2009-13-04

フレーミング信号が隠蔽可能な完全機密化通信

Perfect Classified Communication Channel with Encrypted Framing Signal

80817296 松岡洋樹(Hiroki Matsuoka)　Supervisor 西宏章(Hiroaki Nishi)

1. 緒　論

近年，新たな暗号解読法としてサイドチャネルアタックが注目されている．ケーブルに針を刺して電位を読み取るケーブルプロービングやモニターケーブルからの漏洩電磁波を解析して，数 m 離れた PC のモニターを再現する TEMPEST などがこれに該当する．また，高いセキュリティが求められる場合にパケットの存在自体を隠蔽する必要があることから，サイドチャネルアタックへの対応および高度な秘匿化技術が求められている．提案手法は高速通信に必要な DC バランスを考慮した上で，上記のサイドチャネルアタックに対応し，かつパケットの存在を隠蔽することができる新しいセキュリティ手法である．さらにパケットとパケットの区切りであるフレーミング信号を暗号化することでセキュリティレベルを向上する．

2. 完全機密化通信

完全機密化通信は，信号伝送路を流れるすべての信号を機密化し，盗聴しても 0 と 1 の乱数として見えるレイヤ 1 機密化通信システムである．完全機密化通信ではルータやネットワークスイッチといった中継点で，送られてきたパケットの復号化と暗号化を繰り返し，パケットを目的地まで転送する．本提案システムでは機密化手法として AES[1]を用いており，その特性を利用して 8B/10B や 64B/66B[2]などの符号化手法を実装することなく DC バランスを維持する．

3. フレーミング信号暗号化

従来手法では，送信側と受信側の同期をとるためデリミタとしてフレーミング信号を付加していた．そのため，第三者は容易にパケットの先頭を知ることができた．提案手法はフレーミング信号を機密化することにより，第三者にパケットの先頭情報を隠蔽し，従来手法に比べセキュリティレベルを向上することができる手法である．本研究では，フレーミング信号暗号化手法として，パケットにフレーミング信号を付加した後に暗号化を行う FBE(Framing Before Encryption)と暗号化されたパケットに別途暗号化されたフレーミング信号を付加する FAE(Framing After Encryption)の 2 種類の暗号手法を提案する．

まず，FBE についての説明をする．AES 変換では 128 ビット情報の変換が行われるため，その入力であるパケットデータとフレーミング信号の合計が 128 ビットにならなければならない．一般的に入力されるデータは 8 ビットのブロック単位で構成されているため，フレーミングは 8 ビットの倍数になることが条件となる．さらにスループット減少率を小さくするためには，フレーミング信号のビット幅が小さいことが求められるため，FBE ではフレーミング信号をデータのブロックと等しい 8 ビットとする．フレーミング信号の作成方法として，従来エラー検出や認証などのデータ整合性の検査として用いられていたチェックサムまたは CRC を用いる．したがって，データ 120 ビットにフレーミング信号 8 ビットを加えた構成となる．しかし，FBE にはこのフレーム構造に起因する問題点がいくつかある．レイヤ 2 から XAUI や XGMII などのインターフェイスを用いてレイヤ 1 に転送される時，32 ビットのブロックで送られ，データブロックとして必要な 120 ビットが 32 ビットの倍数ではないため，これらのインターフェイス仕様に変更が求められる．さらに，FBE は 120B/128B 変換とみなすことができるため，スループットの減少率は 6.25%となる，結果，スループット減少率が 3.03%である従来の符号化手法 64B/66B に比べて大きく転送スループットの低下を招く．即ち高速通信路に FBE を利用することが困難であるといえる．FBE はこれらの問題があるが，AES を改変することなく利用できるため，AES が有する暗号化強度をそのまま引き継ぐことができるというメリットがある．

次に FAE について説明する．FAE では FBE の問題点を解決することができる．スループット減少率を小さくするために，暗号化されたフレーミングを 1 ビットとし，128B/129B 変換とする．この場合，スループット減少率が 0.78%となり，64B/66B より小さく転送効率が良い．また，入力側が 128 ビットであるためレイヤ 2 から送られてきた 32 ビットのデータブロック構造そのまま利用できる．次にフレーミング信号の暗号化手順を説明する．フレーミング信号暗号化手法には，データを暗号化する際に用いる AES モジュールを利用しデータ暗号化と同時にフレーミング信号を得る方法を提案する．この方法では，回路コストの削減も期待できる．AES は，ラウンド変換とよばれる変換方式を繰り返すことによって暗号文を作成する．フレーミング信号暗号化にはこの各ラウンド変換によって変換されたラウンドデータを用いる．図 1 はフレーミング信号暗号化の流れを作成したものである．

