マルチメディア通信と分散処理 42 － 8
（１９８９．５．１９）

大規模広域分散環境 WIDE の構築

村井 純 東京大学
加藤 朗 東京工業大学
佐藤智満 慶應義塾大学
楠本博之 電総研
山口英 大阪大学

広域に展開する大規模分散環境 WIDE(Widely Integrated Distributed Environment) の構築を開始した。実際の構築は、実験基盤となる WIDE インターネットの構築とそれを利用した各種技術の実験開発から成り立っている。ここでは、WIDE の概要とその実験基盤の構築について報告し、そこで現在実験されている通信技術、経路制御、資源名前管理、セキュリティの各技術とその問題点について議論する。

Large-scale Wide-area Distributed Environment -WIDE-

Jun Murai
University of Tokyo
Akira Kato
Tokyo Institute of Technology
Tomomitsu Sato
Keio University
Hiroyuki Kusumoto
Electrotechnical Laboratory
Suguru Yamaguchi
Osaka University

WIDE(Widely Integrated Distributed Environment) is a research project to construct a wide-area and large-scale distributed environment on Japanese research environment. This paper introduces overview of the project and discusses about the researches going on in the project, such as, communication technology, routing functions, resource management, security handling which all are essential subjects to develop such an environment.

1 はじめに

情報科学・情報工学の発達と通信技術の進歩により、分散された計算機資源を有効に利用できる分散型の計算機環境を前提とした計算機システムの研究が急務になっている。

計算機環境を構成する要素はパーソナルコンピュータからスーパーコンピュータに至る多種の計算機システムとなり、そのオペレーティングシステムも多様である。また、ローカルエリアネットワークのような近距離の分散資源を接続するための技術のみならず、遠隔地に分散する計算機資源を有機的に接続し、広域の分散環境を構成するための通信技術も比較的自由に利用できるようになってきた。これらのあたらしい背景においては、従来個別に研究されてきたオペレーティングシステム、通信技術、コンピュータネットワーク、コンピュータアプリケーションに関するそれぞれの研究成果をふまえ、国際的な範囲を含む大規模広域分散環境の構築に関する技術の確立が必要である。

WIDE(Widely Integrated Distributed Environment) [1]の目的は、局所的な分散環境とそれらの接続という階層的な構造に基づいた大規模な分散環境を構築するための技術を実証的に確立することにある。そのために、実際に運営されている複数のローカルエリアネットワーク間を、分散環境を構築するために充分な速度の回線を用いて接続し、その上に実用に耐える大規模広域分散環境のプロトタイプを構築する。この環境の構築に際して、ネットワーク間パケットのための経路制御機能、ゲートウェイにおける制御機能、広域分散環境の管理機能と応用機能に関する研究と研究成果の実証を行う。

大規模広域分散環境の基礎となる研究課題には、コンピュータネットワーク、オペレーティングシステム、分散処理、耐故障システム技術などがある。特に、コンピュータネットワークに関しては、局所的分散処理を含むローカルエリアネットワークと、広域ネットワークに関する研究が行われ、実績がある。これからの計算機環境の代表的モデルとなる大規模広域分散環境の構築という視点は、これらの研究分野で本来追及されていた目標と異なるために、これらの成果の単純な組み合わせでは本研究の目的を達成することはできない。本研究の特色は、これらの分野の統合的な研究成果を目指し、通信技術、通信経路、計算機システム、社会科学的背景、オペレーティングシステムなどに関する異種性を前提とした統合的な環境を構築するための技術を確立する点にある。

広域的に分散されているローカルエリアネットワークや計算機システムを接続し、そこに共通の環境を構築する実験はJUNET [8] によって実現され、200 を越える組織を接続し、分散資源の名前管理、経路制御、通信技術、日本語に基づいた通信機能などに関する研究が行われ、それぞれの成果が実証されている [7]。分散環境の広域化に伴う信頼性への要求に関する研究は、セキュリティ機能の研究としての [1]、資源の名前管理に関しては [2] の成果があがっている。

