[研究論文]

安全な M2M 通信システムを実現するための グループ鍵管理手法に関する一考察

岡崎美蘭

情報ネットワーク・コミュニケーション学科

A Study of Group Key Management Method for Secure Machine-to-Machine Communication Systems

Mirang OKAZAKI

Abstract

In M2M (Machine-to-Machine) communication systems, sensor nodes send sensing information such as temperature or humidity to their server directly or indirectly through multi-hop routing. Since the sensor has a limited low cost and computational resources, a symmetric key encryption scheme is suited to encrypt sensory data. Recently, a hierarchical group key management method has been proposed to decrease the number of keys to be managed. However, since group key management devices are more expensive than sensor devices they should be efficiently deployed. In this paper, we propose an efficient group key management devices deployment scheme with k-means clustering algorithm.

Keywords: M2M, IoT, Group Key, LKH, key sharing, k-means

1. はじめに

近年ウェアラブルデバイスを始め様々なセンサーデバイスの普及により M2M(Machine-to-Machine) /IoT(Internet of Things)通信サービスが注目を集めている．M2M とは，多種・多様な産業設備からのセンサーデータを収集し分析することで，都市，環境，流通，農業，医療など多様な社会基盤産業における生産性を高め,新たなサービスの創出につなげることが可能になると期待されている［1-8］．例えば，農作物を生産する施設内の温度センサーデータを収集することで，適切な生産時期の把握，流通・消費・販売データなどの活用による生産性向上，エネルギーコスト削減,新たな食文化の創出などが可能になる．また，医療機器に通信機能を搭載することで，健康状態の遠隔管理や在宅の患者に対する遠隔診察などが可能となる．

M2M サービスは膨大な数のデバイスで成り立っており，人間が介在しないので,第三者からの破壊行為や不正使用によるデータの傍受・改ざんの危険性が高い．そのため，M2M では，正当な機器のみがサービスに参加できるように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 デバイスは，安価かつ小型であるため計算資源が限られており,暗号化処理に計算量の多い公開鍵暗号方式を用いることは困難である[9]．そこで共通鍵暗号方式を用いたデータの暗号化が適切である．しかし，M2M ネットワークにおけるノード数は非常に多いため，サーバが管理する共通鍵の数が膨大になるという問題がある．

そこでグループ暗号通信方式が注目されている.グループ暗号通信方式はグループの鍵管理が効率的であるが,グループメンバーの変更による鍵更新が必要とされる.グループ鍵の更新におけるサーバの負担および通信量を抑えることを目的として，LKH（Logical Key Hierarchy）と呼ばれるグループ鍵管理手法が提案されている[10,11]. 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.ここで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グループ鍵の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

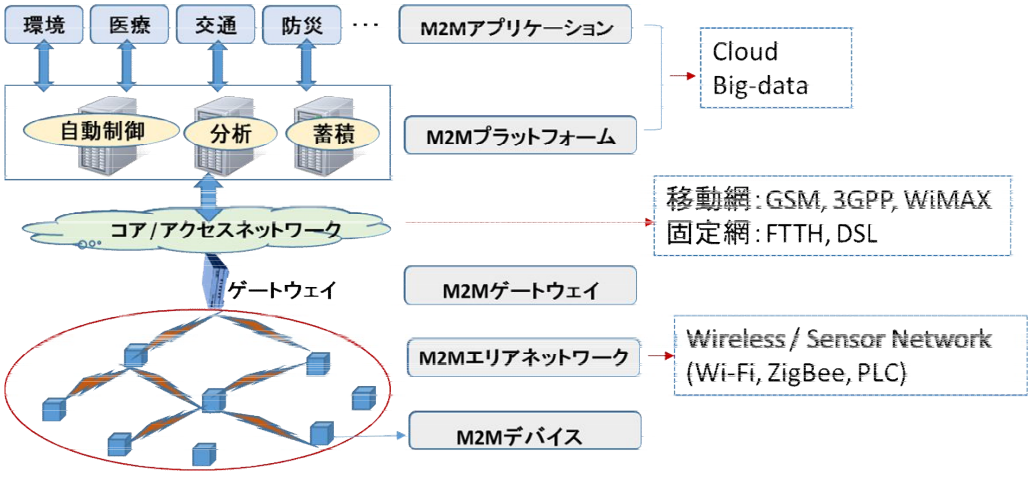

Fig.1 Structure of M2M System Architecture

の負荷が大きくなる．さらに，各ノードが管理する鍵数が多くなり，計算資源が限られたセンサネットワークへの実用化には課題が残る．

本研究では，グループ鍵更新におけるサーバの負荷を考慮した分散型鍵管理手法について検討する．そこで，自身に隣接するノードと共に任意のサブグループを形成し管理するノード（以下，SGM ノードと呼ぶ）を導入する． SGM (Sub Group Management) ノードは， 計算資源に余裕があり信頼できるノードである．SGM ノードを導入することでグループ鍵の更新時に配布する鍵数を低減させることができる．しかし，SGM ノードは一般的なデバイスノードに対して高価であり，多くのノードと通信を行うため，より効率的な配置が求められている．そこで，配置できる SGM ノード数を制限した際に，k 平均法を用いて SGM ノードの配置場所を効率的に決定する方式について検討する．これにより，無駄な SGM の配置を避け，各 SGM ノードが配下のノードと通信を行う際に必要とする電力量を低減し，通信距離およびホップ数を改善することが期待される．最後に計算機シミュレーションにより， 本方式の有効性を示す．