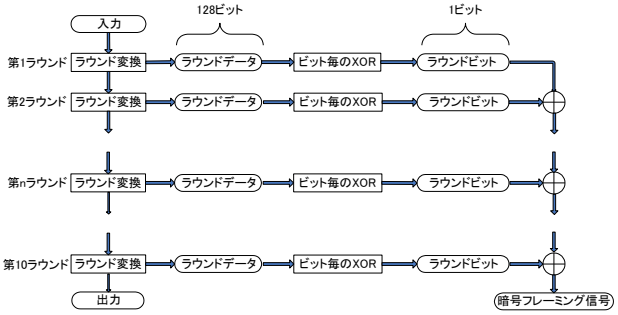

図 1　FAE のフレーミング信号暗号化の流れ

本研究では鍵長が 128 ビットである AES-128 を用いて説明を行う．このとき，ラウンド変換は 10 回繰り返される．

はじめに，128 ビットのラウンドデータにあるそれぞれのビットに対する XOR を計算する．算出される結果は 1 ビットであり，これをラウンドビットと呼ぶ．この計算を各ラウンドデータに対して行い，10 個のラウンドビットを得る．次に，これらのラウンドビットの XOR をとることによって，1 ビットのデータを得ることができ，このデータを暗号化されたフレーミング信号として利用する．この計算過程は，XOR を利用した計算のみで構成されるため，少ない回路コストで実装することができる．

次に，スペシャルキャラクターの表現方法について述べる．スペシャルキャラクターはアイドリングやリンク障害通知などの制御コードを示す情報である．従来手法が有する利便性

を損ねないためには，スペシャルキャラクターが表現できる必要がある．例えば，従来手法の 64B/66B では 2 ビットのフレーミング信号{01}と{10}の 2 種類を用いてペイロード内にあるスペシャルキャラクターの有無を判別している．

FBE では，8 ビットのフレーミング信号内の 1 ビットを用いてスペシャルキャラクターの有無を判別する．すなわち，7 ビットをデータ同期のためのフレーミング信号とし，残りの 1 ビットをスペシャルキャラクターの判別に利用する．この 1 ビットのフレーミング信号も AES によって暗号化されるため秘匿できる．

FAE では，スペシャルキャラクターを保証するためにフレーミング信号を 2 ビットにして，1 ビットをデータ同期用，残りの 1 ビットをスペシャルキャラクター用とする．これにより，128B/130B となり，スループット減少率は 1.57%と大きくなるが，それでもなお 64B/66B 手法より小さい．また，スペシャルキャラクター用のフレーミング信号暗号化手法はデータ同期用フレーミング信号暗号化とほぼ同等の手法を用いる．10 個のラウンドデータから 5 個のラウンドデータを選択し，選択したデータに対してラウンドビットを求め，それらの XOR を算出して 1 ビットのデータを得る．その結果と初期値(スペシャルキャラクターが含まれているなら{0}，含まれていなければ{1})との XOR を行い，最終的な出力をスペシャルキャラクター用のフレーミング信号とする．

4. ハードウエアアーキテクチャ

代表として，FAE のアーキテクチャを図 2 に示す．左側が送信側，右側が受信側である．

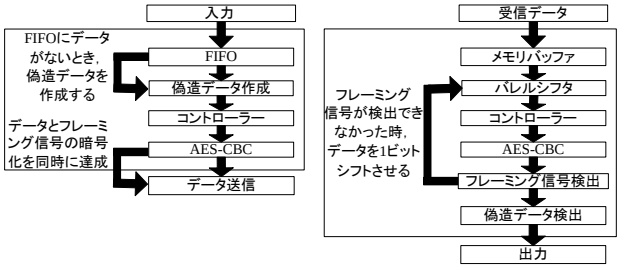

図 2　FAE のアーキテクチャ

はじめに，　送信側の流れを説明する．入力データは FIFO に格納される．もし，この FIFO にデータがなかった場合，偽造データが作成される．FBE の場合，入力データ，偽造データどちらのデータに対しても，フレーミング信号が作成され，128 ビットのデータブロックをつくる．これらのデータに対して，AES-CBC を用いて共に暗号化する．AES-CBC は AES のモードの 1 種であり，同一データがネットワーク上に流れにくくすることができる．FBE では暗号化されたデータをそのまま送信し，FAE では第 3 章で述べた方法を用いてフレーミング信号の暗号化を行い暗号データに付与して送信する．

