6W-01

安全なM2M通信システムのためのグループ鍵管理手法に関する一検討

陳　致豪† 喜多　義弘† 朴　美娘† 岡崎　直宣‡
神奈川工科大学† 宮崎大学‡

1. はじめに

M2M(Machine-to-Machine)通信システムは，膨大な数のデバイス（センサノード）からデータを収集し分析する通信システムであり，近年ではスマートメータをはじめとする様々な社会基礎産業サービスで利用されている．しかし，M2M通信システムには，外部からの攻撃者や中継ノードのなりすましによるデータの傍受・改ざんなどの脅威があり，データの暗号化や送信元確認など機器間での安全な通信が必要になる．

M2M 通信システムで膨大な数のセンサノードを統括するサーバは，データの暗号化に必要な暗号鍵をセンサノードごとに配布・管理するため，安全で効率的な鍵管理手法が必要になる．

そこで本研究では，安全で効率的な鍵管理のための分散型グループ鍵管理手法について提案する．

2. 従来手法

データの暗号化は，データの傍受・改ざんを防ぐための手法として有用である．しかし，ノード数が多いセンサネットワークにおいて，グループに属する全てのノードに 1 対 1 で暗号化したデータを配布することは，サーバへの負荷が大きい．そのため，全てのノードが同一の暗号鍵を用いて暗号化を行うグループ暗号方式を用いることによって，サーバの負荷を軽減する方式が必要である．また，一般にセンサノードは電力が有限であるため，センサを長く使用するために通信量を減少させることは重要である．

サーバの負荷および通信量の軽減を行うため，LKH（Logical Key Hierarchy）というグループ鍵管理手法がある[1]．LKH は，鍵木と呼ぶ木構造に基づいて，ボトムアップに各ノードのグループ鍵を更新する手法である．各ノードのグループ鍵は，子ノードの鍵を用いて暗号化し，各ノードでの末端ノードに配布する．この手法により，暗号化した鍵のサイズや鍵配布に要する通信回数を削減できるため，効率的に鍵更新を行うことができる．しかし，ノードの離脱のたびにサーバは鍵更新を行う必要があるため，ノード数が多いほど鍵更新回数が増え，サーバの負荷が大きくなる．

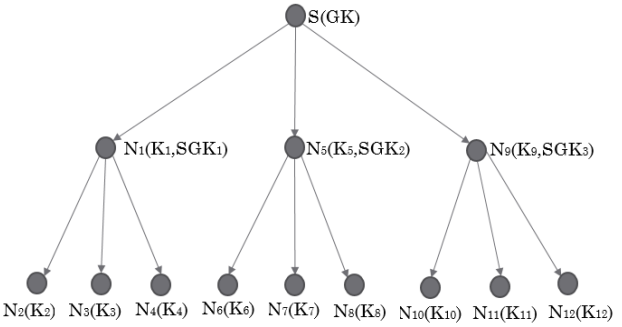

図 1．分散型グループ鍵管理手法

3. 分散型グループ鍵管理手法

本研究では，グループ鍵管理システム[2]に基づいて，M2M 通信システムの分散型グループ鍵管理手法を提案する．グループ鍵管理システムとは，各ノードが一時的なグループ鍵管理者になることで，サーバでの鍵更新回数を抑えるグループ鍵管理手法である．各ノードは子ノードとともに，自身を根とするグループ（以降，サブグループ）を形成する．そして，サブグループ内でノードの加入・離脱があった際，サブグループ鍵を作成し，サブグループ内に配布する．サーバは，サブグループにデータを送信する前に，グループ鍵を更新し，サブグループ鍵で暗号化し，サブグループ内にグループ鍵を配布する．この手法により，サーバはデータ送信時にグループ鍵を更新するだけで良いため，ノードの加入・離脱が頻繁に行われても，サーバでの鍵更新回数は増加しない．

グループ鍵管理システムでは，更新した鍵の暗号化に，公開鍵暗号方式を用いている．公開鍵を用いることによって，安全にサブグループ内で鍵を配信することができるが，センサノードの性能は有限であるため，公開鍵を用いることはノードへの負荷が大きい．そこで本提案では，対称鍵暗号方式を用いて暗号化を行う．

図 1 に，提案手法である分散型グループ鍵管理手法の全体像を示す．サブグループを管理す

A Study on Group Key Management Method for Secure Machine-to-Machine Communication Systems
Kanagawa Institute of Technology†
University of Miyazaki‡

