データ指向型アーキテクチャに基づく無線センサネットワークプロトコルの開発

研究代表者　　森　慎　太　郎　　福岡大学　工学部　助教

1 はじめに

1-1 背　景

近年，有線ネットワークの研究領域において，インターネットなどで幅広く用いられている IP に基づくホスト指向型ネットワーク(HCN; host-centric network)に代わり，送受信データに着目して設計されたデータ(コンテンツ)指向型ネットワーク(ICN; Information-centric network)に基づくネットワークシステムが検討されている[1]．一方，インターネットに多様かつ多数のモノが接続されるモノのインターネット(IoT; Internet of Things)は，「人と人」をつなぐという従来のコミュニケーションの概念を「モノ」(M2M; machine to machine)へと拡大させた大きなパラダイムシフトであり，新しい無線センサネットワーク(WSN; wireless sensor network)として幅広い分野において利活用が研究されている．例えば，大量のセンサノード(SN; sensor node)を用いたモニタリングを行うユースケースとして，インフラ点検，災害・防災モニタリング，農林水産資源の観測など数多く登場し，効率的に膨大なデータを無線伝送する手法の確立は重要な課題になってくる．一方，技術面を見ると，既存の有線・無線の通信ネットワーク基盤を支える IP (Internet protocol) ネットワークは成熟しているが，将来の新しい情報社会を支える通信インフラを考えたときには十分に対処できるとは考えにくく，新たなアーキテクチャの導入の検討を真剣に考えるべきである．

とくに，数年先の社会では 5G による無線通信サービスが提供され，IoT/M2M に基づく高度なサービスが社会に浸透していると考えられる．すでに現代社会においても，スマートホン等のモバイル端末でインターネットにアクセスするとき，Google，Facebook，Amazon 等の成熟した共通のサービスに人々の興味は偏っており，「エンド・ツー・エンド」から「コンテンツ」にパラダイムシフトしている．従って，将来の無線ネットワークシステムは，既存の IP ネットワークに基づいたネットワーク設計ではなく，次世代インターネットアーキテクチャとして研究されている ICN に基づくアーキテクチャ設計を導入するべきであり，そうなることは必然であると考えられる．文献[2]においても同じ視点に立って，ここ数年の研究成果について調査・報告されている．

1-2 動　機

本研究開発に着想したのは，文献[3]において生体通信に WSN を応用する場合において，ICN に基づく新たなプロトコル設計を開発したことにある．文献[3]においては，設計・評価については新規性が高く有望な研究として評価された反面，有効性・信頼性の面では荒削りの部分も多い点が大きな課題であった．ICN を WSN に導入する場合，ネーミング手法，名前解決手法，ルーチング手法，キャッシング手法，モビリティおよびセキュリティの各事項を検討する必要がある．そして，とくにこれらの要素技術の中でもキャッシング手法は重要な位置づけであると考え，理論的なプロトコル設計をだけではなく，計算機シミュレーションに基づく基礎的な評価を行い，新しい WSN の基盤インフラの構築に必要な基礎的な知見を得られることに期待している．

1-3 目　的

以上の状況を鑑みて，ICN に基づく設計を IoT/M2M の要素技術である WSN に導入することを目的として，効果的なキャッシング手法の提案および評価を行う．具体的には，コンテンツを要求する Subscriber に対して，そのコンテンツを持っている Publisher 間にリンクを構築する．このとき，そのリンク上を中継する SN がコンテンツを保有するオンパスキャッシングと，それ以外のノードが自発的にコンテンツを蓄えるオフパスキャッシングがある．一般に無線通信では電波を用いて通信を行うために，送受信を行う SN の近隣 SN がその通信をオーバヒアリング現象によって得られる固有の特徴を持っている．そこで，本研究では，このオーバヒアリング現象の特徴を有効に利用して，WSN を構成する各 SN がオフパスキャッシングを行う手法を研究開発することを目的とする．また，本研究は，新たに複雑な機構を導入することなく，オーバヘッドなく

オフパスキャッシングを実現できる点に特徴がある．

また，効率的にキャッシングデータを SN に取り込むために，その無線通信信号処理に関して逐次干渉抑圧除去(SIC; successive interference cancellation)[4]を導入する．無線通信の分野において，SIC はセルラネットワークの無線信号処理手法の要素技術として開発されている(高速モバイル通信の新しいシステム向けには IC チップとして実装・実用化されている[5])．基本コンセプトは，受信信号を復元する場合に，その中で最も信号強度が強い信号から順番に復号する．もし復号に成功するとき，その復号データを再び符号化したのちに受信信号から引き算する．その処理をくりかえして行うことにより，復元対象信号の最大の干渉源を順番に取り除けるために復号成功確率を高めることができる．一方，SIC の考え方はネットワークの研究分野においては考慮されておらず，本研究が SIC を導入する際の新規性として主張している．

さらに，本研究開発の進捗課程において，テストベッドに基づく評価に先立ち，センシングデータを安全に無線センサネットワーク内で共有するためのメカニズムを考える必要性がある点に気付いている．そこで，安全にセンシングデータを共有するメカニズムとして，ビットコインの核となる要素技術であるブロックチェーン[6][7]を開発システムに導入して改良を施した．とくに，従前の IP ネットワーク等のホスト指向型ネットワークとは異なる解決アプローチにて分散情報共有手法を実現する必要があり，ブロックチェーンは，ICN に基づく WSN に対して親和性が高いと考えている．

1-4 本研究開発の貢献と本報告書の構成

本研究開発の貢献，本報告書の構成，および発表資料の関係は次の通りである．

- ICN に基づく WSN の効率的なキャッシング手法の開発(第 2 章)
  - 本研究の核となる提案手法のコンセプトの提案(発表資料，2017 年 4 月)
  - 高効率キャッシング手法のプロトコル設計の提案(発表資料，2017 年 7 月)
  - 本研究開発が必要となるユースケースの提示および有効性評価(発表資料，2017 年 9 月)
- クロスレイヤ設計に基づく最適設計の開発と計算機シミュレーション評価(第 3 章)
  - 高効率キャッシング手法の最適化設計の提案とシミュレーション評価(発表資料，2017 年 12 月)
- ブロックチェーンを用いた安全なキャッシング手法の開発と基礎評価(第 4 章)
  - キャッシング手法を安全に行うためのコンセプトの提案と予備実験報告(発表資料,2018 年 3 月)
  - 安全キャッシング手法のプロトコル設計の提案とシミュレーション評価(発表資料,2018 年 5 月)