以下，2 章では M2M 通信システムのセキュリティ要求条件，3 章ではセキュリティソリューションについて述べる．4 章では，本研究での提案方式である分散型グループ鍵管理手法について示し， 5 章で評価を述べる．

2. M2M 通信システムのセキュリティ要求条件

2.1 M2M 通信システム構造

M2M (Machine-to-Machine) とは， 人間の介在なしに遠隔の機器同士が通信を行うことである．そもそも機械同士が通信し会うこと自体は目新しいことではない． 例えば，水位や流量などの河川情報のテレメータ観測，自動販売機の管理システム，重機のモニタリングシステム，エレベータの状態監視システム，公共バスの運行管理システムなども M2M 通信システムである．

しかしながら，近年スマートコミュニティ，スマートシティ，スマートグリッド，スマートウォーターなどに代表されるように，持続可能な社会の構築が求められるようになってきたことが，M2M に対して新たな視点を与えている．スマート化を図るためには，消費電力，流通，交通，位置，利用履歴などの多様なデータをセンサーなどから収集し，得られたデータを有機的に結合し，社会基盤の効率化及び高度化を実現しなければならないためである．

図 1 に M2M 通信システムのアーキテクチャを示す．システムを構成する機能は次のようになる．

(1) M2M デバイス

自販機，自動車，メディカルデバイス，複合機，スマートメータ，工作機器などのセンサーやアクチュエータ群として，各種アプリケーションが組み込まれている．M2M デバイスは， コア/アクセスネットワークと次のような 2 つの形態で接続される．

・**直接接続：**M2M デバイスに WAN 通信モジュールが装備されており，通信事業者のアクセスネットワークに直接アクセスする形態になる．この場合，M2M デバイスはネットワークやアプリケーションドメインに対する登録， 認証，許可，管理およびプロビジョニングといった手順を自ら実行することになる．

・**ゲートウェイ経由の間接接続：**M2M デバイスが M2M ゲートウェイを経由してネットワークやアプリケーションドメインに接続される形態である．この場合 M2M デバイスは，M2M エリアネットワークを使ってゲートウェイに接続される．この接続形態は，アプリケーションの実行のみを可能とするような低価格デバイスに適用される．また，上記で挙げたアプリケーションに対する登録，認証，許可，管理などの手順を実行するためには，M2M ゲートウェイに実装された M2M サービス提供能力 (SC: Service Capability) を利用する．

(2) M2M エリアネットワーク

M2M デバイスと M2M ゲートウェイの間の接続を行うための近距離無線技術 (ZigBee, Bluetooth, 無線 LAN 等) や電力線通信 (PLC: Power Line Communication) 技術を指す．

(3) M2M ゲートウェイ

コア／アクセスネットワークからの接続を終端し，エリアネットワークへの中継機能を提供する装置として，サーバとデバイスとでデバイス管理プロトコル（OMA-DM）やデータ取得プロトコルが異なる場合の変換，サーバから直接到達できないデバイスに対する遠隔初期設定の支援などの M2M SC を実装している．これは，通常１つあるいは複数の M2M エリアネットワークへの接続を可能とする．

(4) M2M プラットフォーム

複数のアプリケーションが汎用的に使用可能なコア／アクセスネットワークの共通機能を提供するミドルウェア（ソフトウェア）である．M2M プラットフォーム事業者によって提供され，ETSI TC M2M[4]や TIA TR-50[5]などで標準化が行われている．

ここでは，M2M デバイスのモニタリング，故障検知，課金，認証，アクティベーション，SIM カード管理などとともに，ローミングやプロバイダの切り替えなどのサポート機能を担う．

(5) M2M アプリケーション

個々の M2M サービスに対応して，クラウド上のアプリケーションサーバ上で動作するものとして，M2M サービス事業者によって提供される．例えば，電力会社が提供するスマートメータの収集や解析を行うバックエンドのアプリケーションが挙げられる．アプリケーションは，インフラ側の M2M サーバとフィールド側の M2M デバイスに組み込まれて動作する．

2.2 M2M における安全性の問題

多くの M2M ソリューションは膨大な数のデバイスで成り立っており，かつそれらのデバイスが扱うデータ量はわずかで，各デバイスからのデータ伝送量もきわめて少ない．M2M デバイスは人間が介在しないので，第三者からの破壊行為や不正使用による危険性がある．

例えば，本来はユーザの心拍数や血圧を計測しネットワーク経由で健康状況を監視するために用いられる M2M デバイスから，悪意のある第三者が通信モジュールを引き抜き，自らのスマートフォンに SIM カードとして挿入し不正利用することができる．これは，端末をネットワークに登録するために必要なあらゆる情報が SIM カードに記録されているからである．すなわち，ネットワーク側からは，不正に SIM カードを利用している端末を明示的に特定する手段がないということである．

