3B-4

ユビキタスコンピューティングを構成する自律センサノードのセキュアな統合システムの開発 *

大林真人† 西山裕之† 溝口文雄†

東京都立産業技術研究所 情報科学グループ‡
東京理科大学 情報メディアセンター§

1 はじめに

近年，ユビキタスコンピューティングの構築による実環境の高度化，情報化を通じて，センサネットワークの利便性，重要性が認識されつつある [2]．センサネットワークは，無線通信機能を備えた非常に小型の計算機（ノード）によって構成されるものであり，多様なセンサを搭載した複数のセンサノードを，アドホックネットワークで相互接続することによって実現される．その適用事例としては，人体への装着や屋外における災害対策としての使用が考えられる．このとき，悪意ある攻撃者によって，パケットの改竄や，なりすまし，情報の傍受が安易に行われることを防ぐ必要が生じる．また，ユビキタス環境を構築するためには，ノード間における動的な協調が必要とされる．協調の具体例としては，状況の変化と環境内のセンサ反応に対応した機器制御や，特定環境における侵入者の認証が挙げられる．本稿では，これらの問題を解決するために，非常に限定されたリソースを使用することを前提とした，セキュアなセンサノード間協調システムを開発する．本システムは，我々の先行研究におけるマルチエージェントシステム [3] のフレームワークをセンサネットワークに適用することによって実現される．また，エージェント間協調におけるデータの暗号化および認証を実装することによってセキュアな協調動作を実現する．そして，評価実験により，本システムの有効性を検討する．

2 設計方針

2.1 TinyMRL 処理系の開発

我々は，センサネットワークを使用したユビキタス環境の構築の過程における上述した問題を簡単に解決することを目的として，センサノード間におけるセキュアな協調システムを実現するためのマルチエージェント言語”TinyMRL” の開発を行う．我々は先行研究において，マルチエージェント言語 MRL によるロボット間の動的な協調を実現している [3]．MRL は並列計算機上で動作することを前提とした処理系であり，並列論理型言語をベースとして，強力なユニフィケーション機能や共有変数の活用による分散・並列プロセス群の同期処理を簡潔に記述することに成功した言語である．しかし，MRL は並列計算機と UNIX を必要とするため，極めて限られたリソースしか持たないセンサノードに適用することは不可能である．また，論理型言語の記述性と特徴は難解であり，一般の開発者には受け入れがたい．さらに，通常の手続き型言語で使用される for，while ループなどの使用を許さないため，あらゆる種類の制御計算の記述が困難を極めた．これに対して，TinyMRL とは，西山らによるマルチエージェント言語 MRL をセンサノード上で動作させることを前提として組込み機器への実装に適合させた言語処理系である．この特徴として，非常に小規模なリソース (8bit や 16bitCPU を含む) を持つ計算機上で動作することが可能であることが挙げられる．MRL の特徴を引き継いだ点として，GHC(Gurded Horn Clause) によるルールの定義を伴う述語の集合によるエージェントの状態遷移を記述することを可能としている．また，無線によるデータ通信におけるセキュリティ機能を実装し，システムコールとして提供することによって，セキュアな通信を簡便に実装することを可能としている．図 1 は，動作ルールとして定義された述語群の実行処理の流れを示している．各述語は，名称や引数によってグループ化され，他の述語から呼び出されることによってグループ毎に実行可能状態に移る．そして，他のノードとの通信やセンサ入力値を使用してユニフィケーションが行われ，適合した述語のみが実行される．

2.2 TinyMRL 処理系のセキュリティ機能

一般に，センサノードとして使用するハードウェアは，一般の計算機と比較して非常に限られたリソースしか持たない．Perrig らによる μTESLA および SNEP

---

*The Design of Multi-agent System for Secure Sensor Network

†Makoto Obayashi, Hiroyuki Nishiyama and Fumio Mizoguchi

‡Tokyo Metropolitan Industirial Technology Research Institute, Information Science Group