2 ICN に基づく WSN における効率的なキャッシング手法の開発

2-1 関連研究

有線ネットワークの研究分野において，ICN は次世代インターネットアーキテクチャとして検討されているが，無線ネットワークにおいても導入されつつある[1][2]．例えば，文献[8][9]においては，セルラネットワークにおいて，基地局のゲートウェイやルータに高頻度にアクセスされるデータのキャッシュを保存する手法が提案されている．すなわち，同一データを一括配信することができるためにコアネットワークのトラヒックの削減を実現することができる．このとき，ICN はコンテンツ配信ネットワーク(CDN; content delivery network)と類似しているが，CDN はネットワークのサーバ内にコンテンツをキャッシュするのに対して，ICN は末端ノードのキャッシュに幅広くコンテンツを蓄積してゆく点が異なる．また，文献[10]ではデバイス間通信に基づくセルラネットワークにおいて，仮想化と ICN メカニズムの導入している．

他方，文献[11]において数多くの ICN に関する研究の分析により，キャッシング手法をオンパスキャッシングとオフパスキャッシングの 2 種類に分類している．すなわち，オンパスキャッシングはコンテンツが転送される際の中継ノードにキャッシュするのに対し，オフパスキャッシングは経路外のノード同士においても積極的にコンテンツをコピーしてゆくことである．そして，典型的な ICN フレームワークにおいてキャッシング手法を概観すると，DONA(data-oriented network architecture)[12]と NDN(named data networking)[13]においては，オンパスキャッシングが標準で具備されている．両者を拡張するために，文献[14]では 4 種類のオフパスキャッシング手法を導入している．また，文献[15]においてユーザの協調キャッシング手法，文献[16]においてキャッシュするデータの選択手法，文献[17]においてサービス品質(QoS; quality of service)を保証した映像ストリーミング配信のための動的キャッシング手法を提案している．

2-2 ネットワークモデル

ICN に基づく WSN では，コンテンツデータは SN に蓄積される．また，CDN と同様の方針に基づき，ICN においては，オリジナルデータとコピーデータを区別しない．従って，図 1 に示すように，提案手法では，それらのセンシングデータはコンテンツデータとして SN に具備されたキャッシュメモリに保存してゆく．任意のセンシングデータの取得手順に関して，一般的な WSN では，SN はインターネットを介してクラウドサーバに接続され，かつセンシングデータはクラウドサーバに一元的に管理されているため，センシングデータの取得を希望するユーザはクラウドサーバにアクセスすればよい．一方，提案手法では，WSN 内に蓄積されているコンテンツデータの中から，当該センシングデータを探索する必要があるため，ユーザは WSN に属するゲートウェイノードにアクセスする．そして，そのゲートウェイノードは Subscriber としてセンシングデータ取得リクエストを WSN 内にブロードキャストして，ユーザに代わって探索を行うための手続きを開始する．また，ユーザが所望するセンシングデータを保有するセンサノードは Publisher として，先のリクエストに対するレスポンスとして当該センシングデータを伝送することで，センシングデータ取得に関するタスクが完了する．

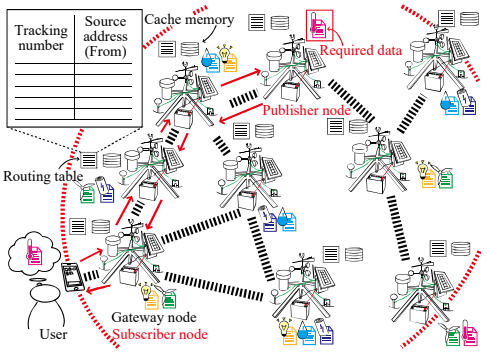

図 1 ネットワークモデル

Publisher から Subscriber に向けてセンシングデータをルーチングするしくみとしては，提案手法ではルーチングテーブルを各センサノードに具備しており，リクエストパケットの追跡情報をフラッディングされる際に順次記録していくことにより実現可能である．また，リクエストパケットのヘッダにおいて追跡情報を挿入することにより，各リクエストを区別でき，かつ各 SN に対してユニークなアドレスを付与することにより，次に送信するべき（受信されるべき）相手方を識別することが可能になると想定している．

2-3 オーバヒアリング現象に基づくキャッシング手法

図 2 に示すように，キャッシング手法として，提案手法はオンパスキャッシングおよびオフパスキャッシングを用いる．オンパスキャッシングに関しては，提案手法は他研究・従来手法と同様に，レスポンス処理において Publisher から Subscriber に対してセンシングデータが伝送される際に，リレーノードと呼ぶルーチング経路上の SN が具備するキャッシュメモリにリレーノード自身が転送するセンシングデータを蓄積する．一方，オフパスキャッシングに関しては，オーバヒアリング現象に基づき，リレーノードの通信可能カバレッジエリアに在圏する SN が転送されるセンシングデータを聴守し，そのオーバヒアリングされたセンシングデータを蓄積する．

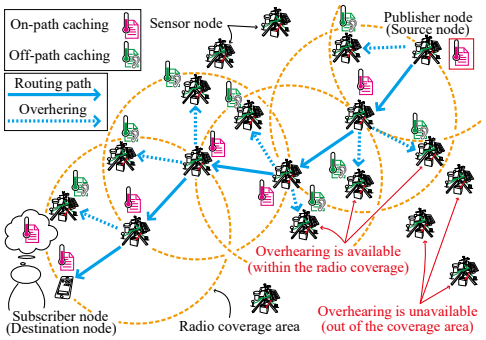

図 2 オーバヒアリング現象に基づく
提案キャッシング手法の概観

提案手法は，オーバヒアリング現象を用いることにより，リレーノードとオーバヒアリングする隣接センサノード間において，余計な無線通信を相互に行う必要はない．一方，オーバヒアリング現象に基づき聴守を行う際には，無線受信信号処理に対する消費電力の増大，およびキャッシュメモリ容量の積み増しが必要である．これらの点に関して，たとえ SN に具備されたマイクロコントローラ等の演算処理にかかる消費電力が増大したとしても，無線通信に必要な消費電力と比べて小さいため，提案手法を導入することによる無線通信回数の削減に従う SN の総消費電力を改善することが可能である．また，キャッシュメモリの追増コストに関しても，提案手法を導入することによる無線通信回数の削減に基づく電波の周波数資源の節約は，その対価を支払ったとしても十分な意義があると考える．ただし，SN に具備されるキャッシュメモリの容量は有限であるため，提案手法を導入する環境に応じて，キャッシュメモリに蓄積されたセンシングデータの破棄ルールを定める必要がある．この点に関しては本稿の検討対象外であるため，詳細なルールの決定方法については今後の課題である．

2-4 SIC に基づくキャッシング手法

先述した通り，SN は隣接 SN の信号をオーバヒアリング現象に基づき受信することができ，2-3 で述べた手法に基づき肯定的に利用することができる反面，データ受信確率を低減させる干渉の原因となる諸刃の剣になりうる．そこで，その受信された情報に基づきオフパスキャッシングにおける他の SN から受ける干渉の低減を SIC 技術の導入により実現する．図 3 に示すように，i 番目の SN からj 番目の SN に伝送される信号強度を$P_{i,j}$，j 番目のノードがオーバヒアリング現象に基づき受信可能な SN の集合を$\mathcal{M}_j$と定義する．$P_{i,j}$を所望信号とするとき，一般に受信側で所望信号が復号可能な条件は式(1)で表される．

$$\mathcal{H}: \frac{P_{i,j}}{\sum_{k\in\mathcal{M}_j}^{k\neq i} P_{k,j} + \sigma^2} \geq \Lambda \qquad (1)$$