一方，不正アクセス者は，SIM カードを抜き取ることなく，M2M デバイスとアクセスネットワーク間に交わされている制御信号やデータトラフィックを盗み取ることで，正当なデバイスの認証情報を不正取得することもできる．

2.3 M2M セキュリティの要求条件

M2M サービスは通信事業者，M2M オペレータ，アプリケーションプロバイダ，エンドユーザ，およびデバイスメーカなど複数のプレイヤーにより提供される．ここでは，想定される脅威からエンド・ツー・エンドで各プレイヤーを保護するために必要となる M2M セキュリティの要求条件について述べる．

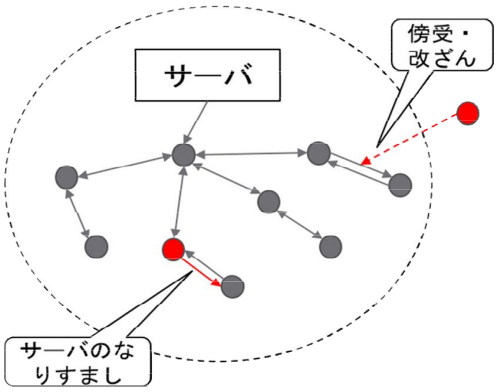

Fig.2　Security Problem of M2M System

(1) M2M デバイスユーザを保護するための要件

多くの M2M デバイスから集められるデータは本来守秘性が高いものである．例えば，子供の位置情報をリアルタイムで追跡して取得するアプリケーションでは，権限が与えられていない者に子供の位置情報を取得されてはならない．従って，蓄積されたデータに関する情報がネットワーク上のいかなる場所にあっても盗まれないようにしなければならない．

また，デバイス ID は位置情報など他のデータと関連付けられていることが多いので，それ自体が価値ある情報となっている．従って，いくつかのアプリケーションでは，エンドユーザ ID を見せないようにすることが重要となる．ユーザ ID が判明することによりデバイスとその利用履歴がネットワーク上で不正者によって盗み取られないように，デバイス ID は暗号化をすべきである．

(2) ネットワークプロバイダを保護するための要件

一般的に M2M デバイスは，アプリケーションプロバイダによって保有され，エンドユーザの住居や施設内にて利用されることが多い．例えば，スマートメータの場合，メータは電力会社によって保有され，家庭や小規模な事業所などで利用され，場合によっては屋外など監視や保護が行き届かない場所に設置されている．従って，これらのデバイスは盗難の危険性に晒されている．

不正者が正当なデバイス情報を利用してネットワークサービスへアクセスする形態も，通信事業者に対する脅威となる．この形態の攻撃は，マルウェアやスパイウェアなどのように，悪意あるソフトウェアを利用することで M2M デバイスではない端末（スマートフォンや PDA など）からも実行可能である．M2M サービスでは，次の特徴からこのような攻撃を受けやすい．

・安価なデバイス：心拍モニタデバイスの中でも低コス

トなものは，1分間あたりの平均脈拍を測定し，携帯電話網を介してリモートサーバにこの情報をおくるだけがその機能になる．このようなデバイスは，一般にそれ以上の機能やタスクを持たない.同様に家庭向けスマートメータの場合も,一定期間中に使用された電力や水の量を測定し,この情報を電力会社,水道会社に送信することが唯一の機能になる．つまりデバイスは，他のデバイスやサーバと接続する必要はなく,通信モジュールは単一のデータセッションに特化して製造されていればよいことになる.従ってこのようなデバイスは通常，安価にはなるが，構成がシンプルなため偽装や改ざんなど不正行為が容易となり,不正アクセス者にとってハッキングがしやすくなる．

・アクセスの容易性：M2M サービスでは，多くのデバイスが見える場所に物理的にアクセス可能な状態で設置される静的な構成が多い.これには2つの問題がある.第一に,不正アクセス者がデバイスに物理的なアクセスをして,取り外し可能なカードに記載されている認証情報を抜き取り,その情報をもとに悪意ある行動をとることが可能であること．第二に，不正アクセス者は容易にアクセスネットワーク ID や，割り当てられている一時的な M2M デバイス ID を特定することができることである．

(3) アプリケーションプロバイダを保護するための要件

不正アクセス者は,デバイスからアプリケーションサーバに伝送されるデータ（または，逆方向のデータの場合もあり得る)を改ざんすることによって不当な利益を得る可能性がある．または，ネットワーク上の他のデバイスを装って，サーバにデータをアップロードすることでできる．例えば，スマートメータサービスにおいて，悪意をもった家庭のオーナーが電気料金の支払いを逃れるために,メータ ID を変えて隣人を装うこともできる．また，不正アクセス者が不当なデバイスを正当なデバイスであると偽り，正しくない情報をサーバに送信するケースもあり得る.従って，次の共通のセキュリティ要件が必要となる．

・相互認証：サーバは認証された M2M デバイスのみがネットワークと M2M システムにアクセスできるようにしなければならない．一方 M2M デバイス側でも，コマンドや管理に伴うアップデートなどのデータを受信する前にサーバを認証すべきである．このような相互認証処理は，M2M デバイスと M2M サービスプロバイダのネットワーク間で，データ伝送が開始される前に完了しなければならない．

