 図 3 a) と同様である．図では，$V'_{2(U1,U2)}$ および，$V'_{2(U2,U3)}$ が構成されているため，U_1 から U_2 を経由して U_3 に至る経路で V_1, V_2 の VON 送信証明書の付与と検証が省略されている．U_2 では，VON V_2 までメッセージを復号化したのち，U_3 へ転送している．このとき，受信したメッセージをセッション共通鍵 $S_{V'_{2(U_1,U_2)}}$ で復号したデータを，$S_{V'_{2(U_2,U_3)}}$ で暗号化して U_3 へ転送すればよく，証明書を検証する処理はせずに済む．

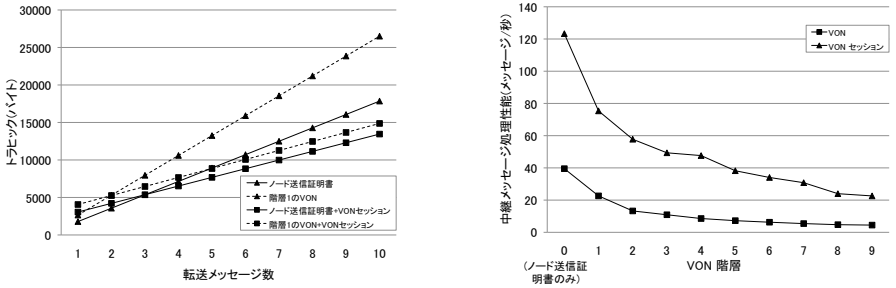
Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

4. 携帯端末向けプロトタイプの試作

本稿で示した VON 機能を，DTN によりフラッディングを行なう Android OS 向けモジュール上に試作し，フィージビリティ検証を行なった．試作にあたっては，オーバレイネットワークのミドルウェアである PIAX [*1] の DTN モジュールを拡張した．現状の実装では，公開鍵暗号は 1024 ビット RSA，署名アルゴリズムに RSA SHA1，共通鍵による暗号アルゴリズムには，AES256 を用いた．また，ノード証明書，VON 証明書では，承認機関の共通鍵暗号によるメッセージ認証アルゴリズム HMAC SHA1 を用いている．また，メッセージ交換でのデータ表現形式としては，Web 等で広く用いられるようになっている JSON を用いた．JSON は，そのままではバイナリデータを扱えないため，署名データ，暗号化されたデータは BASE64 によりエンコードされた文字列として表現している．

図 4(a) は，通常の VON および VON セッションにおけるトラヒックを示している．横軸は，ノード間で交換されるメッセージ数，縦軸は，ネットワークに流れるバイト数である．各メッセージは，512 バイトであるが，ノード送信証明書が付与されたメッセージは，署名等のデータを含めると 1,784 バイトとなっている．図では，VON の指定がなく，ノード送信証明書のみの場合と 1 階層の VON が指定された場合を示している．VON セッションのデータは，VON セッションを初期化するための VON セッション構成要求とその返答のトラヒックを含んでいる．本実装では，階層なしの VON では，4 メッセージ以上，1 階層の VON では，3 メッセージ以上のメッセージを隣接ノードに送信する場合に，VON セッションを構成する方がトラヒックを抑えられている．

図 4(b) は，1GHz ARM Cortex A8 の CPU と，512MB の RAM を具備し，Android 2.3 が稼働する携帯端末上で，512 バイトの本文を持つメッセージの中継を行なう際の処理性能 (1 秒あたりのメッセージ転送処理数) を示している．処理時間として受信から転送開始までの時間を計測しており，ネットワークでの送信時間は含んでいない．処理性能は 100 回の試行の平均処理時間を基に算出している．横軸は VON の階層の深さを示しており，0 は階層なし，ノード送信証明書のみの場合である．通常の VON では，階層なし場合，40 メッセージ/秒，1 階層の VON では，23 メッセージ/秒，VON セッションを構成した場合，階層なしならば，123 メッセージ/秒，1 階層の VON では，75 メッセージ/秒の中継性能となっている．例えば，300kbps 程度の実効通信速度が得られる無線ネットワークでは，1 階層のサイズのメッセージの転送を行なうとき，全通信帯域を使用できたとしても 20 メッセージ/秒程度が上限となるため，中継処理よりもネットワークの性能がボトルネックとなる．



(a) メッセージ数に対するトラヒック　　(b) VON 階層毎のメッセージ転送性能

図 4 試作プロトタイプにおける性能

図 5 は，上記環境で，1 階層の VON でメッセージを転送処理したときの処理時間の内訳を示している (横軸はミリ秒)．通常の VON においては，RSA SHA1 による署名処理が多くの処理時間を占めている (約 40 %) が，VON セッションでは，AES 暗号化処理が加わるものの署名処理は不要となるため，全体の処理時間は大幅に削減されている．また，通常の VON および VON セッションを用いた場合いずれも JSON 文字列の生成と解析に多くの処理時間を要しており，それぞれ，49%, 68% を占めている．とくにメモリ確保処理が多発する JSON 文字列の生成に時間を要している．

