様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年６月３日現在

機関番号：13302
研究種目：若手研究（Ｂ）
研究期間：2010～2012
課題番号：22700066
研究課題名（和文）センサネットワークのセキュアで効率的なデータ集約技術に関する研究
研究課題名（英文）Research of secure and efficient data aggregation technology of a wireless sensor networks

研究代表者
面 和成（OMOTE KAZUMASA）
北陸先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：50417507

研究成果の概要（和文）：我々は，ランダムウォークを行う攻撃者が複数のノードを捕縛する攻撃に対して,効率的かつ安全なセンサネットワークのアグリゲーションプロトコルを提案した．我々のプロトコルは，TESLA 技術のアイディアを用いて，アグリゲーションと検証を同時に行うことによって結果チェックフェーズを設けずに，安全性を満たす１往復通信を達成した．また，我々のプロトコルの密集量，通信量，計算量が一定（O(1)）であることを理論的に示した．さらに，新たな認証セキュアアグリゲーション方式を提案した．

研究成果の概要（英文）：We proposed an efficient and optimally secure sensor network aggregation protocol against multiple corrupted nodes by a random-walk adversary. Our protocol achieved one round-trip communication to satisfy optimal security without the result-checking phase, by conducting aggregation along with the verification, based on the idea of TESLA technique. We also showed that the congestion complexity, communication complexity and computational cost in our protocol were constant, i.e., O(1). Furthermore, we proposed a basic MAC aggregation protocol.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	500,000	150,000	650,000
2011 年度	800,000	240,000	1,040,000
2012 年度	500,000	150,000	650,000
年度			
総　計	1,800,000	540,000	2,340,000

研究分野：情報セキュリティ
科研費の分科・細目：情報学，計算機システム・ネットワーク
キーワード：センサ，情報の完全性，アグリゲーション

１．研究開始当初の背景

近年，安心・安全・快適なユビキタス社会の実現に向け，センサネットワーク技術が注目を集めている．センサネットワークとは，センサノード（センサとデータ処理機能や無線機能を実装した装置，以下ノードと呼ぶ）を広範囲に分布させ，測定したセンサデータをノード間で無線通信するものである．センサネットワークでは，環境情報（気温や湿度など）や交通情報（人感，車感知など）などの様々な情報がセンシングされ，これらセンシングされた数多くのセンサデータが現稼働ノードのみで構成されるアドホックネットワークを通じて基地局に収集される．

センサネットワークにおいては，電池で駆動するノードの消費電力を抑えることが省エネルギーの観点からも重要である．その一方で，ノードに改ざん・なりすまし防止のセ

キュリティを実現するためには，その通信や演算にかかる消費電力が新たに必要である．低消費電力化の対策としては，少ない計算量やメモリ量でも実行可能なセキュリティの演算技術を利用することが有効である．さらに，他ノードからのセンサデータや認証データの中継もノード自身が行うため，各ノードの通信量を抑えることも低消費電力化の観点で重要である．そこで，近年セキュアアグリゲーションと呼ばれる通信量を削減する技術が盛んに研究されるようになってきた．セキュアアグリゲーションとは，合計値や平均値などの統計データを安全かつ効率的に得るために，各センサデータが中間ノードを介して集計されながら基地局に収集される方式である．残念ながら，一般的にセキュアアグリゲーション方式では個別ノードからの情報が失われるため，各ノードのセンサデータの改ざんチェックが困難になる．そのため，多くの方式では中間ノードが安全であることを仮定しており，中間ノードが改ざん・なりすまし等の不正を行う攻撃モデルのもとで未だ十分に解析・評価はなされていない．

セキュリティはデータアグリゲーションにおいて必須の要求事項である．なぜなら，一般的にセンサは安全でない場所に設置されるにも関わらず，耐タンパハードウェアを持たないためである．攻撃者は，リプレイ攻撃や改ざん，遅延，ドロップ，さらにはデータの順序を変えるといった不正を行うということを想定する．しかしながら，ほとんどのアグリゲーションプロトコルは，全ての中間ノード（センシングだけでなく他のセンサからのデータの転送も行うノード）が信頼できるものと仮定している．実際，中間ノードは不正が発見されないようにデータを改ざんできる．なぜなら，改ざんされたセンサデータは正当なセンサデータと区別できないからである．