2 大規模広域分散環境の構築

本研究の対象とする計算機環境の規模としての目標は大学・研究組織上での分散環境を想定しているので、その範囲としては世界全体を含むことになる。このような基盤を構築するための実験として当面の対象となるのはわが国の大学を中心とした計算機環境の統合的な確立に必要な技術の追求である。このような環境におけるネットワーク技術を実現するためには、画一的な技術を基盤にした単純なネットワーク構造を期待するのは不可能なばかりでなく、環境に応じた最適な技術の利用という視点では効率が悪い。柔軟な基礎技術への対応とそれに基づいた開放的なシステム構造を開発する必要がある。そのために、ここでは次のような項目に分類して研究活動を行なうことにした。

2.1 異種通信技術の利用

実際の大規模分散環境を構築するためには使用可能な下位の通信技術が具体的な一定のプロトコル構造によって利用された時の性質を実証的に把握しておくことが重要である。したがって、本研究の一つの焦点は、対象として想定している環境の中で利用され得る異種通信技術を最も効率的に利用するための技術の確立である。この異種性は、バンド幅、動的なスループットの変化、動的なラウンドトリップ時間の変化、コネクション確立に対するオーバヘッド、回線の課金システムなどに関する各特性として整理し、これらの積極的な制御機構の基盤を開発する。具体的には、公衆電話回線、アナログ専用回線、デジタル専用回線、公衆パケット交換網、プライベートパケット交換網、ISDN と、サテライト経由と海底ケーブル経由の国際回線をすべて同じ上位プロトコルで利用できる環境を実験基盤として開発する。

2.2 強じんなネットワーク構造

大規模で広域に渡る分散環境の基盤を考えると、中継ノードやそれらを接続する回線の障害などに起因するネットワークの分断問題に対する技術を確立する必要がある。この問題は経路制御手順を用いた冗長経路の利用として一般に解決されるが、**WIDE**ではこの問題を前項で得られる各種通信技術の特

[1]本研究は電気通信基金普及財団昭和63年度研究助成金並びに WIDE プロジェクト共同研究各社の助成と協力によって行なわれている。

性の評価を利用して、これに基づいたネットワーク構造の強じん化を行なっている。特に、回線交換式の課金システムに基づいた公衆回線やISDNの接続とパケット交換式の通信技術を用いた接続はネットワーク間接続のバックアップ回線として効果がある。これによって、速やかな障害の検出、その伝搬、効率的なバックアップ回線の利用、それに対応する経路制御、最終的なオペレータ介在の復帰、といった一連の体系を確立することができる。

2.3 ゲートウェイ機能

ネットワーク間接続の概念は [11] でその基盤が提案されたように、ネットワーク毎に異なる技術と運用方針をその境界であるゲートウェイノードで吸収する必要がある。大規模で複雑なネットワーク間接続を実現するためには現実的な規模を想定して、それに適応する新しい経路制御技術の開発しなければならない。WIDEでは、ある自治ネットワークにおける内部アドレスと外部アドレスへの対応付け、アドレスの書き換え、経路決定アルゴリズムなどに関する多様な実験を行なうことによってこの問題を実証的に追求する。また、WIDEの環境では中継ノードや回線の故障によるバックアップ回線の動的な利用や、その大規模性に起因して全体のネットワーク間接続のトポロジが動的に変化することになる。これに対応するゲートウェイ間プロトコルの開発も急務である。

また、サービスの型に依存した最も有効なデータリンクエンティティの選択もゲートウェイ機能として実現する。実際の自治ネットワークでは、外部に公開するアドレス、ゲートウェイの通過を可能にするアドレスの集合、データリンクのアクセス権などに関する独自のポリシーを行使する要求がある。このような要求もゲートウェイプロトコルをはじめとするゲートウェイ機能として実現する。

2.4 プロセス間通信インターフェース

WIDEの環境における共通の応用技術を開発する基盤として、共通のプロセス関通信インターフェースを提供する。ここでは、サービスのアクセス点とその名前表現、接続の性能状態に対する要求、データの表現形式、認証とセキュリティ機能の各技術に関する複数の副階層のプロセス間通信インターフェースとして実現している。

2.5 資源管理機能

WIDEの環境では共通のサービスを資源の実体として定義し、それに名前を付ける。各資源の名前は名前サーバの機能により階層的な構造を用いて表現できるので、現在使用されている名前管理機構 [5] との整合性が保たれている。資源のアクセス権はここで定義される所有権により実現される。

2.6 応用技術

WIDEの応用技術は上記の資源管理機構とプロセス間通信インターフェースを利用して作成される。現在は、既存のインターネットプロトコルの応用技術と、対話型の会議システムが試作されている。

