モーバイルコンピューティング環境におけるユーザ認証方式*

3W−4

石川 睦　田窪 昭夫　水野 忠則†

静岡大学情報学部‡

1 はじめに

NotePC や PDA の普及によって、コンピュータを持ち運ぶことが可能となり、いつでもどこでもというコンピュータ環境が実現されつつある。

しかし、インターネットに代表される既存のネットワークではホストやユーザの移動が考慮されていないため、こうした移動計算機によるネットワークの利用には様々な問題が生じる。

本研究では、移動計算機によるネットワーク利用に関する問題のうち認証に関するものを述べ、認証モデルの提案およびその性能評価を行なう。

2 モーバイルコンピューティング環境におけるユーザ認証

モーバイルコンピューティング環境ではホストやユーザは自由に動きまわり、どこでもネットワークが利用できることが要求される。

このような環境を考えた場合、ユーザが登録されていないネットワークにおいても何らかの方法で身分を保証できる仕組みを確立する必要がある。

モーバイル環境における既存の認証方式として、GSM や CDPD などが提案されている。

これらの方式は、主にデジタルセルラーネットワークをターゲットに開発されたものであることから、以下の図に破線で示した箇所、つまり認証を行なうサーバ同士を結んでいるネットワークが安全であると仮定されいるという問題がある。

図1 既存の認証方式の問題点

インターネットにみられる一般のネットワークを考えた場合、その部分は必ずしも安全であるとはいえない。

したがって、GSM や CDPD といった既存の方式を一般のネットワークで使用するには問題があるということになる。

3 認証方式モデル

ネットワークでのユーザ認証の方式としては既存の技術として、Kerberos がある。

Kerberos では認証サーバおよびチケットサーバがが発行したチケットと呼ばれる認証子を使って正規のユーザであることを証明する。

この Kerberos をモーバイルコンピューティング環境に当てはめると次の図のようなモデル A が考えられる。

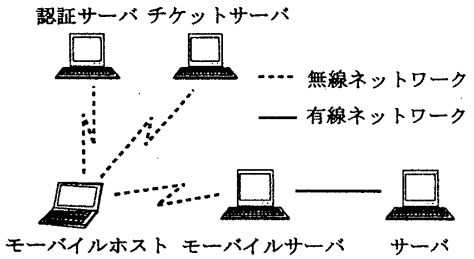

図2 モーバイル認証モデル A

*Authentication of Mobile Computing Environment

†Mutsumi Ishikawa,Akio Takubo and Tadanori Mizuno

‡Shizuoka Univ.

しかし、このモデルの場合、既存の Kerberos に加える修正が最小限で済むというメリットも考えられる一方、帯域が狭くセキュリティ的にも弱い無線ネットワークの多用や、制限が多く性能も低い移動計算機の負荷の増大などから、認証のオーバーヘッドは大きくなるものと考えられる。

そこで、これらを解決するため下図のようなモデルBを提案する。

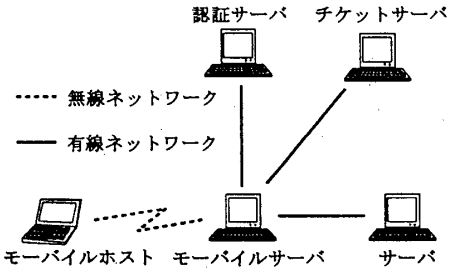

図3 モーバイル認証モデルB

このモデルでは、無線ネットワークの利用を最小限に押えることができ、移動計算機での処理を減らすことが出来る。

4 モデルの評価

今、提案した2つのモデルに関して、その違いがどの程度認証時のオーバーヘッドに影響を与えるかを確かめるため、簡単なシミュレーションを行なった。条件は以下の通りである。

- 認証要求の発生率λは、0.01 (件 / 秒)
- 認証サーバ および Ticket サーバへはλの100 倍の負荷がかかる
- 移動計算機の処理能力および無線ネットワークの速度をパラメータとする。

下図がその結果である。横軸に無線ネットワークの有線ネットワークに対する相対遅延時間、縦軸にモデルBに対するモデルAの相対認証時間をとってある。

また、result5 は移動計算機の性能を固定計算機の5分の1と仮定したもの、result1 は移動計算機と固定計算機を同等と仮定したものである。

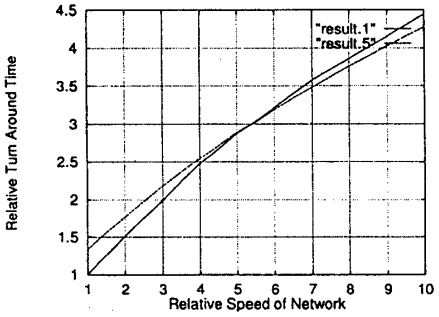

図4シミュレーションの結果

グラフより、移動計算機の処理能力や無線ネットワークの速度が固定計算機、有線ネットワークより劣る現状では、認証に要する時間が短いモデルB が有利であることがいえる。

また、移動計算機が高速な場合と低速な場合の相対認証時間が相対遅延時間 5.5 付近で逆転している。このことから、モデルA において性能の向上を図ろうとした時、移動計算機の性能を向上させるのは相対的に見ると効率の良い方法とはいえない。

5 おわりに

既存のモーバイルコンピューティング環境におけるユーザ認証の問題点について触れ、ユーザ認証に関して新たなモデルを提案し、その性能評価を行なった。

今後はより具体的な仕様について検討して行く方針である。

参考文献

[1] R.Molva,D.Samfat and G. Tsudik "Authentication of Mobile Users" *IEEE Network*, March/April 1994

[2] D.Samfat and R Molva "A Method Providing Identity Privacy to Mobile Users during Authentication" Workshop on MOBILE COMPUTING SYSTEMS and APPLICATIONS