効率性に関して，大規模なセンサネットワークにおいては，データの密集量が一定であることが重要である．センサはたいてい計算機資源が制限されており，電池駆動である．そこで電池を長くもたせるために，通信量を減らすことが最も重要である．特に，基地局周辺の通信量が膨大になるため，この部分のデータの密集量を抑えることが重要である．

２．研究の目的

本研究では，特に理論的な側面に着目しながら，センサネットワークにも適用可能な効率的な演算技術に対象を絞り，これまで少ない計算量やメモリ量で演算可能な改ざん・なりすまし防止技術や認証技術に関する研究を行う．これらは，今後ますます重要となる低消費電力化に大きく貢献できる技術である．本研究では，センサネットワークにおける更なる認証技術の発展のため，まずは差分チェックに基づく効率的なセキュアアグリゲーション方式を提案する．具体的には，ランダムウォークを行う攻撃者が複数のノードを捕縛する攻撃に対して，効率的かつ安全なセンサネットワークのデータアグリゲーションプロトコルを提案する．その後，このセキュアアグリゲーション方式を拡張し，センサデータの代わりに認証に必要なデータをアグリゲーションする方式（MAC アグリゲーションプロトコル）を検討する．

CPS プロトコルは，最適安全なセキュアアグリゲーションとして 2006 年に最初に提案された研究である．これは，共通鍵暗号ベースの方式であるため，密集量や通信量，計算量が効率的(センサ数の log オーダ)である．しかしながら，大規模なセンサネットワークを考える場合，次の 2 つの問題がある．

(1) 各センサの通信量のオーバヘッドが大きい．CPS プロトコルは，1 回のセンシングにおいて，各センサと基地局との間で 2 往復の通信を必要とする．

(2) 各センサの計算量が大きい．基地局だけでなく各センサも，自身のデータの完全性を検証するために最終的なコミットメントを計算する必要がある．上記 2 つの問題を解決するために，差分チェックに基づく効率的なセキュアアグリゲーションプロトコルを提案する．

本研究は，上記 2 つの問題を解決するものである．

さらに，新たな認証セキュアアグリゲーション方式の構築に向けて，まずは単一送信者，複数受信者のセンサネットワーク環境において，準同型性を持つ認証子（MAC）の検討を行った．これは，データアグリゲーションと同様の処理を行うネットワークコーディングにおける MAC 処理に関する研究である．ネットワークコーディング環境では，データが処理されるため，各データに MAC が付加されている場合，データ処理と同時に MAC も処理される必要がある．従来研究では，この MAC 処理が不十分であったので，本研究ではこの問題を解決する．

３．研究の方法

提案データアグリゲーションプロトコルは，既存研究の CPS プロトコルを改良するものであり，差分チェックに基づく手法である．特に，1 回のセンシングにおいて，各センサと基地局との間で 1 往復の通信しか必要としない利点を持つ．より具体的には，TESLA 技術のアイディアを用いて，アグリゲーションと検証を同時に行うことによって結果をチェックするフェーズを設けずに，安全性を