(4) ブートストラップにおけるネットワーク認証の要求

M2M サービスでは，多くのデバイスが利用されるが，各デバイスから伝送される個々のデータ量は少ない.従って,デバイスの利用や維持にかかる支出を抑える必要がある．そこで，デバイスのブートストラップ（起動）は，できるだけ自動化されるべきである．

さらに通信事業者は,いつデバイスがブートストラップアプリケーションを実行するか分らない．そこで，デバイスがセキュリティ鍵や他の信頼情報をまだ処理していないにもかかわらず,通信事業者にデバイスを認識させデータ通信を許可するためのネットワークアクセス ID を使ったデバイス認証が必要となる．

3. M2M におけるセキュリティソリューション

安全な M2M サービスを提供するためには，データの暗号化はもちろんデバイスのアクセス制御，M2M ノード間の安全な通信路の確立，デバイス ID の保護対策を行う必要がある．本研究では，M2M データの暗号化における鍵管理問題について検討する．

3.1 暗号化方式

M2M 通信システムにおけるデータの暗号化方式には共通鍵暗号方式と公開鍵暗号方式が考えられる.一般的に共通鍵暗号方式は,暗号化に伴う処理を高速に行うことができる一方,サーバは各デバイスに対して個別に鍵を用意する必要がある．一方，公開鍵暗号方式を用いた場合，サーバは自身の秘密鍵と公開鍵のみを管理すればよいが,暗号化処理の演算量が膨大となる欠点がある．

M2M デバイスには，コスト削減の必要性からプロセッサの能力の制約のあるセンサーなどが使用されるケースが多い.また,センサーのようにデータの取得だけではなく,アクチュエータなどサーバ側から機器の電源の ON/OFF やソフトウェアの更新など,何らかの動作を制御するためのメッセージを送信するケースも考えなければならない．従って計算資源の限られたセンサー端末において,公開鍵暗号方式の利用は不適である．

M2M デバイスの乗っ取り対策として，次のような方法により保護する．この方法では，不正アクセス者がデバイス ID と共通の秘密鍵を取得できない限り，端末を乗っ取ることはできない．

・送信側は共通の秘密鍵を用いて，パケットの中身をハッシュ化し，それをメッセージの末尾に付加する．

・受信側は，同じ秘密鍵を用いて受信データのハッシュ化を行い,メッセージに付加された送信側のハッシュ値との比較を行う．もし，ハッシュ値が一致したら，受信側はそのメッセージの信頼性が確認できたことになる．

3.2 グループ鍵管理手法

共通鍵暗号方式を利用する際に,サーバが管理しなければならないデバイスの共通鍵数を低減するために,複数のデバイスをグループ化して一つのグループ鍵（GK:Group Key）を用いて暗号化を行うのが効率的である．

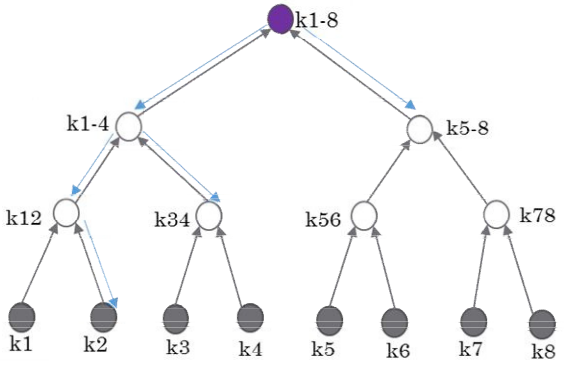

Fig.3　Example of LKH

グループ鍵暗号方式において，サーバはネットワーク全体で共通のグループ鍵を用いてデータを暗号化し，各ノードに送信する．しかし，グループメンバーの加入・離脱のたびにグループ鍵を更新する必要がある．また，一つの鍵を長期間使用することはセキュリティ上問題があるため，グループ鍵を定期的に更新する必要がある．グループ鍵の定期更新や新規メンバーの参加の場合は，それまで使用されていたグループ鍵で新しいグループ鍵を暗号化し，同報通信で送信すれば良いが，メンバーが離脱した場合は，新しいグループ鍵の暗号化のために古いグループ鍵を使用することはできない．そこで，各メンバーがサーバと個別に共有する鍵を用いて新しいグループ鍵を配布することが考えられるが，サーバでメンバー数と同じ回数のグループ鍵暗号化処理が必要となるため非効率である．

グループ鍵の更新におけるサーバの負担およびネットワークの通信量を抑えることを目的とした LKH(Logical Key Hierarcy)と呼ばれるグループ鍵管理手法が提案されている[10, 11]．LKH では，図 3 に示すような木構造を用いて鍵管理を行う．ここで，各葉ノードはグループのメンバーと一対一に対応しており，i 番目のメンバーは葉ノード ki と同一になる．サーバ（根ノード）は i 番目のメンバーに対し，ki から根ノードに至る経路上にあるすべてのノードに対して，ノード鍵と呼ばれる暗号鍵を割り当てる．例えば，図 3 の k_1 に対応するメンバーには，k_1，k_{12}，$k_{1\text{-}4}$，$k_{1\text{-}8}$ の 4 つのノード鍵が与えられる．ここで，根ノードのノード鍵 $k_{1\text{-}8}$ はすべてのメンバーが所有するため，グループ鍵と呼ばれる．