ただし，Λを受信可能な信号強度のスレショルド値，σ^2を周辺環境雑音と定義する．

また，図 3 において，yをj 番目の SN における受信信号と定義するとき，式(2)で表すことができる．

$$y = \sum_{m=1}^{M_j} P_{m,j} \qquad (2)$$

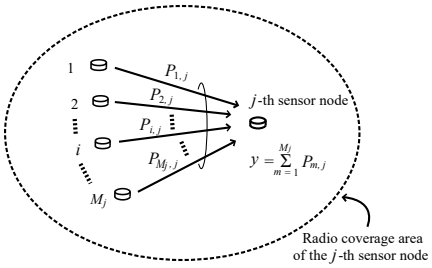

図 3 信号の受信モデル

本研究おいて開発した復号器の信号処理手順のブロック図を図 4 に示す．初回の復号処理では，式(1)に基づき受信信号の中で最も強力な受信強度の信号を復号する．正しく復号することができるとき，再度，復元した信号を符号化して，受信信号に対して引き算に相当する信号処理を施す．同様の手続きに従い 2 番目に強力な信号に対して準用し，復号可能な信号がなくなるまで繰り返し処理する．すなわち，正しく復号できた信号数をK，正しく復号できた信号を$\hat{y}$，その信号に基づき再符号化した信号を$\bar{y}$と定義するとき，提案手法の復号手続きは式(3)で表せる．また，式(1)から式(3)において，$\bar{y}$，P の信号強度は降順になっている．

$$\begin{aligned}
&\text{Step 1:} && \frac{\hat{y}_1}{y} = \frac{P_{1,j}}{\sum_{m=1}^{M_j-1} P_{m,j} + \sigma^2} \geq \Lambda \\
&\text{Step 2:} && \frac{\hat{y}_2}{y-\bar{y}_1} = \frac{P_{2,j}}{\sum_{m=1}^{M_j-2} P_{m,j} + \sigma^2} \geq \Lambda \qquad (3)\\
&\quad\vdots && \quad\vdots \\
&\text{Step } K\text{:} && \frac{\hat{y}_K}{y-\sum_{k=1}^{K-1}\bar{y}_k} = \frac{P_{K,j}}{\sum_{m=1}^{M_j-K} P_{m,j} + \sigma^2} \geq \Lambda
\end{aligned}$$

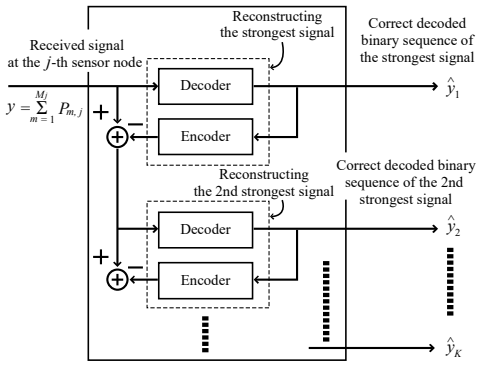

図 4 SIC に基づく復号器の信号処理手順

3 クロスレイヤ設計に基づく信号処理の最適化

3-1 開発システムのプロトコルスタック構成

ICN に基づく WSN システムに対し，第 2 章で述べたオーバヒアリング現象および SIC 技術に基づくキャッシング手法を導入する場合，そのプロトコル設計は柔軟かつ統合的に取り扱うべきである．プロトコルスタックの最適化については，クロスレイヤ設計に基づく設計手法が挙げられる[18][19]．クロスレイヤ設計は，従前のレイヤ設計(OSI 基本参照モデル等)に対し，レイヤ間で情報共有を図ることにより柔軟なレイヤ設計を実現する手法である．とくに，文献[19]に定義される隣接レイヤ間の結合に基づく設計コンセプトを用いて，図 5 に示すようなプロトコルスタックを設計する．具体的には，従前 HCN における，TCP/UDP，IP，MAC レイヤを ICN レイヤとして再定義を行う．そして，ICN レイヤを C-plane と U-plane と呼ぶ制御機能とデータ伝送機能の 2 種類に分類して各機能を実現させる．

3-2 クロスレイヤ設計に基づく信号処理手順

提案する ICN に基づく WSN に対して，クロスレイヤ設計を用いた SN の信号処理手順を図 6 に示す．図 6 に示すように，観測エリアから取得したセンシングデータは自身のキャッシュメモリに蓄積してゆく．キャッシュメモリには自身のセンシングデータに加えて，オーバヒアリングした他 SN のセンシングデータも可能な限り保存してゆく．また，センシングデータの送受信については，TX/RX RF(radio frequency)モジュールを用いて行う．一方，マイクロコントローラはセンシングデータとルーチングテーブルの管理だけでなく，キャッシュメモリと RF モジュールの制御も行う．このとき，その制御に必要な信号伝送は，文献[19]における上位レイヤから下位レイヤに対するサイド情報に基づくクロスレイヤ設計に従って設計している．

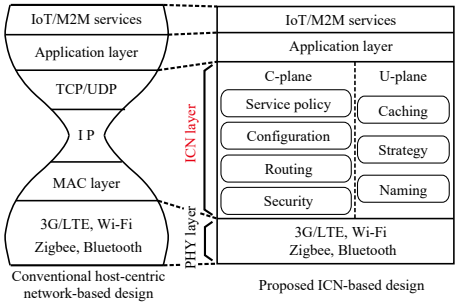

図 5 開発システムのプロトコルスタック

図 6 の RF モジュールおよび無線通信路のエミュレータにおける詳細な信号処理手順を図 7 に示す．図 7a)に示すように，送信パケットに対して誤り検出のための巡回冗長検査(CRC; cyclic redundancy check)符号化を施し，ビットごとに二位相偏移変調(BPSK; binary phase shift keying)方式に基づく変調処理を行う．一方，図 7c)に示すように，受信側において軟判定復号を行いそのレプリカを用いて SIC 技術を適用する．図 7c)における復号器と符号器は図 4 に示すブロックと同じもので，第 2-4 節において述べた手順に従ってパケットの復元を行い，信号の減算処理等を行う．

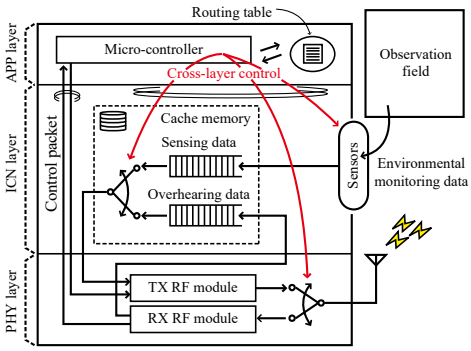

図 6 開発センサノードの信号処理手順

3-3 シミュレーションモデル（無線伝搬モデル）

図 7b)に示すように，パケット誤り率は受信信号強度インジケータ(RSSI; received signal strength indication)に基づき計算する．一般的に，リンクバジェットは，式(4)より表現することができる．ただし，P_{TX} および P_{RX} は送受信器の電力，G_{TX} および G_{RX} は送受信器に具備されているアンテナ利得，L_{TX} および L_{RX} は送受信器を構成する電子回路等における減衰と定義する．いずれのパラメタについても，用いる RF モジュールに依存して決定される．

