論 文 内 容 の 要 旨

博士論文題目

Constructing Efficient Infrastructures for Secure Communication with Various Autonomy

（種々の自律度に応じた効率のよいセキュア通信基盤に関する研究）

氏 名　毛利 寿志

（論文内容の要旨）

計算機ネットワーク上で提供されるサービスが拡大されるに従い，セキュリティ保護等を目的としたシステム管理基盤技術がますます重要となっている．その一例として，信頼できないネットワーク上でセキュア通信を行うために必要不可欠な暗号鍵共有がある．一般的なネットワークでは，すでに実用的な公開鍵暗号技術などが研究されており，鍵共有方式を包括するセキュリティ基盤技術の構築が問題となっている．一方，アドホックネットワークやセンサネットワークなどのように，セキュリティ基盤技術の構築そのものが問題となっているようなネットワークも存在する．アドホックネットワークでは，ノードの移動性及び信頼できる第三者機関の不在などの制約により，既存の公開鍵暗号基盤をそのまま利用できないという問題点が指摘されており，信頼できる第三者を仮定しない公開鍵交換方式の構築が問題となっている．また，センサネットワークでは，センサノードの計算，通信，メモリ資源の制約により，公開鍵暗号や鍵共有プロトコルそのものの使用ができないため，事前に各センサノードに暗号鍵を埋め込んでおく方式が注目されている．

本論文では，従来のネットワークとアドホック，センサネットワークに関し，それぞれの特徴や制約に沿った効率のよいセキュリティ基盤技術を提案している．

信用管理とは，公開鍵暗号基盤に基づいたアクセス制御技術である．第2章では，システムの内部状態を導入した信用管理モデルを提案している．まず，システムの振る舞いを定義するために，ポリシ記述言語が提案されている．さらに，与えられたポリシが与えられた検証項目を満たすかどうかを決定する問題として検証問題が定義され，モデル検査手法を用いてこの問題を解く手法が提案されている．ある具体例についてPrologを用いたモデル検査手法の実装法が提案され，検証に要する時間が示されている．

アドホックネットワークにおける鍵共有手法に関する研究として，各ユーザが各自で公開鍵証明書を発行し合うような，web-of-trust 型信頼モデルが注目されている．第3章では，アドホックネットワーク上のweb-of-trust 型信頼モデルにおける証明書連鎖発見アルゴリズムを提案している．提案アルゴリズムは，信頼モデル上で証明書連鎖を探索する段階と，見つけた証明書連鎖を収集する段階から成る．探索段階では，信頼モデル上で生成木を構成する分散アルゴリズムを利用している．また，提案手法と既存手法の通信コストが数値解析，及び計算機シミュレーションによって比較され，提案手法の方が少ないコストで証明書連鎖を発見できることが示されている．

センサネットワークにおける鍵共有方式に関する研究として，センサネットワークの施行前に各センサノードに事前に鍵を複数組み込んでから各センサノードを配布する鍵事前格納方式が注目されている．第4章では，各ノードへの鍵事前格納について，代数幾何に基づいた新しい方式を提案している．具体的には，有限二次平面上の各格子点にそれぞれ異なる鍵を割り当て，ある一直線上にある全ての鍵を一つのノードに格納するような方式を提案している．さらに，提案手法の効率性，頑健性が数値解析によって評価され，提案手法の方が既存手法より効率が良く頑健であることが示されている．

氏　名	毛利　寿志

(論文審査結果の要旨)

本論文では，計算機ノードの能力とトポロジーの固定度が異なる3種の計算機ネットワークに対して，安全な通信を効率良く行うための以下のような新しい技法を提案している．

(1) PKI ディジタル証明書(以降，単に証明書と略記)に基づく認証と伝統的なアクセス制御技法を組合せることにより，サービス提供者と利用者双方の安全性を確保しつつ，できる限り利用者への利便性を高めるための信用管理技術が注目されている．しかし従来の信用管理モデルには状態の概念がなく，そのため実用的な信用管理に用いるには難点があった．本研究では内部状態の概念を陽に取り入れた新しい信用管理モデルが定義され，併せて，提案モデルにおける安全性を自動検証する手法が提案されている．実例題に対して Prolog や SPIN を用いた検証が行われており，提案手法の有効性が示されている．

(2) ノードの移動性等により，信頼できる CA を仮定できないアドホックネットワークにおいて，PKI による信用確立を行う有効な手法の一つに web-of-trust 型モデルがある．このモデルでは，あるノード u が他のノード v と安全な通信を行う場合には，u から v への証明書連鎖を発見し連鎖を構成する証明書をすべて収集しなければならない．本論文では，証明書連鎖発見手順を探索と収集の2つの段階に区分し，探索段階で送信されるパケットには発見された証明書を添付しない，収集段階では証明書を探索ノードに直接送信する，という効率化を行ったアルゴリズムを提案している．数値解析と計算機シミュレーションの双方により，従来手法と比較して証明書連鎖発見の効率が大きく向上することが示されている．

(3) 気象観測その他多くの分野でセンサネットワークの有用性が高まりつつある．センサノード(以下，センサと略記)は軽量であるため PKI のようなセキュリティ基盤は利用できない．そこで，あらかじめ出荷時に通信に用いられる暗号鍵を一定数各センサに格納し，センサ同士が同一の鍵を共有しているならばそれを用いて安全な通信を行うという，鍵事前格納方式が注目されている．なおセンサノードは通常の計算機と比較して盗難に遭う可能性が高い．そこで，任意の2つのセンサが同一の鍵を所有している確率(鍵共有確率)を高めることと，1つのセンサが盗難されても他のセンサ間の通信の安全性が失われない確率(対盗難耐性)を高めることが重要である．本論文では有限幾何における直線上の格子点集合をセンサに格納する鍵集合に対応づける手法を提案している．そして，解析的な手法により，鍵共有確率と対盗難耐性のトレードオフが従来手法より高まることが理論的に示されている．

以上の通り，本論文で提案する手法と得られた結果は，情報セキュリティ，とりわけ，計算機ノードの能力とトポロジーの固定度の異なる種々のネットワークにおいて安全な通信を実現するための効率的な手法を与えており，博士(工学)の学位論文として価値あるものと認める．