LKH におけるグループ鍵更新は鍵木に基づいてボトムアップに行われる．例えば，図 3 で k_1 を所有するメンバーが離脱する場合，このメンバーが所有するノード鍵 k_{12}，$k_{1\text{-}4}$，$k_{1\text{-}8}$ は安全ではないので，新しいノード鍵に置き換え，これらの鍵を所有するメンバーに配布する必要がある．そこで，まず k_{12} の新しいノード鍵（k_2 とする）をその子ノード鍵 k_2 で暗号化して k_2 をもつメンバーに送信する．同様に $k_{1\text{-}4}$ の新しいノード鍵（$k_{2\text{-}4}$ とする）を新しいノード鍵 k_2 および k_{34} で暗号化し，それぞれのメンバーに送信される．最後に新しいグループ鍵（$k_{2\text{-}8}$ とする）は，$k_{5\text{-}8}$ および先ほど更新された $k_{2\text{-}4}$ でそれぞれ暗号化し，それぞれのメンバーに送信される．このようにサーバが送出する鍵更新の通信回数は 5 個であり，グループ鍵を各メンバーに個別に送信する手法と比較して，2 個低減させることがわかる．

一般にメンバー数 N，鍵木が次数 d の階層で表されるとき，サーバが送出する鍵更新の通信回数は $d\log_d N$ となる．しかし，ノード数が多いセンサネットワークの場合，LKH の鍵木の次数 d が大きくなり，すべてのノードが鍵更新を終える前には，ノード間の暗号通信ができない問題点がある．さらに，各ノードが管理すべき鍵数が次数 d と同じとなり，計算資源が限られたセンサノードへの適用においては課題が残る．

LKH と類似の仕組みをスマートメータに適用した手法が提案されている[12]．しかし，この手法はサーバが全てのグループ鍵を作成・管理しているため，サーバの負荷が重い．Eschenauer 等が提案した EG プロトコル[13]はサーバが事前に要素鍵プールを作成し，鍵プール中の鍵をランダムに各ノードに送信する．そして，ブロードキャストを行う際に，各ノードがランダムに配布された鍵の最適な組み合わせによって，ブロードキャストする．本方式ではサブグループに依存せずに，目的のノードに直接データを送信することが可能であるが，事前に全てのノードに大量の要素鍵を格納する必要がある．また，グループ外のノードがグループ鍵を用いて復号できるという問題もある．また，金子等[14]はサーバが幾何学的性質を利用することで，単一のメッセージ送信のみで，各ノードに鍵配送を行う方式を提案している．各ノードは固有鍵 1 つを持ち，サーバが

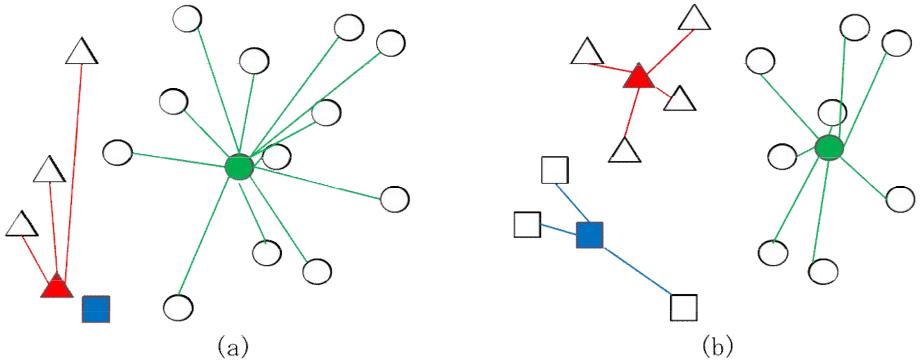

Fig.4　(a) SGM allocated in random　　(b) SGM allocated by k-means method

グループ鍵を配送するノードの数によらず，1 つのメッセージのみで容易にグループ鍵を配送できる特徴をもつ．しかし，本方式はサーバおよびノードの両端末において計算量が多く，解析攻撃に弱いというセキュリティ上の問題が課題として残っている．

本研究では，安全性が保証されている観点から，LKH に着目する．しかしながら，上述のように，LKH はサーバの負荷とグループ鍵の更新に時間がかかるという問題点がある．そこで， 我々は LKH におけるサーバの負荷とグループ鍵を更新する即時性を改善する手法について検討する．

4. 分散型グループ鍵管理手法

本研究では，グループ鍵更新におけるサーバの負荷を改善するための，分散型グループ鍵管理手法について検討する．

4.1 SGM（Sub-Group Management）ノード導入

本研究では，LKH における問題点を解決するために，自身に隣接するノードと共に任意のサブグループを形成し管理するノード（以下，SGM ノードと呼ぶ）を導入する．SGM ノードは，自身を根とするサブグループを形成し，サブグループメンバーを管理することができるサブグループ鍵（SGK:Sub-Group Key）を生成し，サブグループ内に配布する．また，サブグループ内でノードの加入・離脱があった際には，新規のサブグループ鍵（SGK）を作成し配布することで，M2M デバイスのグループ鍵を管理することができる．