§Tokyo University of Science, Information Media Center

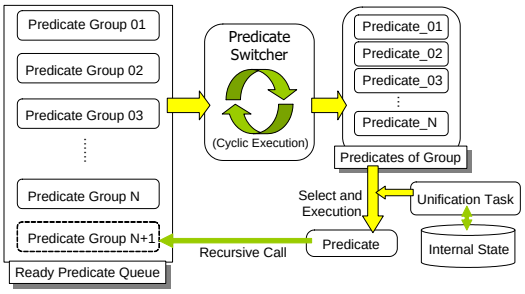

図 1: 述語の選択と実行の流れ

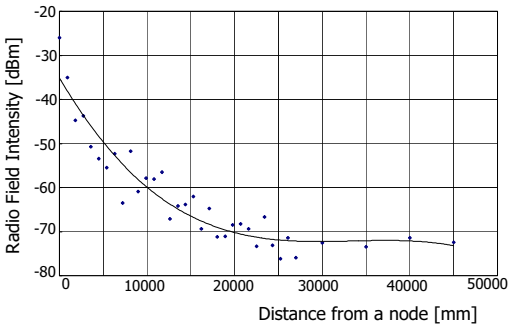

図 2: 実験環境において計測されたノードからの距離と電波強度の実測値

は，このようなデバイスによって構築されたネットワークにおけるセキュリティを確保することを試みている [1]．我々は，これらの関連研究によって提案されている手法を，マルチエージェントの処理系に融合させることによってシステムの構築を試みた．TinyMRL 処理系では，限られたリソースを持つセンサノード間のセキュアな通信を実現する機構を実装するとともに，エージェントアプリケーションからセキュリティ機能を隠蔽することによって，アプリケーションの開発者が意識せずにセキュアな通信を実現することを可能とする．TinyMRL 処理系が提供するセキュリティ機能は，データの暗号化による傍受の防止，セマンティックセキュリティの実現，データ認証である．ここで，開発者自身が設置した全てのノードは信頼することが可能であり，悪意のある攻撃者によるクラッキングの試みは，他のノードによるアドホックネットワークへの参加を通じて行われるものと仮定する．また，開発者自身が動作定義し，設置したノードには，あらかじめ，共通の秘密鍵を持つものとする．データの暗号化および復号化，データ認証に使用される全ての鍵は，信頼できるノードが共通して所持する秘密鍵から生成される．

3 評価実験および考察

次に，評価実験によって本システムによる有効性を検討する．なお，センサネットワークのデバイスには，Crossbow 社の MOTE MICA2（CPU:ATmega128L, ROM:128Kbyte，RAM:4kbyte）を使用した．我々の実験環境におけるセンサノードの電波強度を図 2 に示す．ノードは，約 15000mm の間隔で配置され，パケットは DSDV によるアルゴリズムによってルーティングされる．パケットのホップ回数と通信速度の結果は図 3 に示す通りである．グラフより，ホップ数の増加にしたがって，通信の所要時間が増加することが確認できる．また，パケットの認証処理や暗号化処理を付加することによって，処理時間が増大することが確認できる．しかしながら，その差は 200msec 程度であり，認証や暗号処理を行わないセンサネットワーク本来の処理速度・通信速度（図中の項目 C) を考慮すると，十分実用に耐えうるものと考えられる．

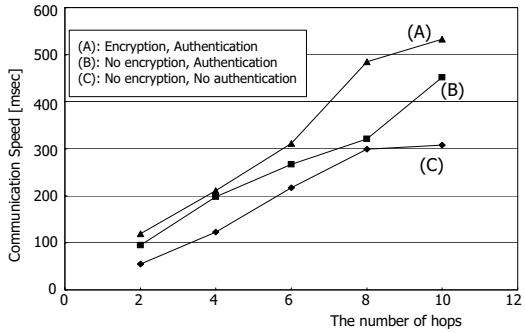

図 3: メッセージの暗号化・認証の実行とマルチホップによる通信に要する所要時間

4 結論

本研究において，我々は，アドホックネットワークを使用した相互通信を行うセンサネットワークのノード間相互作用によって発生する協調および競合の解消を実現するためのエージェント言語および処理系を開発した．また，無線アドホックネットワークにおける安全な通信を実現するために，限られたリソース上で動作するセキュリティシステムを構築し，エージェント処理系と融合させることによって，セキュリティを意識せずにセンサノードの動作設定を行うことを可能とした．そして，評価実験を通じて，我々の開発したシステムの有効性を示した．

参考文献

[1] A.Perrig , R.Szewczyk , V.Wen , D.Culler , J.D.Tygar, “SPINS: security protocols for sensor netowrks,” Proceedings of the 7th annual international conference on Mobile computing and networking, pp.189-199, July 2001, Rome, Italy.

[2] B.Warneke, M.Last, B.Liebowitz, and K.Pister. Smart dust: Communicating with a cubic-millimeter computer. IEEE Computer, pages 44-51, January 2001

[3] 西山裕之，大林真人，大和田勇人，溝口文雄: “ロボット間協調を容易に実現する並列論理プログラミング言語の設計”，ロボット学会誌，vol.19，No.5，pp.620-631，2001.