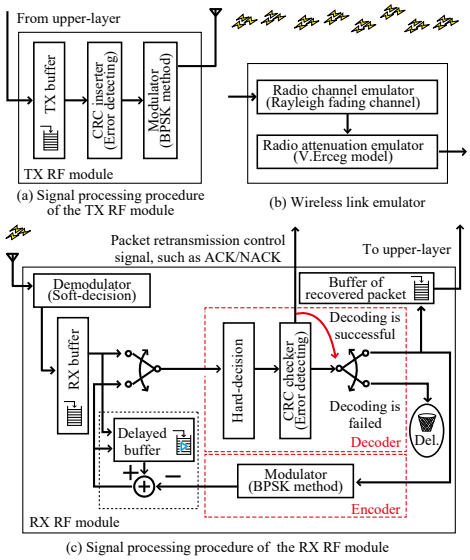

図 7 送受信 RF モジュールの信号処理手順

$$P_{\mathrm{RX}} = P_{\mathrm{TX}} - L_{\mathrm{TX}} + G_{\mathrm{TX}} - L_{\mathrm{P}} + G_{\mathrm{RX}} - L_{\mathrm{RX}} \ (\mathrm{dB}) \qquad (4)$$

また，式(4)において，L_{P} は無線通信路の伝搬減衰であり，本研究開発の評価において文献[18]に示すモデルを用いる．すなわち，L_{P} は，式(5)に従い計算する．ただし，d は送受信ノード間の距離，λ は無線通信に用いる搬送波の波長，h_0 はアンテナの高さ，d_0 は文献[20]に示されている固定値である．また，a，b，c の各パラメタは，無線伝搬環境に依存して決定される固定値であり，文献[20]において示されている．

$$L_{\mathrm{P}} = \alpha + 10 \cdot \beta \cdot \log_{10}\,(d/d_0)$$
$$\alpha = 20 \log_{10}\,(4\pi d_0/\lambda) \qquad (5)$$
$$\beta = a - bh_0 + c/h_0$$

他方，計算機シミュレーションに必要なパケット誤り率は信号対雑音比(SNR; signal-to-noise ratio)とビット誤り率に基づき算出する．具体的には，受信側 SN の信号電力と SNR γ は式(6)の関係がある．

$$\gamma = P_{\mathrm{RX}} / K_{\mathrm{B}} \tau_{\mathrm{o}} \qquad (6)$$

ただし，K_{B}(=4.0×10^{-21} W/Hz)はボルツマン定数，τ_{o}はハードウェア装置のシステム温度である．また，レイリーフェージング環境における BPSK 方式のビット誤り率 p_{b} は式(7)から計算できる[21]．

$$p_{\mathrm{b}} = \frac{1}{2} \cdot \left(1 - \sqrt{\gamma/(\gamma+1)} \right) \qquad (7)$$

従って，パケット長を ℓ と定義するとき，式(7)よりパケット誤り率 p_{e} は式(8)から計算できる．

$$p_{\mathrm{e}} = 1 - (1 - p_{\mathrm{b}})^{\ell} \qquad (8)$$

3-4 計算機シミュレーション

図 6 および図 7 における RF モジュール，無線伝搬モデル，キャッシュメモリに対して，C++言語を用いて計算機シミュレータを実装した．表 1 にシミュレーション諸元を示す．シミュレーションシナリオとして，センサノードは観測フィールドに対してランダムに配備(センサノードの位置は一様分布に従う乱数に基づき決定)した．そのうえで，Publisher と Subscriber の組み合わせをランダムに決定し，両ノード間のルーチングは転送距離が最小になるパスを選択した．開発したシミュレータにおいては，ルーチング経路の最小パスを決定するために，Dijkstra アルゴリズム[22]に基づき算出した．また，RF デバイスの固定パラメタ設定については，WSN の無線伝送に幅広く用いられている XBee モジュール[23]に基づき決定した．

表 1 シミュレーション諸元

試行回数		10,000
観測エリア		10 km^2
パケット長		ℓ = 1,000 bit
Publisher/Subscriber 数		100
SN	送信電力	R_{TX} = 0 dBm (1 mW)
	アンテナ利得	$G_{\mathrm{TX}} = G_{\mathrm{RX}}$ = 0 dBi
	装置損失	$L_{\mathrm{TX}} = L_{\mathrm{RX}}$ = 0 dB
	アンテナ高	h_0 = 0.5 m
	搬送波周波数	2.4 GHz (λ = 0.125 m)
	変調方式	BPSK
雑音電力 (システム温度)		N_0 = −171.94 dBm (τ_{o} = 1,600 K)
固定パラメタ		d_0 = 100, a = 3.6, b = 0.005, c = 20
チャネルモデル		レイリーフェージング
所望パケット誤り率		p_{e} = 1% (Req. p_{b} = 10^{-5})

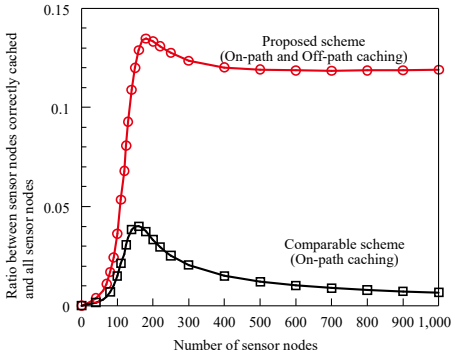

図 8 キャッシング成功ノードの割合
対センサノード数

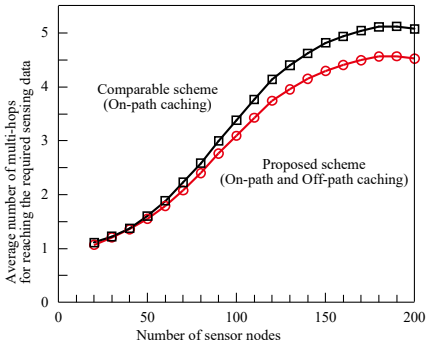

図 9 平均マルチホップ数
対センサノード数

図 8 に WSN を構成する全 SN に対するキャッシングに成功した SN の割合 $\overline{\rho}$ の結果を示す．SN 数が増大するにつれてオーバヒアリング現象の効果により $\overline{\rho}$ が増大するが，SN 数が 180 をピークとして $\overline{\rho}$ は減少した．また，提案キャッシングメカニズムを用いない手法と