SGM ノードとは一般的なデバイスノードに対して高価で，コンセントレータのような高計算能力を持つデバイスを想定する．従って，より効率的な SGM ノードの配置手法を検討しなければならない．すなわち，各 SGM ノードをランダムに配置した場合と比較し，通信に伴う消費電力量を低減できるように設置しなければならない．

4.2 k 平均法を用いた SGM 配置手法

k 平均法は与えられた n 点を k 個のクラスタに分類するクラスタリングアルゴリズムのひとつである．最初に k 点をランダムに選択し，n 個のノードを k 個のうち最も近傍に位置する点のクラスタに分類する．その後分類された各クラスタの重心までのユークリッド距離の和が極小となるような k 点の位置を得ることができる．

図 4 に，(a)ランダムに 3 つのクラスタの重心が選択された場合と，(b)k 平均法によって 3 つのクラスタの重心が選択された場合の例を示す．図中において，丸，正方形と三角型は各クラスタを示し，色が塗られたものは各クラスタの重心の位置を示す．ここで白抜きのものをセンサノード，色で塗られたものを SGM ノードとみなす．図 4 からわかる通り，k 平均法を用いることにより，センサノードと SGM ノード間の距離を短くすることができ，通信に必要な消費電力を低減できることが期待される．

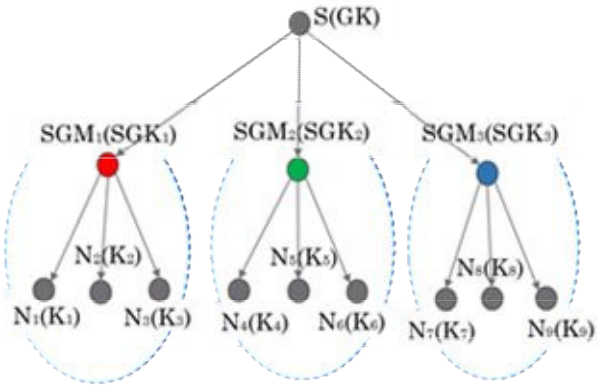

Fig.5 Distributed Group Key Management Method

● k 平均法を用いた SGM 配置アルゴリズム

(1) n 個のセンサノードが配置された M2M ネットワークに対し，配置する SGM ノードの数 k を定め，ランダムに k 個の SGM ノードを初期配置する．

(2) 各 SGM ノードは周囲のセンサノードを自身の一番近いクラスタに所属させる．

(3) 各クラスタの重心を計算し，それらの点に SGM ノードを再配置する．

(4) (2)に戻って繰り返し計算する．各ノードの所属するクラスタおよび重心に変化がなくなったら，操作を終了する． □

4.3 分散型グループ鍵管理手法

図 5 に，k 平均法に基づき SGM を配置した場合の M2M ネットワークの分散型グループ鍵管理手法の全体像を示す．図中において，S は鍵管理サーバ，N_1～N_9 はセンサノードを示し，SGM ノードは SGM_i とする．各センサノード N_i にはノードの固有鍵 K_i を所持していることを前提とする．また，SGM ノードは予めサブグループ内の全ノードの固有鍵を所持しているとする．SGM ノードはサブグループ鍵（SGK）を作成し，サブグループ内のノードの固有鍵で暗号化して配布する．さらに，サーバ S はすべての SGM ノードのサブグループ鍵(SGK_i)を所持していると仮定する．

グループ鍵を共有する手順は次のようになる．

(1)鍵管理サーバ S はグループ鍵（GK）を生成し，各サブグループ鍵(SGK_i)で暗号化して SGM ノードへ配布する．

(2)SGM ノードは，グループ鍵（GK）を各ノードの固有鍵 K_i で暗号化して配布する．

サーバ S がグループ内の全ノードにメッセージ送信するとき（例えば，バージョンアップなど），グループ鍵(GK)でメッセージの暗号化を行い全ノードに送信する．サーバが各サブグループと通信するときはサブグループ鍵(SGK_i)を使用し，センサノードと 1 対 1 通信するときは各ノードの固有鍵（Ki）を使用する．