5. 考　　察

本稿で述べた方法では，不正ノードが盗聴等で不正に入手したメッセージのコピーを大量に再送信する DoS 攻撃の懸念がある．DoS 攻撃の方法として，コピーを大量に同じ相手に再送信する攻撃と，無差別な大量の相手にコピーを再送信する攻撃が考えられる．前者への対処として，C^m_{AU} や $C^m_{AUV_nV_i}$ における署名対象に，ノードが一意に発生する乱数データを含めることとし，受信ノード上で，同じ乱数を含むメッセージを出すノードからの転送を一定時間拒否する等が考えられる．後者への対処としては，ルーティングプロトコル

[*1] http://www.piax.org/

Vol.2011-DPS-146 No.28
Vol.2011-CSEC-52 No.28
2011/3/11

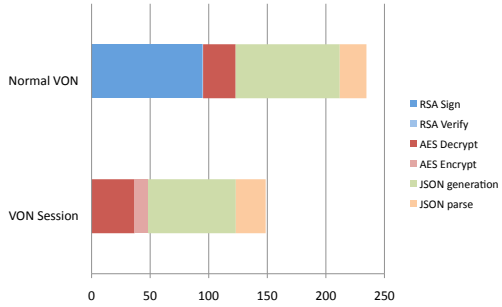


図 5 メッセージ処理時間の内訳

上，送信され得ないメッセージを受信したノードを拒否する等の対策が考えられる．DTN の Epidemic Routing[6] 等では，こうした流通済みのメッセージは拡散しないようにする機構を持っている．

また，本文中で述べた方法は，公開鍵暗号の秘密鍵，および，VON の共通鍵は，安全に保存される前提である．とくに，スマートフォンや PC 上の実装では，クラックされたアプリケーション等により，メモリの内容を不正に読み取られる危険性は考慮する必要がある．耐タンパ性のあるチップ上で鍵保存と暗号処理を行なう等，実装上行なえる対策は取る必要がある．さらに，本方法は，正規メンバノードが全て規定通りの動作をする仮定のもとでのみ有効となる方法であり，正規メンバノードが一つでも不正な挙動を示すと成立しない．とくに暗号を解いた後に別の経路で流通させるといった不正には対処できず，別の対策が必要である．

また，先に述べた通り，各ノードはある程度同期した内部時計を持っている前提となっている．時刻が進んだノードがあるときは，有効期限が切れたと誤認識し，意図する利用者に転送されない問題が生じる．この場合であっても，VON が持つルーティングプロトコルに経路の冗長性があれば，時刻が正確なノードによる経路でメッセージを宛先まで転送できる可能性はある．一方，時刻が遅れたノードがあるときは，証明書の有効期限を過ぎてもメッセージを中継してしまう可能性がある．このとき，暗号化のための共通鍵更新がなされていれば，復号は不可能であり，新たに発信されたメッセージは意図せぬノードへ配信されない．

試作したプロトタイプでは，インターネットでの互換性や，対応モジュール実装の容易性の観点で，通信形式として JSON 形式を用いた．本稿の検証は，特に最適化を行なっておらず，最も単純なデータ転送手順の実装に基づくものであり，JSON 以外のバイナリ送受信に適した形式を用いる，冗長に送信されるデータを圧縮する等の工夫により，大幅にデータ量の削減や性能の向上ができる可能性はある．

6. おわりに

P2P ネットワーク上に，仮想化されたオーバレイネットワークを構成するための機構の設計とプロトタイプ実装によるフィージビリティ検証を行なった．

プロトタイプ実装により実用上問題ない動作が可能であることは確認できたが，現状では，先に述べた通り，データ授受に冗長な点がある等の課題もある．今後は，IMS のような外部の認証と連携したサービス構成等の実際の運用への適用や，安全性・メッセージ送信の確実性を保ちつつメッセージ量を削減する方法等について，さらに検討を進めたい．

謝辞 本処理系の開発，及び検証は，日本電信電話株式会社 NTT サービスインテグレーション基盤研究所と国立情報学研究所の提供する研究設備，回線を利用した共同研究の一環として実施している．ここに記して謝意を示す．

参 考 文 献

1) Asokan, N., Kostianinen, K., Ginzboorg, P., Ott, J., and Luo, C.: Towards Securing Disruption-Tolerant Networking, *Technical Report*, NRC-TR-2007-007, Nokia Research Center (2007).
2) Kate, A., Zaverucha, G., and Hengartner, U.: Anonymity and Security in Delay Tolerant Networks, *Proceedings of the 3rd International Conference on Security and Privacy in Communication Networks (SecureComm 2007)*, pp.504–513 (2007).
3) Fall, K.: A Delay-tolerant Network Architecture for Challenged Internets, *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM '03)*, pp.27–34 (2003).
4) Boneh, D., Gentry, C. and Waters, B.: Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, *Proceedings of Crypto '05*, Springer, pp. 258–275 (2005).
5) Srinivasan, K., Ramanathan, P.: Reliable Multicasting in Disruption Tolerant Networks, *Proceedings of IEEE Global Telecommunications Conference, 2010 (GLOBECOM 2010)*, pp.1–5 (2010).
6) Vahdat, A., Becker, D.: Epidemic Routing for Partially-Connected Ad Hoc Networks, *Duke Tech Report CS-2000-06* (2000).