2.7 ネットワーク管理運用技術

大規模なネットワークの運用には、ネットワーク管理や診断のプロトコルの開発やそれに基づいた管理運用技術を確立する必要がある。WIDEではセキュリティやアクセス権などのポリシー行使の制御、日常のネットワーク維持、故障時の対策などを技術的に体系付け、ガイドラインや応用技術として実現する。

3 WIDEインターネットの構築

本論文執筆現在のWIDEの実験は、東京大学、東京工業大学、慶應義塾大学、大阪大学、青山学院大学、電総研を相互に接続する表1に示した環境を用いて行なわれている。

回線は3.4KHzのアナログ専用回線、64Kbpsのデジタル専用回線、学術情報センターの提供するX.25プライベートパケット交換網、公衆電話回線、INSネット-64(ISDN)を使用している。

全体のプロトコルはインターネットプロトコル(TCP/IP体系)を用いている。これを基盤にプロトコルやデータ形式に関する実験を行なっている。OSIのプロトコル体系への移行や実験もこの基盤上で行なっている。図1にWIDE接続の現状を示す。

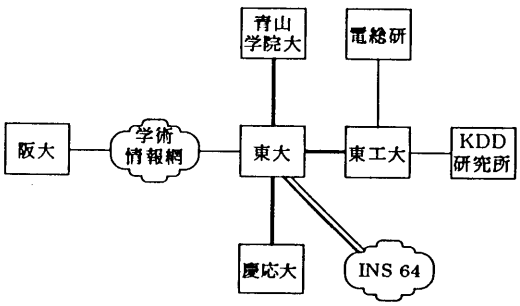

図 1: WIDE接続の現状

4 異種通信技術の利用

広域大規模分散環境にあたっての要求の一つとして、多様な異種通信技術をIP等の共通のプロトコル体系の中で柔軟に、かつ、効率的に利用するた

Table 1: WIDE の接続組織と方式

接続組織名	回線種別	バンド幅	Dial Up の有無
慶應義塾大学↔ 東京大学	デジタル専用回線	64K	有
東京大学 ↔ 東京工業大学	デジタル専用回線	64K	有
東京大学 ↔ 青山学院大学	デジタル専用回線	64K	有
東京大学 ↔ 大阪大学	学術情報網 (X.25)	9.6K	有
東京工業大学↔ KDD 研究所	3.4KHz 音声専用回線	9.6K	有
東京工業大学↔ 電総研	3.4KHz 音声専用回線	9.6K	有
東京大学 ↔NSFNET/CSNET	学術情報網 (X.25)	9.6K	有

この他に ISDN の設置を行なっている。

めの技術がある。このためには、単一的な専用回線やサブネットワークの利用に比べて、異種通信技術の並列利用には経済的にも、性能的にも有利である可能性がある。

特に、わが国には、DDX, Venus-P, INS ネット 64 といったパケット交換サービスの充実、学術情報センターの提供するプライベートパケット交換網といった背景環境がある。WIDE では、このような X.25 パケット交換網の効率的な利用を実験開発した [3]。また、INS ネット-64 の B チャネルや公衆電話回線を専用回線や X.25 パケット交換網と同じ上位プロトコルで利用するための技術も、経済・技術の両面から広域大規模分散環境の構築に重要な技術である。

従来の電話回線に高速モデムという組合せは、CSNET や JUNET で実験され、前者のものは PheneNet のユーザが anonymous FTP などのサービスを享受できるということで、実用されている。しかしながら、これは経路制御上の問題から逆向きの接続や複数のダイアルアップリンクを跨った通信などは現在は実用されていない。

このような回線交換型の通信技術を用いた場合、接続が断続的である。そのために、接続の確立と切断のタイミングのための技術を確立する必要が有る。経済的には、接続時間の合計が常時接続した場合に比較して一定以下の場合に同程度の専用回線サービスよりも有利となる。この割合が十分大きければ (例えば 90%以上)、故障率がやや高い通常のリンクとして取り使うこともできるが、この割合は一般には 30%程度と考えられるので別の取り扱いが必要になる。