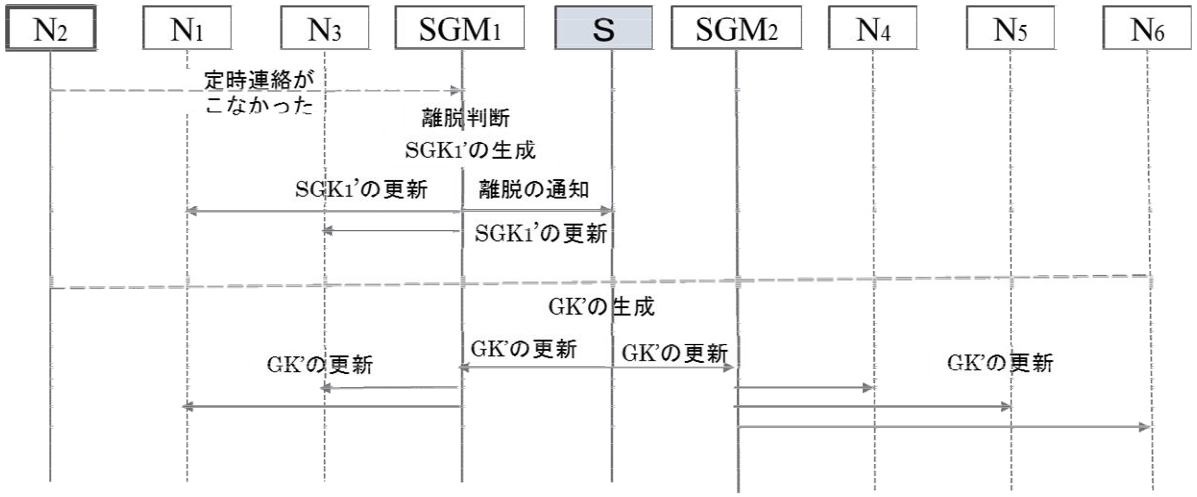

Fig.6 Proposed Group Key Updating Sequence: N_2 leaving

一方，サーバがグループ鍵を更新する場合，新しいグループ鍵を各 SGM ノードのサブグループ鍵で暗号化し，SGM ノードに配布すると，SGM ノードはサブグループ内の各ノードの固有鍵で暗号化して配布する．

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の更新については，以下にそれぞれ述べる．例えば，図 5 でノード N_2 が離脱するときの鍵更新プロトコルを図 6 に示す．

- **センサノードの離脱**

(1) SGM_1 ノードの定時連絡（ビーコン信号）を受信しなかった場合，SGM_1 ノードはノード N_2 を離脱と判断し，新しいサブグループ鍵（SGK_1'）を生成する．

(2) SGM_1 ノードは，新しいサブグループ鍵（SGK_1'）をサブグループ内の各ノードに対し，それぞれの固有鍵で暗号化して配布する．同時に，サーバにノード N_2 が離脱したことを伝えるため，新しいサブグループ鍵をサーバに送信する．

(3) サーバは，新しいグループ鍵（GK'）を生成し，各 SGM ノードに対し，それぞれのサブグループ鍵で暗号化して配布する．

(4) 各 SGM ノードはサブグループに所属する各ノードに自身のサブグループ鍵で暗号化した新しいグループ鍵を送信する．

□

- **センサノードの新規加入**

(1) 加入するノードはビーコン信号を発信し，それを受信した SGM ノードは応答信号を返信する．加入するノードは受信した応答信号の受信時刻と信号強度により，最も近隣に位置する SGM ノードを選択する．

(2) 加入するノードは，(1)で選択した SGM ノードに加入要求を自身の固有鍵で暗号化して送信する．

(3) 加入要求を受け取った SGM ノードは，サーバに新規ノードの加入要求を転送する．

(4) サーバは，加入要求を復号することにより，加入ノードの正当性を判断し，加入するノードの固有鍵を加入先の SGM ノードの固有鍵で暗号化し，SGM ノードに送付する．

(5) SGM ノードは，暗号化されたノードの固有鍵を自身の固有鍵で復号し，加入するノードの固有鍵を取得する．

(6) SGM ノードが SGK を更新する手順は次のように 2 つに分けられる．

(6-i) SGK を更新しない場合（加入）

(1) SGM ノードは，現在使用しているサブグループ鍵をそのノードの固有鍵で暗号化し配布する．

(2) グループ鍵についても同様に送る．

(6-ii) SGK を更新する場合（加入）

(1) 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，それぞれの固有鍵で暗号化して配布する．

(2) SGM ノードは，サーバに新しいサブグループ鍵をサーバとの固有鍵で暗号化して送る．

□

SGM ノードを導入することにより，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，サーバが処理しなければならない処理を低減することが可能となる．

5. 評価

表 1 に，SGM ノードをランダムに配置した場合と k 平均法を用いた際の，各センサノードと自身に最も近い SGM ノードまでの距離の二乗の平均およびその標準偏差を示す．距離の二乗で評価を行った理由として，送信電力は距離の二乗に比例して減衰するためである．

本シミュレーションにおいて，シミュレーションエリアは 100m×100m とし，センサノードはいずれの方式に対し

Table 1 Comparison of SGM distribution methods

センサ ノード数	SGM ノード数	ランダム配置 距離の二乗和平均値	ランダム配置 標準偏差	k 平均法配置 距離の二乗和平均値	k 平均法配置 標準偏差
1,000	10	359.775	345.2511	165.1883	109.2805
	100	30.888	29.18382	14.14284	12.52476
5,000	10	392.8678	362.9496	170.5069	107.9234
	100	36.2246	40.05011	16.51841	12.24052
10,000	10	385.6642	393.4227	169.2803	110.3956
	100	39.7515	48.44475	16.45647	11.11673

シミュレーションの仮想環境は 100x100 平方メートルの正方形地域

てもランダムに配置する. センサノード数を 1000, 5000, 10000 と SGM ノード数を 10 と 100 で行った. 表 1 より, k 平均法を用いた場合,いずれの SGM ノード数の組み合わせにおいても, 約 55%の低減となることがわかるため, SGM 通信に必要な消費電力を低減できる.

次は,グループ鍵更新におけるサーバでの通信回数と各ノードでの鍵管理数について評価する.