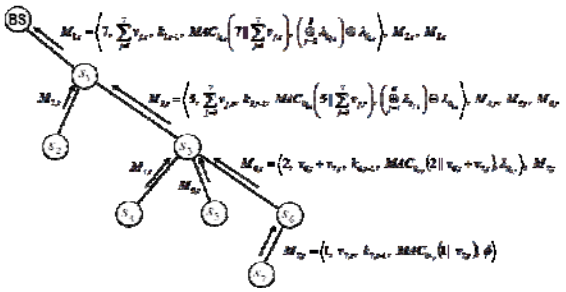

図 1 提案データアグリゲーション
プロトコルの具体例

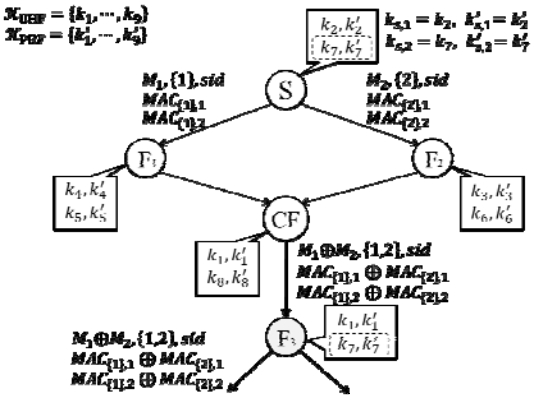

図 2 提案 MAC アグリゲーション
プロトコルの具体例

満たす1往復通信を達成した.TESLA技術は,共通鍵暗号ベースの効率的なブロードキャスト認証方式である．この TESLA 技術を適用することによって，前回のセンシング結果の検証と今回のセンシングを同時に行うことができる．

図 1 は，提案データアグリゲーションプロトコルの具体的な通信内容である．各メッセージは，センシングデータ，前回センシング時の MAC の秘密鍵，MAC，検証結果の MAC アグリゲーション値から構成される．前回センシング時の MAC の秘密鍵をここで暴露することによって，前回センシング時の MAC の正当性をチェックできる．また，検証結果の MAC アグリゲーション値は，正当性チェックのフラグに対する MAC のアグリゲーションであり，最終的に基地局のみがこれを検証できる．

提案 MAC アグリゲーションプロトコルは，一般的な準同型認証子の構成法の一つである Cater-Wagman MAC(データを入力とした(準同型)ユニバーサルハッシュ関数の出力に擬似乱数を加算したもの）に焦点をあて，まずは単一送信者，複数受信者のセンサネットワーク環境において，準同型 MAC の構築を行った．

図 2 は，提案 MAC アグリゲーションプロトコルの具体的な通信内容である．ここでは，XOR ネットワークコーディング環境を想定し，これと非常に相性が良い XOR 連結を行う Cater-Wagman MAC を用いた．これには秘密鍵が 2 種類必要であり，確率的鍵事前格納方式を用いることによって，中間ノードが確率的に MAC を検証できる．もちろん，基地局は全ての MAC を検証できる．図 2 から，MAC の数が終始 2 個になっている（MAC のアグリゲーションが達成されている）ことが分かる．

４．研究成果

セキュアアグリゲーションに関して 2 つのプロトコルを提案した．提案データアグリゲーションプロトコルでは，従来の研究では 2 往復の通信が必要であったのに対し，提案プロトコルでは 1 往復の通信で済むように TESLA 技術のアイディアを用いて改良され，通信量が大きく効率化された．この研究成果は，雑誌論文（①），学会発表（㉑,㉖）で発表された．

一方，提案 MAC アグリゲーションプロトコルでは，単一送信者，複数受信者の XOR ネットワークコーディング環境において，準同型性を持つ MAC を構築し，データが逐次変更されるデータの完全性を保つことができる方式を提案した．この研究成果は，学会発表（②,⑥,⑪）で発表された．

５．主な発表論文等

〔雑誌論文〕（計 3 件）

① Atsuko Miyaji and Kazumasa Omote , "Efficient and Secure Aggregation of Sensor Data against Multiple Corrupted Nodes", IEICE Trans., Information and Systems, vol. E94-D, No.10(2011), 1955-1965, 査読有

②Keita Emura, Atsuko Miyaji, and Kazumasa Omote, "A Timed-Release Proxy Re-Encryption Scheme", IEICE Trans., Fundamentals. vol. E94-A, No.8(2011), 1682-1695, 査読有

③ Kazumasa Omote and Kazuhiko Kato, "Practical and Secure Recovery of Disk Encryption Key Using Smart Cards", IEICE Trans., Information and Systems. vol. E93-D, No.5(2010), 1080-1086, 査読有

〔学会発表〕（計 26 件）

①Atsuko Miyaji and Kazumasa Omote, "How to Build Random Key Pre-distribution Schemes with Self-healing for Multiphase WSNs", The 27th IEEE International Conference on Advanced Information Networking and Applications, AINA 2013,IEEE, 1-8, 2013.3.25, スペイン, 査読有