比較して，SN 数が 100，180，600，1,000 台のとき，各々，1.42 倍，2.61 倍，8.85 倍，17.0 倍の改善が得られた．

図 9 に Publisher から Subscriber に対して正しく要求パケットが伝送された場合において，その平均マルチホップ数の結果を示す．SN 数が多くなるにつれて，パケットを中継するリレーノードになり得る SN も増大するため，平均マルチホップ数は増大する．また，ICN に基づく WSN において開発手法は比較手法と比べてキャッシングされたデータも多くなるため(図 8)，要求パケットにヒットする確率も高くなるので，平均マルチホップ数は改善した．具体的には，SN 数が 50，100，150，200 の場合，各々，3.35%，8.51%，10.8%，10.9%の改善が得られた．

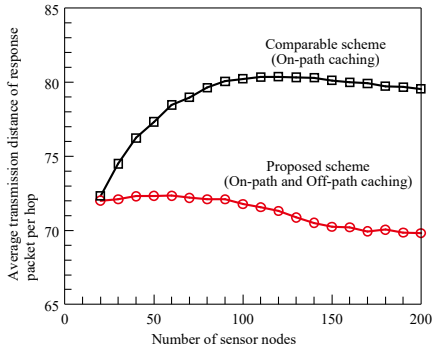

図 10 平均伝送距離対センサノード数

図 10 に Publisher と Subscriber 間の伝送リンクの平均転送距離対 SN 数の結果を示す．SN 数が 100 未満の領域においては，十分なキャッシュがなされないため，提案メカニズムを導入する効果がみられなかったが，それ以外の領域においては特性改善がみられた．具体的には，SN 数が 50，100，150，200 の場合，各々，6.46%，10.5%，12.3%，12.2%の改善が得られた．

4 ブロックチェーンを用いたセキュアキャッシング手法の開発

4-1 関連研究

ICN におけるキャッシングに対する安全にデータを取り扱う手法として，文献[23]は NDN におけるセキュリティアタック保護フレームワークを考案し，文献[24]において最適化を図っている．また，文献[25]では NDN におけるキャッシュ汚染を目的とした攻撃を防ぐ手法の考案，文献[26]および文献[27]において，NDN に対する攻撃シナリオの分析とモデルを構築している．一方，文献[28]および文献[29]において，ホームネットワークシステムにおける個人情報に対して安全に取り扱うための手法を考案している．また，文献[30]において IoT 分野におけるブロックチェーンを考慮した研究動向を概観している．

4-2 提案セキュアキャッシングシステムの概観

ブロックチェーン技術を導入する場合，認証のためのマイニング処理に対して多くの計算量が必要である．そのため WSN を構成する SN のようにハードウェア資源が乏しいデバイスに対しては，ブロックチェーンをそのまま適用させることは不可能である．そこで，図 11 に示すように，ICN-plane と WSN-plane と呼ぶ 2 階層モデルに基づき，SN，CH (cluster head)，Coordinator をハードウェア制限に基づき分類した．

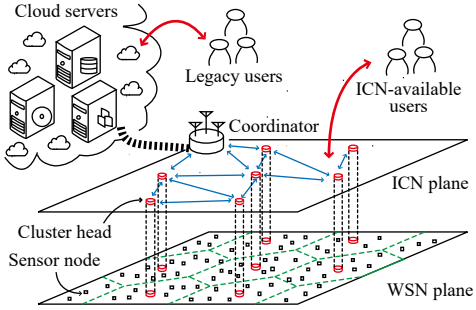

図 11 セキュア ICN-WSN の概観

本研究で想定するネットワーク構成について，データの流れとして，SN はいくつかのクラスタにグループ分けを行い，各々のクラスタに対して CH を設定する．CH は自身が支配するクラスタに属する SN から集めたセンシングデータをひとまとめにして，coordinator を介してクラウドに集約させる．他方，ICN-plane を構成する CH と coordinator は，ICN に基づく情報提供も行う．ここで，第 2 章における SN はハードウェア資源が十分にある場合を想定していたが，実際にはそのような環境は稀である．すなわち，第 2 章で定義する SN を第 4 章では CH と SN にハードウェア資源の制限の有無に従って分類して開発システムの適用範囲拡大を図っている．

4-3 セキュアなセンシングデータの収集手法

センシングデータ収集に先立ち，公開鍵暗号アルゴリズム $\Pi(\mathcal{G},\mathcal{E},\mathcal{D})$ に基づき CH は公開鍵と秘密鍵を生成する．$\Pi(\cdot)$ を構成する $\mathcal{G}(\cdot)$，$\mathcal{E}(\cdot)$，$\mathcal{D}(\cdot)$ は，各々，鍵生成関数，符号化関数，復号関数である．M 台の

CH の集合 $\mathbb{L}=\{L_1, L_2, \cdots, L_M\}$，および i 番目のクラスタに属する N_i 台の SN の集合 $\mathbb{S}=\{S_{i,1}, S_{i,2}, \cdots, S_{i,Ni}\}$ を定義する．このとき，i 番目のクラスタに割り当てられた CH L_i は，i 番目のクラスタに属する j 番目の SN $S_{i,j}$ に対し，1 組の公開鍵・秘密鍵を式(9)に基づき生成する．ただし，演算子 $\oplus$ は任意のビットごとの融合演算子である．また，式(9)に基づき生成した秘密鍵は CH と SN で共有され，公開鍵は CH に保存される．

$$\left(\overline{\mathcal{PK}}_{i,j}, \overline{\mathcal{SK}}_{i,j}\right) = \mathcal{G}\left(L_i \oplus S_{i,j}\right) \tag{9}$$

同様の手続きにて，CH と coordinator の間においても公開鍵・秘密鍵の組をやりとりする．すなわち，coordinator は L_i と式(10)に基づき公開鍵・秘密鍵を生成する．

$$\left(\widehat{\mathcal{PK}}_i, \widehat{\mathcal{SK}}_i\right) = \mathcal{G}\left(L_i\right) \tag{10}$$

図 12 のステージ①において，SN $S_{i,j}$ はセンシングデータ $D_{i,j}$ を生成して，式(11)に基づき電子署名を付与する．

$$\langle D_{i,j} \mid \overline{\mathcal{SK}}_{i,j} \rangle = \mathcal{E}\left(D_{i,j}, \overline{\mathcal{SK}}_{i,j}\right) \tag{11}$$