このようなダイアルアップ回線で接続される 2 点の間での経路制御情報のとりあつかいには新しい技術を導入しなければならない。従来の経路制御・選択技術を用いると、接続が確立している場合には、両者ははそれぞれの経路情報を交換しそれぞれを広告し、接続が切断された状態の場合には切断された接続の反対側のネットワークを弱く (メトリックを極端に大きくして) 広告することで実現できる。また、通信が発生するサービスの種類に依存した経路制御が行なわれる機構を実現し、バッチ的な要求に有効な利用を行なうこともできる。

ダイアルアップリンクとして最近サービスが始まった ISDN(INS ネット 64) による接続は、パケット交換と同時に回線交換を扱うことができるので、これからのダイアルアップリンクを提供する上で期待されている。この場合、定常状態では ISDN の D チャネル によるパケット交換を使用しておき、ある特定のサイトあるいはドメインへのトラフィックが急増した場合、適当なところに B チャネル の 64kbps のリンクを利用し、動的に帯域を増加させることができる。これによって、経済的かつ必要な場合には十分な高速性が確保できるリンクを構築することができる。

5 強じんなネットワーク間接続

WIDE は広域分散環境を提供するネットワークであり、各組織を相互接続するゲートウェイには高い信頼性と稼働率が要求される。回線断、隣接ゲートウェイの故障といった障害時においても、各ゲートウェイが協調し正常な動作を維持できるようにするために、WIDE においては各ゲートウェイの「生き残り戦略」を定め障害に備える。

ゲートウェイの「生き残り戦略」とは、ネットワークの状態変化、例えば、ある接続の故障、ふくそうの発生、ゲートウェイ自身の故障などに対応して、ゲートウェイの機能をいかに維持していくかの戦略のことである。当然、経路制御の方針とアルゴリズムも状況によって変化する。

また、WIDE のゲートウェイは各ネットワークの所有者のポリシーに依存した技術が提供されているので以下に述べるような障害時の処理に関しても選択は可能である。

ゲートウェイが障害発生時に維持すべき機能として以下の項目があげられる。

- ネットワークの管理
  WIDE ゲートウェイにおける機能の対象の一つに通信の優先度がある。そこで、ネットワー

クの障害管理のためのトラフィックは優先的に扱う。このような情報の伝達が遅れたり、中断したりすると、それにより無駄なトラフィックの再送や障害時においては効率的でないルーティングを続ける可能性が生じてしまう。

- ネットワークの分断の回避
  複数のIP接続を持つゲートウェイの場合、経路制御を変更してネットワークが分断されないようにする。また通常のIP接続が障害によりすべて使用不可能になった場合には緊急用のダイアルアップ接続により接続の維持をはかる。

- 障害発生の報告
  障害が発生し始めたら管理者等へ自動的に連絡する。

これらの機能を維持するためにWIDEゲートウェイは以下の3段階の生き残り戦略をとる。WIDEインターネットには管理者の常駐するオペレーションセンタを設置する。最終的な障害の処理はここで行なう。

1. まずIPの接続を確保する。
   ふくそう、回線障害等で他のひとつのゲートウェイとの間の接続が利用不可能になった場合、代替経路があればそちらへトラフィックを経路制御し、IPでの接続が分断されないようにする。次に他のすべてのゲートウェイとの通常の接続が利用不可能になった場合には、ダイアルアップ接続(公衆電話回線、パケット交換、ISDN)により最適なゲートウェイへの接続を行ない、管理情報を優先的に通過させ、可能な限り通常のトラフィックも処理する。

2. IP以外の方法を試みる
   上記の試みも不可能な場合には、IPネットワークとしてとしてネットワークの残りの部分と分断された場合にゲートウェイ は、uucpを含んだのIP以外の手段(WIDE用緊急プロトコル)によりオペレーションセンタへ障害発生メッセージを送付する。また管理情報の交換もこの手段により行なう。

3. オペレーションセンタへのあらゆる種類の接続ができなくなったときには、その旨をそのゲートウェイのシステム管理者へ知らせる。また前2段階においても異常、障害発生をシステム管理者へ知らせることが必要であり、そのための手段として以下のような方法が考えられる。

   - ダイアルアップ による管理者へが登録している音声電話への呼出。またはポケットベルへの呼出。
   - 予め用意されたFAXの送出。
   - その他。

またWIDEでは、WIDEゲートウェイ に対するクラスを定義し認定する。この定義、認定にあたっては、障害時、緊急時のポリシー、バックアップネットワークの有無とその種類を考慮する。