②浅野貴哉, 宮地充子, 面和成. "ネットワ

ークコーディングに適した MAC の一考察″, The 30th Symposium on Cryptography and Information Security, SCIS2013 (2013-03), 2B4-1, 2013.1.23, 京都
③森俊貴, 面和成. ″Nexat を用いた攻撃予測に関する考察″, The 30th Symposium on Cryptography and Information Security, SCIS2013 (2013-03), 3C4-3, 2013.1.24, 京都
④Tran Thao Phuong, Kazumasa Omote, Nguyen Gia Luyen, and Nguyen Dinh Thuc, ″Improvement of multi-user searchable encrypted data scheme″, The 7th International Conference for Internet Technology and Secured Transactions, ICITST 2012, IEEE, 396-401, 2012.12.10, 英国, 査読有
⑤ Kazumasa Omote, Tran Thao Phuong. ″Improvement of Network coding-based System for Ensuring Data Integrity in Cloud Computing″, IPSJ SIG Technical Report, Vol.2012-CSEC-58 No.21, 2012.7.20, 札幌
⑥ Kazuya Izawa, Atsuko Miyaji, and Kazumasa Omote, ″Lightweight Integrity for XOR Network Coding in Wireless Sensor Networks″, The 8th International Conference on Information Security Practice and Experience , ISPEC 2012, Lecture Notes in Computer Science, 7232 (2012), Springer-Verlag, 245-258 , 2012.4.11, 中国, 査読有
⑦Tatsuro Iida, Keita Emura, Atsuko Miyaji and Kazumasa Omote, ″An Intrusion and Random-Number-Leakage Resilient Scheme in Mobile Unattended WSNs″, The 8th International Workshop on Heterogeneous Wireless Networks (AINA 2012 Workshops), HWISE 2012, IEEE, 552-557, 2012.3.27, 福岡, 査読有
⑧Keita Emura, Atsuko Miyaji, and Kazumasa Omote, ″A Revocable Group Signature Scheme with the Property of Hiding the Number of Revoked Users″, The 14th International Conference on Information Security and Cryptology, ICISC 2011, Lecture Notes in Computer Science, 7259(2012), Springer-Verlag, 186-203, 2011.11.30, 韓国, 査読有
⑨ Yusuke Sakai, Keita Emura, Goichiro Hanaoka, Yutaka Kawai, and Kazumasa Omote, ″Towards Restricting Plaintext Space in Public Key Encryption″, The 6th International Workshop on Security, IWSEC 2011, Lecture Notes in Computer Science, 7038 (2011), Springer-Verlag, 193-209, 2011.11.10, 東京, 査読有
⑩Keita Emura, Atsuko Miyaji, and Kazumasa Omote, ″Adaptive Secure-Channel Free Public-Key Encryption with Keyword Search Implies Timed Release Encryption″, The 14th Information Security Conference, ISC 2011, Lecture Notes in Computer Science, 7001 (2011), Springer-Verlag, 102-118, 2011.10.27, 中国, 査読有
⑪伊澤和也, 宮地充子, 面和成. ″汚染攻撃に耐性を持つ XOR ネットワーク符号化の比較・評価″, Computer Security Symposium, CSS2011-2B4-4 (2011-10), 498-503 , 2011.10.20, 新潟
⑫ Tatsuro Iida, Atsuko Miyaji, and Kazumasa Omote, ″POLISH: Proactive co-Operative LInk Self-Healing for Wireless Sensor Networks″, The 13th International Symposium on Stabilization, Safety, and Security of Distributed Systems, SSS 2011, Lecture Notes in Computer Science, 6976 (2011), Springer-Verlag, 253-267, 2011.10.11, フランス, 査読有
⑬飯田達朗, 面和成, 宮地充子. ″ワイヤレスセンサネットワークにおける自己治癒機能を有する鍵共有方式の検討″, IPSJ SIG Tech. Rep., Vol.2011-CSEC-52(2011-3), No.31, 2011.3.11, 大阪
⑭伊澤和也, 面和成, 宮地充子. ″ワイヤレスセンサネットワークにおける MicaZ を用いたデータアグリゲーション実装の検討″, IPSJ SIG Tech. Rep., Vol.2011-CSEC-52(2011-3), No.32, 2011.3.11, 大阪
⑮江村恵太, 花岡悟一郎, 川合豊, 松田隆宏, 面和成, 坂井祐介. ″メッセージ依存開示可能グループ署名と匿名掲示板への応用″, The 2011 Symposium on Cryptography and Information Security, SCIS2011, 3A1-4, 2011.1.27, 小倉
⑯江村恵太, 花岡悟一郎, 川合豊, 面和成, 坂井祐介. ″公開鍵暗号における平文空間の制限の実現に向けて″, The 2011 Symposium on Cryptography and Information Security, SCIS2011, 3C2-1, 2011.1.27, 小倉
⑰江村恵太, 宮地充子, 面和成. ″匿名 ID ベース暗号を用いたセキュアチャネルフリー検索可能公開鍵暗号方式の一般的構成法″, The 2011 Symposium on Cryptography and Information Security, SCIS2011, 4C2-6, 2011.1.27, 小倉
⑱ Hisashige Ito, Atsuko Miyaji, and Kazumasa Omote, ″RPoK: A Strongly Resilient Polynomial-based Random Key Pre-distribution Scheme for Multiphase Wireless Sensor Networks″, The 8th Grobal Communications Conference Exhibition & Industry Forum, IEEE GLOBECOM 2010, 1-5,