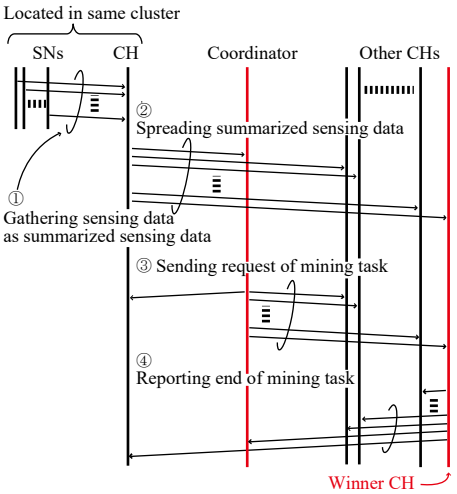

図 12 センシングデータの収集手順

電子署名が付与されたセンシングデータは，自身が属するクラスタに割り当てられた CH に無線伝送する．一方， SN から集めた SN に対して公開鍵を用いて，式(11)に基づき認証を行う．すなわち，式(11)に基づく評価の結果，CH は受信したセンシングデータに対して，生成した SN が正しいかという点，および伝送途中に改ざんされていない点を知ることができる．ただし，式(12)において，$\widehat{D}_{i,j}$ は $D_{i,j}$ に対して正当に復号されたセンシングデータと定義する．

$$\widehat{D}_{i,j} = \mathcal{D}\left(\langle D_{i,j} \mid \overline{\mathcal{SK}}_{i,j} \rangle, \overline{\mathcal{PK}}_{i,j}\right) \tag{12}$$

復元されたセンシングデータは CH のバッファメモリに蓄積され，K 個のセンシングデータを集約センシングデータ(summarized sensing data)としてひとまとめにする．集約センシングデータは，第 4-4 節において述べる提案ブロックチェーンが取り扱うデータ部分(transaction)に相当する．そのために，集約センシングデータは図 12 のステージ②において ICN-plane を構成するノードに対してブロードキャストする．式(11)および式(12)と同様の手続きにて，集約センシングデータに対しても電子署名を付与することにより，配布されるデータの正当性の確認手段を担保している．

4-4 ブロックチェーンに基づくキャッシングデータの管理手法

図 13 に開発システムのブロックチェーンにおいて，各々のブロックは，前ブロックのハッシュ値 $h_{n-1}|_\kappa$，集約センシングデータ D_n，ナンス I_n，現ブロックのハッシュ値 $h_n|_\kappa$ から構成される．集約センシングデータをブロックチェーンに加えるためには，式(13)に基づくハッシュ値の計算に基づくマイニングを行う．そのために，図 12 のステージ③において，coordinator は CH に対してマイニング処理の依頼を出す．

$$h_n|_\kappa = \mathcal{H}(h_{n-1}|_\kappa \oplus D_n \oplus I_n) \tag{13}$$

マイニング処理は，I_n をランダムに変更して式(13)に基づき計算してゆくとき，$h_n|_\kappa$ に対し 0 ビットが κ 個並ぶ

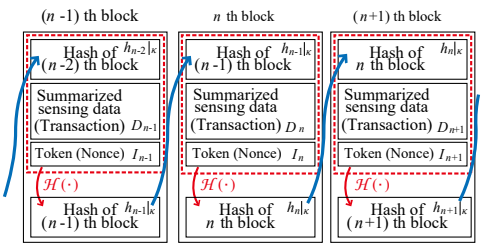

図 13 開発システムのブロックチェーン

条件を満たすハッシュ値を可能な限り速く見つけることである．このとき，ハッシュ関数 $\mathcal{H}(\cdot)$ と κ の設定により計算の難易度を柔軟に変更することが可能であり，適用する WSN に応じたパラメタを決定する必要がある．具体的には，第 4-5 節において実機による試作機を用いて数値例を示す．また，ブロックチェーンに基づくデータの強固性については，ハッシュ関数の逆関数を用いた計算は計算機システムの特徴より困難であるため担保されている．また，マイニングに成功した CH は，図 12 のステージ④に示す報告メッセージをブロードキャストして，他の CH や coordinator はブロックチェーンに新規ブロックを追加する．

4-5 ハッシュ関数のパラメタの数値例

式(13)におけるパラメタ κ の設定値を概算するために，Raspberry Pi 3 (Raspbian kernel ver. 4.9)[31]を用いて実測した．ハッシュ関数は MD5 (message digest algorithm 5)[32]と SHA-1 (first-generation secured hash algorithm)[33]を対象として，C++言語を用いてシミュレータを実装した．ハッシュ関数の実装は，CLX C++ library[34]，処理時間の計測には C++標準ライブラリ(std::chorono)を利用し，g++ compiler ver. 6.3.0[35]を用いてコンパイルした．図 14 に，パラメタ κ に対し 100 回の試行に対する平均処理時間を示す．実験結果より，ブロック長を 100 kbyte，500 kbyte，1 Mbyte に設定するとき，マイニング時間を 1 分または 10 分を想定するとき，表 2 に従い κ を決定すれば良いことが分かった．

4-6 開発システムの動作条件

集約センシングデータが示すポアソン分布に従い生成されるとき，その平均値 $\bar{\lambda}$ は式(14)に基づき計算できる．

$$\bar{\lambda} = v\bar{N}M/K \qquad (14)$$

ただし，M をクラスタ数，K を集約されたセンシングデータ数，$\bar{N}$ を 1 クラスタあたりの平均 SN 数，v を単位時間あたりに生成される SN 1 台あたりのセンシングデータ数と定義する．一方，集約センシングデータがマイニングによってポアソン分布に従い認証されるとき，その平均値 $\bar{\mu}$ は式(15)に基づき計算できる．

$$\bar{\mu} = 1/\varepsilon\overline{T_{\text{mining}}} \qquad (15)$$

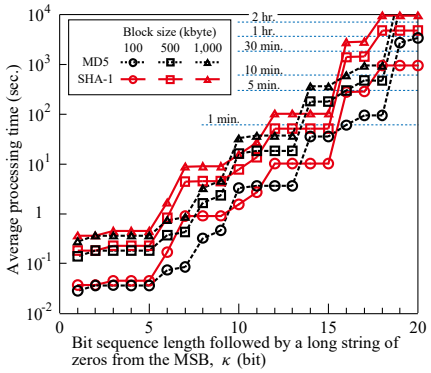

図 14 マイニング時間と κ の関係

ブロックチェーンの仕組み上，あるブロックが認証されたとしても，そのあといくつかのブロックがつながれなければ信用されない．その後続して接続されるブロック数を ε，1 回あたりの認証時間を T_{mining} と定義する．例えば，ビットコイン[6]においては，ε は 6，T_{mining} は 10 分程度に設定されている．

このとき，式(16)の条件を満たすとき，提案システムは動作する．

$$\rho = \bar{\lambda}/\bar{\mu} \leq 1 \qquad (16)$$

表 2 κ の設定値の一例

ﾊﾟｹｯﾄ長 (kbyte)	MD5		SHA-1	
	1 分	10 分	1 分	10 分
100	14	17	12	16
500	13	17	12	12
1,000	10	14	11	12

4-7 計算機シミュレーション

第 4-6 節に示した確率統計モデルに対して，LPWA (low-power wide area) network に基づく WSN[36][37]に開発システムを導入した場合において，センシングデータの取得に係る応答時間に対して，計算機シミュレーションを用いて評価した．表 3 にシミュレーション諸元を示す．とくに，無線通信路のエミュレーションについては，第 3-3 節と同様のモデルを用いて計算している．