以下にWIDEゲートウェイクラスを決定する要素をあげる。

- 複数の他のWIDEゲートウェイとのIP接続。
- ISDN等のダイアルアップによるオペレーションセンタのゲートウェイとの接続。
- 音声回線 第有るアップによるオペレーションセンタのゲートウェイとの接続。
- 緊急プロトコル(uucp等)によるオペレーションセンタのゲートウェイとの接続。
- ゲートウェイ管理者への通常の電話による連絡。
- ゲートウェイ管理者へのポケットベルによる呼出。
- ゲートウェイ管理者へのFAXの送付。
- オペレーションセンタへの通常の電話による連絡。
- オペレーションセンタへのポケットベルによる呼出。
- オペレーションセンタへのFAXの送付。

6 ゲートウェイ機能

ネットワークが広域に接続され、またその広域ネットワーク中に含まれるノードやサブネットワークの数が大きくなる時、経路情報の交換や経路決定に必要なオーバヘッドが非常に大きくなる恐れがある。これに対しては階層的な経路制御法が有効であると考えられている。しかし、これらの経路制御法はそれに対応したアドレス体系を採用し、それに基づいたネットワーク層プロトコルが実現されているネットワークでのみ使用可能である。現在のTCP/IPプロトコル体系では2段階(サブネット[6]使用によって3段階)の階層を有しているが、それ以上の階層を実現することは不可能である。

この問題点を広域分散環境という観点から、ネットワーク層プロトコルを大幅に変更することなく解決する一つの方法は、個々のアドレスの解釈を変更し、動的な解釈を導入することである。ゲートウェイにおける動的なアドレス割り当てと書き換えは、設定されるコネクションがアドレス空間の大

きさに対して大きくない場合に有効な方法である。この方法によって別なアドレス空間に写像されるメタネットを設定し、メタネット単位の経路制御を行なうことによって、経路制御上のオーバヘッドの低減が可能になる。

このようなゲートウェイにおける動的なアドレス割り当てと書き換えは、ユーザがネットワークサービスを使用する際に、名前からアドレスへの変換を統一的に利用することを前提に、名前サーバの問い合わせ時に割り当てを行なうものである。また、計算ノードの単位は以前としてホストを単位としており、いわゆる分散環境といった場合の要求を満たさない。

この方法をより拡張し、計算機のダウン等によるサービスやコネクションに対する障害を低下させる方法が **WIDE** の目的には必要である。その一つの方法として、この解釈の技術をより高いレイヤで行なうことを考えることができる。トランスポートレベルのアドレスからホストアドレスを排除または排除した解釈を行なう方法がある。つまり、ゲートウェイ等におけるアドレス書き換えをさらに拡張することになる。あるローカルなワークステーション群に対するアドレスを別に定義し、それを G とし、それに含まれるワークステーションを W_n とすると、G を目指してくる外部からの TCP セグメントまたは IP データグラムは、通常のネットワークの系では行き先を失ってしまう。しかしながら、その群に含まれるゲートウェイにおいて、$< G, port_1 > \rightarrow < W_3, port_7 >$ のような写像が定義されれば、適宜パケットの行き先を書換えることによって、正しい送達を行なうことができる。この際 TCP では、チェックサムの計算に仮想 IP ヘッダの内容も加味されているので、チェックサム部の補償が必要である。また、ゲートウェイではその逆変換も行なう。具体的な変換子の定義は、名前サーバなどとの密接な連携が必要である。

上記のような環境を定義することによって、一つの分散系あるいはネットワーク系は、あたかも単一マシンのように外部からは見ることができる。具体的にはある名前サーバを管理していたマシンのクラッシュは、たまたまその名前サーバと通信していた外部の計算機には問題が残るが、クラッシュの情報がゲートウェイに到達し、アドレス変換子が修正された瞬間に通常のサービスを外部に提供できるようになる。また、あるサーバが系内部で移動した場合にでも、通常の分散オペレーティングシステムにおけるプロセス移動の複雑なメカニズムをその系と通信する外部の計算機に要求しないので、広域分散環境で見られるような異機種性の強い環境では有利であると考えられる。このようなゲートウェイにおける機能は、経路制御における交換情報のトラフィックの減少と経路計算の簡易化を実現することができ、名前とアドレス処理の技術との組合せにより、ポリシーの行使、耐故障性の向上といった大規模分散環境のゲートウェイに関する要求を解決することができる。