従来の LKH 手法は鍵木構造により,グループ鍵を効率的に管理するが,ノードが離脱／加入するとサーバまで遡ってグループ鍵を更新する必要がある. これに対して, 提案手法は SGM ノードがマルチホップ数を減少すると同時に,無駄なグループ鍵更新回数を抑えることもできると言える. さらに, LKH はノード数が多いほど, 鍵が配布しにくくなる. 提案手法は SGM ノードの導入により, サブグループ鍵を即時かつ効率的に更新できる上で, k 平均法により通信回数も軽減できる.

表 2 に, LKH 方式と提案方式の比較を示す. LKH の通信回数は鍵木の深さに依存しているので,グループ鍵更新の通信回数は $d\log_d n$ である. 一方, 提案手法では SGM ノードがグループ鍵の配布を行うので,通信回数は SGM ノード数回である. さらに, グループ鍵更新の通信回数は, SGM ノードが管理する各ノードとの通信回数の (n/m)との和となるため, m+ (n/m) になる. また, 各ノードが管理すべき鍵数は鍵木の深さと等量のグループ鍵,サブグループ鍵および自身の固有鍵を管理するため,鍵木の深さ d と等しい. 一方, 提案手法の各ノードはグループ鍵, 自身が属するサブグループの鍵,自身の固有鍵の 3 つのみを管理すればよい.

これらのことから, k 平均法を用いて SGM ノードを配置することにより,再送処理および通信回数を改善できることが期待される.

6. まとめ

本研究では,安全な M2M 通信システムを実現するための SGM に基づいた分散型グループ鍵管理手法を提案した. SGM ノードは多くの配下のセンサノードと通信する必要があるため,通信距離を短くするように配置される必要がある.そこで k 平均法を用いて SGM ノードの配置位置を決定する方式を提案した. 計算機シミュレーションにより, ランダムに SGM ノードを配置した場合と比較して k 平均法を用いることにより約 55%だけ通信距離を低減することを明らかにしたため,容易にグループ鍵を配送することができ, M2M 通信ネットワークに適したものと考えられる. 今後の課題としては,ネットワークシミュレータを用いて実際に SGM ノードの消費電力がどの程度低減されるかを明らかにする. さらに, 大規模ネットワークにおいて, 鍵更新の通信トラフィックとホップ数等を考慮した SGM ノードと各センサノードの配置について検討する.

Table 2 Comparison of proposed method

	LKH 方式[1]	提案方式
サーバの通信回数	$d\log_d n$	m
SGM の通信回数	-	n/m
グループ鍵更新の通信回数	$d\log_d n$	m+ (n/m)
SGM の管理鍵数	-	2+ (n/m)
ノードの管理鍵数	d	3

n: number of group member, d: number of degree, m: number of SGM

参考文献

[1] 森川博之, 鈴木誠, “M2M が未来を創る”, 電子情報通信学会誌, Vol.96 No.5,pp.292-298, May 2013

[2] 山崎徳和[訳]“M2M 基本技術書”, リックテレコム, (2013)

[3] G.Wu, S.Talwar, K.Johnsson, N.Himayat, and K.D.Johnson, “M2M: From mobile to embedded internet,” IEEE Commun.Mag., vol.49, no.4, pp.36-43, April 2011.

[4] K.Chang, A.Soong, M.Tseng, and Z.Xiang, “Global wireless machine-to- machine standardization,” IEEE Internet Comut., vol.15, no.2,pp.64-69,March/April

2011.
[5] ETSI TS 102 690 V1.1.1, “Machine-to- machine communications(M2M),” Functional architecture, Oct.2011.
[6] TIA TIA-4940.005, “Smart device communications,” Reference architecture, Dec.2011.
[7] Open Mobile Alliance, “OMA device management v1.3,” Dec.2012.
[8] ETSI TS 103 092 v.1.1.1, “OMA DM compatible Management Objects for ETSI M2M,” May 2012.
[9] Perrig A, Szewczyk R, Tygar J.D., Wen V, Culler D.E, “SPINS:Security Protocols for Sensor Networks,” Wireless Network Journal, pp.521-534, 2002.
[10] C.K. Wong, M. Gouda, and S. S. Lam, “Secure group communications using key graphs,” IEEE/ACM Trans. Netw., vol. 8, no.1, pp.16-30, 2000.
[11] 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.
[12] 花谷 嘉一, 上林 達, 大場 義洋“M2M通信システム向けグループ鍵管理技術,” 東芝レビュー, 69(1), pp.14-17, 2014.
[13] 村上大樹, 双紙正和“ワイヤレスセンサネットワークにおけるグループ鍵分配プロトコルの考察,” 第48回コンピュータセキュリティ研究会(CSEC), No.27, pp.1-8, 2007.
[14] 金子 良, 岩村 恵市“センサネットワークに適したグループ鍵配送方式の提案,” 第32回暗号と情報セキュリティシンポジウム誌(SCIS2015), 3B3-3, pp.1-6, 2015.
[15] 陳 致豪, 喜多 義弘, 朴 美娘“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, ” 情報処理学会第77回全国大会(IPSJ2015), 6W-01, pp.1-2, 2015.