図 15 に，第 4-6 節に基づき，センサノード数に対して，単位時間あたりに生成される集約センシングデータ数 $\bar{\lambda}$ の計算結果を示す．センサノード数が 75,000 未満の場合，式(14)におけるv，M，K は定数であるため $\bar{\lambda}$ は単調に増大したが，75,000 以上の場合 MAC プロトコルが pure ALOHA 方式を採用したことによりコリジョンのために特性が劣化した．すなわち，SN 数が 88.4 のとき，$\bar{\lambda}$ は最大値をとった．

式(16)の等号成立条件に基づき，$\bar{\lambda}$ が 88.4 の場合，所望 $\bar{\mu}$ は 88.4 になる．そのため，式(15)において，認証時間の上限は 1 ブロックあたり 40.7 秒になる．従って，図 14 に基づき，MD5 アルゴリズムおよび SHA-1 アルゴリズムを使用した場合における κ は，各々，14 および 15 に決定することができる．

開発システムの有効性を評価するために，センシングデータを要求してから提供されるまでの応答時間をベンチマークとして算出した．図 16 にキャッシュメモリに所望センシングデータが保存されていているセンサノード数に対する全体のセンサノード数の割合，すなわちキャッシュヒット確率 η に対する応答時間の結果を示す．応答時間は 10,000 試行の平均値である．開発システムが最良の条件下で働くとき(すなわち，η = 1 のとき)，すべてのセンサノードがすべてのキャッシングデータを保有するため，Subscriber と Publisher は一致するため，応答時間は 0 秒になった．一方，開発システムが最悪の条件下で働くとき(すなわち，η = 0 のとき)，平均応答時間は 176 秒になった．このとき，開発システムが最も悪条件下になるというのは提案キャッシング手法の効果がなく用いない条件と同値である点を補足する．従って，η が 0.2，0.5，0.7 のとき，先の条件の場合と比較して，36.1%，75.1%，95.9%の改善を得た．

表 3 シミュレーション諸元

観測エリア		400 km^2
パケット長		100 kbyte
SN	ノード数	1,000–100,000
	送信間隔	1,200 秒
	送信電力	20 mW
	アンテナ利得	0 dBi
CH	ノード数	25
	アンテナ高	50 m
	アンテナ利得	2.53 dBi
MAC レイヤ	プロトコル	pure ALOHA
	チャネル数	15
	送信時間	4 秒
	最大再送回数	3
	最大バックオフタイム	30 秒
PHY レイヤ	変調方式	BPSK
	誤り訂正符号	なし
	搬送波周波数	920MHz
	チャネルモデル	レイリーフェージング

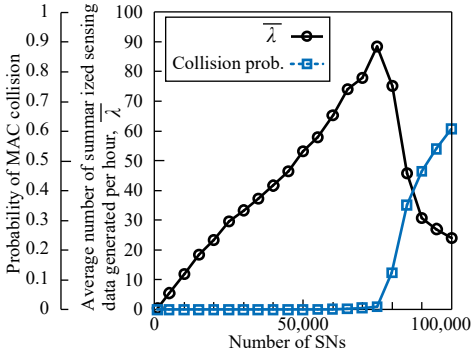

図 15 集約センシングデータ生成数，コリジョン発生確率対センサノード数

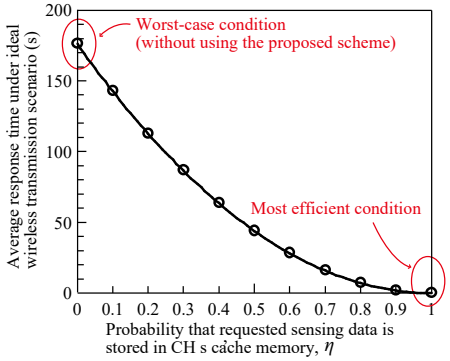

図 16 集約センシングデータ生成数，コリジョン発生確率対センサノード数

5 おわりに

本研究開発では，ICN に基づく WSN に導入することを目的として，効果的なキャッシング手法の提案および評価を行った．具体的には，オーバヒアリング現象に基づくオフパスキャッシングに対し，SIC 技術を併用する手法を開発した．その信号処理手順に関して，クロスレイヤ設計に基づく最適化を試みた．また，計算機シミュレーション評価の結果，開発システムの有効性を示した．

一方，開発システムハードウェア装置に基づく実機を用いた現実的な環境での評価に先立ち，キャッシングデータをセキュアに取り扱う手法の提案および評価を行った．具体的には，ブロックチェーンに基づく分散データベースに基づきキャッシングデータの管理手法を開発した．また，テストベッドを試作してパラメタ設定の数値例，および計算機シミュレーションに基づく開発システムの有効性を示した．本研究開発の目的は達成されたが，開発システムの実践的なテストベット開発と評価が重要な今後の課題であると考える．

【参考文献】

[1] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 26–36, July 2012.

[2] M. Amadeo, C. Campolo, J. Quevedo, D. Corujo, A. Molinaro, A. Iera, R. L. Aguiar, and A. V. Vasilakos, "Information-centric networking for the Internet of Things: Challenges and opportunities," *IEEE Network*, vol. 30, no. 2, pp. 92–100, Mar. 2016.

[3] 森慎太郎, 生越重章, "データ指向型無線センサネットワークにおける生体情報収集手法," *電子情報通信学会技術報告 IN 研究会*, vol. 115, no. 484, pp. 119–124, Miyazaki, Japan, Mar. 2016.

[4] S. Sen, N. Santhapuri, R. R. Choudhury, and S. Nelakuditi, "Successive interference cancellation: A back-of-the-envelope perspective," *Proc. ACM Annual Conf. Special Interest Group on Data Commun. (SIGCOM'10) WS Hot Topics in Networks*, pp. 1–6, New Delhi, India, Oct. 2010.

[5] S. Sambhwani, W. Zhang, and W. Zeng, "Uplink interference cancelation in HSPA: Principles and practice," *QUALCOMM Inc. White Paper*, 28 pages, San Diego, CA, USA, 2009.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Tech. Rep.*, 2008.

[7] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of things," *IEEE Access*, vol. 4, pp. 2292–2303, May 2016.

[8] X. Wang, M. Chen, T. Taleb, A. Ksentini, and V. C. M. Leung, "Cashe in the air: Exploiting content caching and delivery techniques for 5G systems," *IEEE Commun. Mag.*, vol. 52, no. 2, pp. 131–139, Feb. 2014.

[9] C. Liang, F. R. Yu, and X. Zhang, "Information-centric network function virtualization over 5G mobile wireless networks," *IEEE Network*, vol. 29, no. 3, pp. 68–74, May–June 2015.

[10] K. Wang, F. R. Yu, H. Li, and Z. Li, "Information-centric wireless networks with virtualization and D2D communications," *IEEE Wireless Commun.*, vol. 24, no. 3, pp. 104–111, June 2017.