7 セキュリティ

大規模分散環境では、多くの性格の異なる組織が相互に接続され、ネットワークサービスを提供・利用していくことが想定される。このような大規模分散環境では、第三者がネットワークに対して何らかの操作をして不正に情報を入手する危険性をもっている (以下、この様な第三者を侵入者と呼ぶ)。この理由として以下のようなものが考えられる。

1. ネットワークシステムが大規模になればなるほど、ネットワークを介しての遠隔の資源に対するアクセスが増加する。このため侵入者にとって、ネットワークシステムに対して攻撃をすることで情報の入手が容易になる。

2. ネットワークに分散している資源がネットワークを介して相互に接続されることにより、侵入者にとって攻撃する価値のある資源となる (例えばデータベース)。

3. ネットワークによって資源の共有が行われた場合、共有されている資源の保護は、その資源を持つ計算機システムでの保護だけでなく、ネットワークを介して利用している他のホストやネットワークでの保護にも影響されるようになる。

このような理由から **WIDE** においても、ネットワークの通信において、通信内容の保護、サービス利用者の特定、サービス利用者の制限などの機能が提供されることが望まれる。

7.1 モデル

Voydoc はネットワークにおける侵入者を図 2のようにモデル化した [12]。このモデルでは、階層構造をもつ通信プロトコルにおいて、通信を行うある $n+1$ 層のエンティティは双方向の通信路 (これを association と呼ぶ) を n 層が提供する機能を使用して確保する。$n+1$ 層のエンティティ間では PDU(Protocol Data Unit) をやりとりすることで通信を行う。このエンティティは安全なシステム内にあるとする。侵入者は、ネットワークから何らかの不正な方法によって情報を得たり、その運用を妨害するために、やりとりされる PDU に対して操作を加えるネットワーク内におかれた計算機システムと考えた。この場合、エンティティ間でやりとりされる PDU は全て侵入者を通過すると考える。

さらに Voydoc は、このモデルに基づいて、侵入者が行う攻撃として次のようなものを示している。

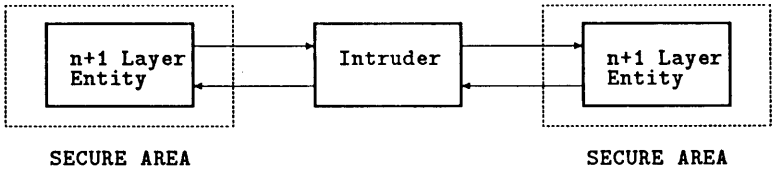

図 2: The association model

1. 消極的攻撃
   消極的攻撃とは、侵入者は単にネットワーク上で交換される PDU を盗聴することで情報を得ることを指す。これに属する攻撃としては次のものがある。

   (a) ネットワーク上でやりとりされる PDU を盗聴などの手段で不正に手に入れる行為 (release of message contents)。

   (b) メッセージ交換のプロトコルなどを解析するトラヒック解析 (traffic analysis)。

2. 積極的攻撃
   積極的攻撃とは、侵入者がネットワーク上のメッセージ交換に対して不正な変更を加えるような攻撃である。これらは次のように分類される。

   (a) message stream modification
   エンティティ間での PDU のやりとりに対して変更を加えるもので、(1)PDU に含まれる制御情報を変更して間違った宛先に PDU を送るようにしたり、偽造した PDU を流し込んだりする変更 (attack on authenticity)、(2)PDU 内に格納されたデータの変更 (attack on integrity)、(3) やりとりされる PDU を選択的に抹消したり、その順序を入れ換えたりする変更 (attack on ordering)、等の攻撃がある。

   (b) denial of message service
   エンティティ間でのメッセージ交換を無効にしてしまうような変更で、(1) やりとりされる PDU を全て廃棄してしまう (discard)、(2)PDU のやりとりを遅らせる (delay)、等の攻撃が含まれる。

   (c) spurious association initiation
   エンティティ間の通信を真似して他のエンティティと association を不正に確立しようとする攻撃で、(1) 以前にエンティティが通信していた内容を記録しておき、後になってそれをそのまま送りつける攻撃 (playback of a previous association)、(2) 侵入者が何らかの方法でエンティティと association を確立する攻撃 (association initiation on false identity)、等が含まれる。