次に受信側の説明を行う．FBE，FAE 共にほぼ同じアーキテクチャである．まず，受信データをメモリバッファに格納する．そのデータを AES-CBC を用いて復号する．その後，フレーミング信号の一致を調べる．フレーミング信号が一致していれば，{0}をデータとして蓄える．次に，フレーミング信号の一致に関わらず，同じ受信データを 1 ビットシフトして一連の流れを繰り返すことを 130 回繰り返す．ただし，この過程でフレーミング信号が一致していれば{シフトした量}をデータとして蓄える．その後，次の受信データに対して同じことを繰り返す．この時，先ほど蓄えられたデータ量をバレルシフタでシフトさせてフレーミング信号の一致を調べる．この一連の作業を繰り返すことによって，フレーミング信号を 1 つに絞ることができる．

5. 評　価

FAE において，暗号化されたフレーミング信号の安全性の評価を行う．入力データとして疑似乱数を用い，128 ビットのデータを 1000 個用意した．これらの入力データに対し，130 ビットの出力データを 1000 個得た．暗号化されたフレーミング信号と暗号化データの相関性を調べるために，ポアソン分布の検定を行う．図 3 は，データ全体，場所的局所性，時間的局所性の 3 つの観点から，{0}または{1}の同一データが連続して出現する個数を表したグラフである．

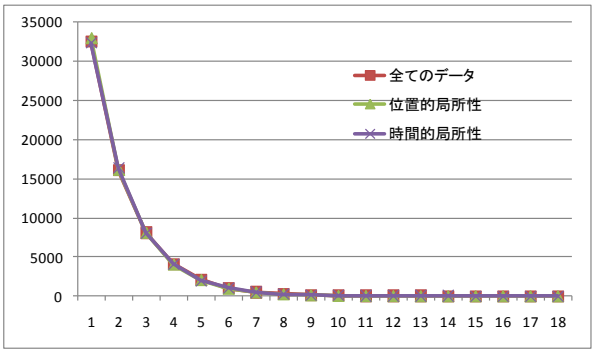

図 3　ポアソン検定の評価図

3 種類のデータからカイ二乗検定を用いたところ，有意水準 5%の検定において帰無仮説が採択される．したがって，暗号化されたフレーミング信号と暗号化データの相関性はなく，悪意ある第三者が本システムを盗聴しようとした場合，データの先頭を判別することはできない．

また，表 1 にこれらの手法の回路サイズと遅延の評価を示す．表 1 から，FAE は FBE に比べ回路サイズの面で小さくなっていることが分かるが，遅延は大きくなっている．

表 1　完全機密化通信のサイズと遅延

		回路サイズ (μ m^2)	遅延(ns)
FBE	チェックサム	60418	3.11
	CRC	58892	3.11
FAE		56966	5.10

6. 結　論

本要旨では，完全機密化通信におけるフレーミング信号の暗号化手法を提案した．その手法として FBE と FAE の 2 種類の提案手法を行った．これらの提案手法は第三者のデータ先頭判別を困難にするため，機密性が高い通信路を確保することができる．FAE は FBE と比べて，遅延の点では劣っているが，スループット減少率，回路サイズ，レイヤ間を移動するインターフェイスによる利便性の面ですぐれている．さらに，暗号化されたフレーミング信号の安全性をポアソン分布の観点から示した．提案手法である完全機密化通信はサイドチャネルアタックを防御し，高度な秘匿化技術を有したセキュリティ技術であるといえる．

参考文献

[1] National Institute of Standards and Technology (NIST) FIPS-197 “Specification for the ADVANCED ENCRYPTION STANDARD (AES)” Nov, 2001

[2] Rick Walker and Richard Dugan, “64b/66b low-overhead coding proposal for serial links”, http://grouper.ieee.org/groups/802/3/10G_study/public/jan00/walkew_1_0100.pdf, 2002.