2010.12.7, 米国, 査読有
⑲江村恵太, 宮地充子, 面和成, ″削除機能付き匿名検証者指定署名とその応用″, IEICE Japan Tech. Rep., ICSS2010-47 (2010-11), 17-22, 2010.11.5, 広島
⑳江村恵太, 宮地充子, 面和成, ″時限式プロキシ再暗号化方式とその応用″, IEICE Japan Tech. Rep., ICSS2010-48 (2010-11), 23-28, 2010.11.5, 広島
㉑ Atsuko Miyaji and Kazumasa Omote, ″Secure Data Aggregation in Wireless Sensor Networks″, Computer Security Symposium, CSS2010-1D2-4 (2010-10), 177-182, 2010.10.19, 岡山
㉒Keita Emura, Atsuko Miyaji, and Kazumasa Omote, ″An Anonymous Designated Verifier Signature Scheme with Revocation: How to Protect a Company's Reputation″, The 4th International Conference on Provable Security, ProvSec 2010, Lecture Notes in Computer Science, 6402 (2010), Springer-Verlag, 184-198, 2010.10.14,マレーシア, 査読有
㉓Keita Emura, Atsuko Miyaji, and Kazumasa Omote, ″A Timed-Release Proxy Re-Encryption Scheme and its Application to Fairly-Opened Multicast Communication″, The 4th International Conference on Provable Security, ProvSec 2010, Lecture Notes in Computer Science, 6402 (2010), Springer-Verlag, 200-213, 2010.10.14,マレーシア, 査読有
㉔飯田達朗, 宮地充子, 面和成, ″マルチフェーズワイヤレスセンサネットワークにおける効率的かつセキュアな鍵共有方式″, Computer Security Symposium. CSS2010-1D2-3 (2010-10), 183-188 , 2010.10.19, 岡山
㉕Keita Emura, Atsuko Miyaji, and Kazumasa Omote, ″An Identity-based Proxy Re-Encryption Scheme with Source Hiding Property, and its Application to a Mailing-list System″, The 7th European Workshop on Public Key Services, Applications and Infrastructures, EuroPKI 2010, Lecture Notes in Computer Science, 6711 (2011), Springer-Verlag, 77-92 , 2010.9.23, ギリシャ, 査読有
㉖ Atsuko Miyaji and Kazumasa Omote, ″Efficient and Optimally Secure In-Network Aggregation in Wireless Sensor Networks″, The 11th International Workshop on Information Security Applications, WISA 2010, Lecture Notes in Computer Science, 6513 (2010), Springer-Verlag. 135-149, 2010.8.25, 韓国, 査読有

〔図書〕(計 0 件)

〔産業財産権〕
○出願状況 (計 0 件)
○取得状況 (計 0 件)

〔その他〕
ホームページ等
http://www.jaist.ac.jp/~omote/

６．研究組織
(1)研究代表者
面　和成 (OMOTE KAZUMASA)
北陸先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：50417507