7.2 WIDE におけるアプローチ

WIDE においては、Voydoc が提唱した association model を適用し、通信におけるセキュリティの問題を考える。

WIDE で提供するサービスにおいては、消極的攻撃に対してはそれを防止する機能を提供し、積極的攻撃に対してはそれを発見する機能を提供することが必要である。WIDE においては、各攻撃に対して次のようなアプローチをとる。

1. WIDE で提供するネットワークサービスの内、特定のサービスについてのみ通信内容の保護や、侵入者の攻撃から保護する必要がある。このため、すべてのネットワークアプリケーションが使用する、ネットワーク層やトランスポート層でセキュリティのための処理 (例えばデータの暗号化) を行うのではなく、特定のサービスに依存した階層 (例えば、プレゼンテーション層やアプリケーション層) において、セキュリティのための処理を行う。

2. PDU の盗聴による情報の入手に対しては、やりとりする PDU の内容の暗号化によって対応する。これにより、侵入者は暗号を解読できない限り PDU の盗聴によって、情報を得ることは不可能になる。

3. WIDE は研究ネットワークであるため、軍事ネットワークと異なり侵入者によるトラヒック解析が重要であるとは考えられない。このため、WIDE においてはこれを防止する手段は特に提供しない。

4. 侵入者が message stream modification を行うためには、PDU 内の情報を入手する必要がある。このため、PDU の内容の暗号化・PDU 内の制御情報の暗号化を行うことによって防止することが可能である。

5. association の不正な確立 (spurious association initiation) に対しては、暗号を用いた利用者認証を使うことで解決する。

6. denail of message service に対しては、各 PDU の送信毎に受信確認を要求したり、PDU に timestamp をつけて不正な PDU の転送遅延が加えられていないかを調べることで、プロトコルとして自動的に発見する機能を負荷することができる。しかしながら、これらの方法は通信コストがかかり、必要以上の処理を伴う。したがって、ネットワーク上でこの問題が発生した時にネットワークサービス毎に個別に対処する。

以上から **WIDE** においては、通信内容の暗号化機構と利用者認証システムの開発を行う。

7.3 利用者認証

これまで、ネットワークシステムにおける利用者認証方法は、多くの研究者によって各種の方式が提案されており、その多くが暗号を利用した通信プロトコルとして提案されている。代表的なプロトコルとして、Needham 等によってその代表的な手法が提案されており、文献 [9] では慣用系暗号と公開鍵暗号を用いた場合のプロトコルが示されている。これらの研究では、プロトコルを設計し、その安全性を議論しているが、実際のシステムの実現や運用における問題についてはあまり考慮していない。

実際に分散環境に利用者確認の機構を構築した例としては、MIT Athena Project の Kerberos[10] が代表的なシステムとして挙げられる。Kerberos では Voydock が [12] において示した方法を基礎に、UNIX システムを中心とした分散環境に対して利用者確認の機構を構築し、実際に Kerberos を適用した多くのネットワークアプリケーションを開発している。Kerberos では暗号化方式として慣用系暗号の DES を用いている。しかしながら、大規模分散環境を Kerberos を用いて管理した場合、一つの Kerberos サーバが管理するネットワークシステム (これをネットワーク A とする) に属す利用者が、他の Kerberos サーバが管理するネットワーク (これをネットワーク B とする) で提供されているサービスを要求する時には、利用者はまずネットワーク B にアクセスするためのチケットをローカルの Kerberos サーバからもらい、次にその鍵をもってネットワーク B の Kerberos サーバにアクセスする。すなわち、n 個の Kerberos サーバが存在するネットワークシステムでは n^2 個の鍵を Kerberos サーバにアクセスするために共有していなければならない。このため、大規模分散環境では Kerveros サーバの数は非常に多くなることが考えられ、それらの相互のアクセスをするための鍵の管理が難しくなるといった欠点がある。

以上のようなことから、**WIDE** では大規模分散環境に適応することのできる新たな利用者認証システムを開発する。このシステムでは、基礎となる暗号方式として公開鍵暗号を用い、Needham が提唱した公開鍵暗号を用いた利用者認証方式を適用することを検討している。これは、公開鍵暗号を用いることで各利用者に割り当てる鍵の管理の分散化が行え、さらに容易に鍵の更新などの運用上の処理が可能になり、大規模分散環境に適応できると考えられるからである。さらに、各利用者に割り当てた鍵を利用することで、通信内容の暗号化が行え、通信内容の保護ができる。