るノード（Sub-Group Management Node，以降，SGM ノード）は，ルータ（コンセントレータ）であり，自身に隣接するノードと共にサブグループを形成する．図中において，S はサーバ，N_1～N_{12} はセンサノードを示し，SGM ノードは N_1，N_5，N_9 とする．K_i はノード N_i の対称鍵を示す．SGM ノードは予めサブグループ内の全ノードの対称鍵を所持していることを前提とする．

センサノードの離脱および新規加入におけるグループ鍵管理について，以下にそれぞれ述べる．

●センサノードの離脱

(1) 離脱するノードは，SGM ノードにグループからの離脱を依頼する．
(2) SGM ノードは，新しいサブグループ鍵（SGK）を生成し，サブグループ内の各ノードに対し，それぞれの対称鍵で暗号化して配布する．
(3) SGM ノードは，サーバにノードが離脱したことを通知すると共に新しいサブグループ鍵を送る．
(4) サーバは，データを全てのノードに配信する前に，全体用のグループ鍵（GK）を更新し，各サブグループに対し，それぞれのサブグループ鍵で暗号化して配布する．

●センサノードの新規加入

(1) 加入するノードは，最寄りの SGM ノードに加入要求を送信する．
(2) 加入要求を受け取った SGM ノードは，サーバに加入要求を転送する．
(3) サーバは，加入するノードの対称鍵を加入先の SGM ノードの対称鍵で暗号化し，SGM ノードに送付する．
(4) SGM ノードは，暗号化された対称鍵を自身の対称鍵で復号化し，加入するノードの対称鍵を取得する．
(5) SGM ノードは，新しいサブグループ鍵（SGK）を生成し，加入したノードを含むサブグループ内の各ノードに対し，それぞれの対称鍵で暗号化して配布する．
(6) SGM ノードは，サーバにノードが加入したことを通知すると共に新しいサブグループ鍵を送る．
(7) サーバは，データを全てのノードに配信する前に，全体用のグループ鍵（GK）を更新し，各サブグループに対し，それぞれのサブグループ鍵で暗号化して配布する．

4. 考察

提案した分散型グループ鍵管理手法は，ノード数が多いセンサネットワークを含む M2M 通信システムを対象にしている．そのため，ルータは移動せず，センサノードは移動可能であることを前提とする．センサノードが移動することにより，接続しているルータが変わることが想定される．その場合に，サブグループからの離脱および加入が発生すると考えられる．

LKH によるグループ鍵管理手法では，ノードの離脱および加入が発生するたびにグループ鍵を更新する必要があるため，サーバへの負荷が大きかった．本提案手法では，SGM ノードによってサブグループ単位での鍵管理を行うため，サーバは全体のグループ鍵を更新するだけで済み，かつ，鍵更新回数も減少する．そのため，サーバの負荷を軽減することができる．これらから，本提案手法によって安全で効率的な鍵管理を行うことができることが期待できる．

5. まとめ

本研究では，M2M 通信システムで安全で効率的な鍵管理のための分散型グループ鍵管理手法について提案した．サブグループを形成し，SGM ノードがサブグループ鍵を管理することにより，サーバでの鍵管理の負荷が軽減できる．また，グループ鍵は各ノードの対称鍵を用いて暗号化して配布するため，安全にグループ鍵を更新することができる．これらにより，本提案手法によって安全で効率的な鍵管理を行うことが期待できる．

今後の課題としては，大規模なネットワークにおいて，鍵更新時に管理する対称鍵数，サーバでの通信トラフィックや更新時間への影響について検討する必要がある．

参考文献

[1] 土江 康太,楫 勇一“センサネットワークにおける LKH グループ鍵配送について,” 第 31 回暗号と情報セキュリティシンポジウム(SCIS2014),3D5-4, pp.1-8, 2014.
[2] 朴 美娘,岡崎 直宣,妹尾 尚一郎“ダイナミックグループ暗号信号のための鍵更新システムの提案と評価,” 電子情報通信学会論文誌.D-I,情報・システム,I-情報処理 J87-D-I(10), pp.907-919, 2004.
[3] 八百 健嗣,中嶋 純,福井 潔“低リソースセンサノード向け代理配信可能データ認証手法の評価,” 第 31 回暗号と情報セキュリティシンポジウム(SCIS2014), 1D1-1, pp.1-7, 2014.