[11] M. Zhang, H. Luo, and H. Zhang, "A survey of caching mechanisms in information-centric networking," *IEEE Commun. Surv. & Tutorials*, vol. 17, no. 3, pp. 1473–1499, Third-quarter 2015.

[12] T. Koponen, M. Chawla, B. Chun, A. Ermoliskiy, K. H. Kim, S. Schenker, and I. Stoica, "A data-oriented (and beyond) network architecture," *Proc. ACM Annual Conf. Special Interest Group on Data Commun. (SIGCOM'07)*, pp. 181–192, Kyoto, Japan, Aug. 2007.

[13] http://www.named-data.net/ . [retrieved: June 2018]

[14] V. Sourlas, L. Gkatzikis, P. Flegkas, and L. Tassiulas, "Distributed cache management in information-centric networks," *IEEE Trans. Network and Service Management*, vol. 10, no. 3, pp. 286–299, Sept. 2013.

[15] S. Wang, J. B. J. Wu, and A. V. Vasilakos, "CPHR: In-network caching for information-centric networking with partitioning and hash-routing," *IEEE/ACM Trans. Networking*, vol. 24, no. 5, pp. 2742–2755, Oct. 2016.

[16] M. Hajimirsadeghi, N. B. Mandayam, and A. Reznik, "Joint caching and pricing strategies for popular content in information centric networks," *IEEE J. Sel. Areas in Commun.*, vol. 35, no. 3, pp. 654–667, Mar. 2017.

[17] W. Li, S. M. A. Oteafy, and H. S. Hassanein, "Rate-selective caching for adaptive streaming over information-centric networks," *IEEE Trans. Computers*, vol. 66, no. 9, pp. 1613–1628, Sept. 2017.

[18] S. Shakkottai, T. S. Rappaport, and P. C. Karlsson, "Cross-layer design for wireless networks," *IEEE Commun. Mag.*, vol. 41, no. 10, pp. 74–80, Oct 2003.

[19] V. Srivastava and M. Motani, "Cross-layer design: A survey and the road ahead," *IEEE Commun. Mag.*, vol. 43, no. 12, pp. 112–119, Dec. 2005.

[20] V. Erceg, L. J. Greenstein, S. Y. Tjandra, S. R. Parkoff, A. Gupta, B. Kulic, and A. A. Julius, "An empirically based path loss model for wireless channels in suburban environments," *IEEE J. Sel. Areas in Commun.*, vol. 17, no. 7, pp. 1205–1211, July 1999.

[21] J. G. Proakis, *Digital communications 5th Edition*, McGraw-Hill, Jan. 2008.

[22] E. W. Dijkstra, “A note on two problems in connection with graphs,” *J. Numerische Mathematrik*, vol. 1, no. 1, pp. 269–271, Dec. 1959.
[22] http://www.digi.com/ . [retrieved: June 2018]
[23] M. Xie, I. Widjaja, and H. Wang, “Enhancing cache robustness for content-centric networking,” *Proc. IEEE Int. Conf. Comp. Commun. (INFOCOM'12)*, pp.2426–2434, Orlando, USA, Mar. 2012.
[24] M. Conti, P. Gasti, and M. Teoli, “A lightweight mechanism for detection of cache pollution attacks in named data networking,” *Computer Networks*, vol. 57, no. 16, pp. 3178–3191, Nov. 2013.
[25] Q. Li, X. Zhang, Q. Zheng, R. Sandhu, and X. Fu, “LIVE: Lightweight integrity verification and content access control for named data networking,” *IEEE Trans. Info. Forensics and Security*, vol. 10, no. 2, pp. 308–320, Oct. 2015.
[26] G. Mauri, R. Raspadori, M. Gerlay, and G. Verticale, “Exploiting information centric networking to build an attacker-controlled content delivery network,” *Proc. 14th IFIP Annual Mediterranean Ad-Hoc Networking Workshop (MED-HOC-NET'15)*, pp. 1–6, Algarve, Portugal, June 2015.
[27] H. Guo, X. Wang, K. Chang, and Y. Tian, “Exploiting path diversity for thwarting pollution attacks in named data networking,” *IEEE Trans. Info. Forensics and Security*, vol. 11, no. 9, pp. 2077–2090, Nov. 2016.
[28] J. Zhang, N. Xue, and X. Huang, “A secure system for pervasive social network-based healthcare,” *IEEE Access*, vol. 4, pp. 9239–9250, Dec. 2016.
[29] A. Dorri, S. S. Kanhere, and R. Jurdak, “Towards an optimized blockchain for IoT,” *IEEE/ACM Second Int. Conf. IoT Design and Implementation (IoTDI'17)*, pp.173–178, Pittsburgh, USA, Apr. 2017.
[30] M. Banerjee, J. Lee, and K. R. Choo, “A blockchain future to Internet of things security: A position paper,” *J. Digital Commun. and Networks*, Oct. 2017.
[31] Raspberry Pi: https://www.raspberrypi.org/ . [retrieved: June 2018]
[32] MD5 algorithm, *IETF RFC 1321*.
[33] SHA-1 algorithm, *IETF RFC 3174*.
[34] CLX C++ library: https://github.com/clown/clx . [retrieved: June 2018]
[35] GNU GCC compiler: https://gcc.gnu.org/ . [retrieved: June 2018]
[36] U. Raza, P. Kulkarni, and M. Sooriyabandara, “Low power wide area networks: An overview,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 2, pp. 855–873, Jan. 2017.
[37] H. Wang and A. O. Fapojuwo, “Survey of enabling technologies of low power and long range machine-to-machine communications,” *IEEE Commun. Surv. Tutorials*, vol. 19, no. 4, pp. 2621–2639, June 2017.
[38] LoRa alliance: https://www.lora-alliance.org/. [retrieved: June 2018]

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
A Study on Off-path Caching Scheme by using Successive Interference Cancellation for Information-Centric Network-based Wireless Sensor Network	Proc. IARIA the 16-th International Conference on Networks (ICN ’17)	2017 年 4 月
コンテンツ指向型無線センサネットワークにおける効率的なキャッシング手法に関する一検討	電子情報通信学会・知的環境とセンサネットワーク(ASN)研究会技術報告	2017 年 7 月
コンテンツ指向型無線センサネットワークにおけるオーバヒアリング現象に基づくオフパスキャッシング手法	2017 年電子情報通信学会ソサイエティ大会	2017 年 9 月
Cross-Layer Design for Caching Scheme	IARIA International Journal on	2017 年 12 月

by using Successive Interference Cancellation in Information-Centric Network-based Wireless Sensor Network	Advances in Networks and Services	
Fundamental Analysis for Blockchain-based Secured Caching Scheme for Information-Centric Network-based Wireless Sensor Network	Proc. 2018 RISP International Workshop on Nonlinear Circuits, Communication, and Signal Processing (NCSP '18)	2018年3月
Secured Caching Scheme by using Blockchain for Information-Centric Network-based Wireless Sensor Network	信号処理学会・Journal on Signal Processing	2018年5月