具体的には、現在大阪大学で開発している SPLICE/AS[1] を適用することを検討している。SPLICE/AS は Needham が示した公開鍵暗号方式を用いた利用者認証プロトコルを基礎とするシステムであり、鍵の分散管理、配送などを行うプロトコルが提供されている。また、広域ネットワークに対する適用についても考慮したシステムであり、**WIDE** に対して適用することが可能であると考えられる。

8 広域分散環境における時刻同期の問題

分散環境における幾つかのアプリケーションでは、リクエストやイベントの発生した時刻が問題となるものが数多くある。このようなアプリケーションでは、timestamp を用いてリクエストやイベントの発生した時刻をやりとりされるメッセージに付け加え、扱われることが多い。このような timestamp が正しく扱われるためには、ネットワーク上のノードの時刻が同期している必要がある。現在、時刻の同期をサポートするシステムとしては timed[4] があるが、timed の場合ネットワーク上の各ノードの時刻を合わすために同報通信を用いている。このため、broadcast channel が提供されることの少ない広域分散環境ではそのまま利用することは不可能であり、何らかの新たなシステムを開発する必要がある。

9 まとめ

広域大規模分散環境の構築に関する研究計画である **WIDE** の概要とその実験基盤の構築に関して報告した。ここでは、初期プロトコルとしてインターネットプロトコル (TCP/IP) を利用し、異種回線技術の開発を行なっている。その大規模性のために、経路制御のためのアドレスや名前、資源の名前に関連する技術の確立が基盤となり、組織間のネットワーク間接続を実現するために各ネットワークの自治性を尊重するための技術とともに、ゲートウェイの技術が実験開発の焦点となる。初期

研究計画は 2 ヶ年で、1988 年度と 1989 年度でプロトタイプを構築する予定である。

謝辞　本研究に関する多くの議論と助言を頂いた WIDE 研究会のメンバーに感謝する。

References

[1] 山口 英, 菱川 薫, and 宮原 秀夫. RPC を意識した分散処理環境における利用者認証機構の設計. In *マルチメディア通信と分散処理研究会*, pages SIGDSP 41–3, 1989.

[2] 村井純 and 田中啓介. 広域分散環境における資源管理. 情報処理学会 *マルチメディア通信と分散処理研究会 報告 88-MDP-36-10*, February 1988.

[3] 本田 和弘, 加瀬 直樹, 尾上 淳, 中島 達夫, 所 真理雄, and 村井 純. WIDE 上の X.25 機能の設計と実装. 情報処理学会 *マルチメディア通信と分散処理研究会 資料 DPS-42-9*, May 1989.

[4] Riccardo Gusella, Stefano Zatti, and James M. Boolm. The berkeley unix time synchronization protocol. *UNIX System Manager's Manual*, SMM:22, April, 1986.

[5] Kevin J.Dunlap. *Name Server Operations Guide for BIND.* University of California Berkeley, April 1986. UNIX System Manager's Manual(SMM).

[6] J. Mogul and J. Postel. *Internet Standard Subnetting Procedure.* August 1985. RFC 950.

[7] Jun Murai and Akira Kato. Current Status of JUNET. In *Future Generations Computer Systems*, pages 205–215, Elsevier Science Publishers B.V., October 1988.

[8] Jun Murai and Akira Kato. Researches in Network Development of JUNET. In *Proceedings of SIGCOMM '87 Workshop*, 1987.

[9] Roger M. Needham and Michael D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. *Communications of the ACM*, Vol. 21, No. 12:993–999, 1978.

[10] Jennifer G. Steiner, Clifford Neuman, and Jeffrey I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In *Proceedings of the USENIX 1988 Winter Conference*, pages 191–202, USENIX, 1988.

[11] V.G.Cerf and R.E.Kahn. A Protocol for Packet Network Interconnection. *IEEE Trans. on Communications*, COM-22(5):637–648, May 1974.

[12] Victor L. Voydock and Stephen T. Kent. Security Mechanisms in High-Level Network Protocols. In *ACM Computing Surveys*, pages 135–171, ACM, 1983.