Considerations Regarding System Configuration and Necessary Conditions for Radio Signal Hiding in Wireless Communications

Hideichi SASAOKA*

(Received April 17, 2014)

Recently, physical layer security has attracted attention in the area of wireless communication; the main technology was a secret key agreement and secret information transmission using radio propagation. Radio signal hiding, which applies the concept of steganography to wireless communication is proposed, and is called radio steganography. However, systematic examination of system configuration and the necessary conditions for radio signal hiding was insufficient. This paper explains the concept of radio signal hiding and clarifies the problem of steganography for wireless communication. Next, a system configuration, the attack model for an eavesdropper, and the necessary conditions are examined for realization of radio signal hiding. Moreover, radio signal hiding using multiple antennas is proposed, and improvement of tolerance to stegonalysis of a proposed system is examined. Furthermore, the function of the stego-key confidentiality is considered.

Key words：physical layer security, information hiding, radio steganography, stegonalysis

キーワード：物理層セキュリティ，情報ハイディング，無線ステガノグラフィ，ステゴ解析

無線通信における無線信号秘匿のシステム構成と所要条件に関する検討

笹岡　秀一

1．はじめに

無線通信は，開かれた空間を通して電波の送受信を行うため，盗聴や不正アクセスなど情報セキュリティ面の脆弱性が問題となっている．この対策としては，暗号技術を使用するのが実用的観点から一般的である．しかし，別の取組として電波（物理層）における情報セキュリティ（所謂，Physical Layer Security）に対する関心が高まっている．物理層セキュリティ技術としては，無線通信路特性を用いた秘密鍵共有 [1-2] と秘密情報伝送 [3] が代表的なものであり，各種の研究が行われている [4]．また，最近，情報ハイディングの概念を無線通信に適用した無線信号秘匿が検討されている [5-6]．

無線信号秘匿は，ステガノグラフィの概念を無線通信に適用したもので，通信行為（無線信号）そのものを秘匿するものである．無線信号秘匿に関しては，これまで埋込み信号にスペクトル拡散信号を用いて方式の提案と初期検討 [5]，OFDM 信号をカバー信号とし OFDM 信号に類似の周波数拡散信号を用いた方式の提案と初期検討 [6] が行われている．しか

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6355, FAX: +81-774-65-6801, E-mail: hsasaoka@mail.doshisha.ac.jp

し、盗聴者による埋込み信号の検知法の検討と検知困難性に対する定量的評価が不十分であった. また, 無線信号秘匿の構成法と所要事項に関する系統的な検討が不十分であった．さらに，埋込み信号の検知（ステゴ解析）を困難とする条件設定に関する汎用的な検討が不足していた.

そこで，本論文では，はじめに無線信号秘匿の技術的な基盤であるステガノグラフィ技術を概説し，ステガノグラフィに対する攻撃（ステゴ解析）と守秘の特徴を明らかにする．次に，無線信号秘匿の概念とその課題，システム構成と攻撃のモデル，ステゴ解析を困難とする条件設定，などを検討する．また，複数アンテナを用いた無線信号秘匿を提案し，ステゴ解析を困難とすると条件設定がより容易となることを示し，提案方式の有効性を明らかにする．さらに，無線信号秘匿が満たすべき条件設定をステゴ解析の性能劣化要因と関連付けて網羅的に検討する．また，守秘性能に関連するステゴ鍵の役割・機能について幅広く検討する．これらにより無線信号秘匿に関して，今後取組むべき検討課題を明らかにする.

2．ステガノグラフィ技術

2.1 情報ハイディング

情報ハイディング（情報隠匿 : Information hiding）とは，ある情報メディアにその情報と異なる別の情報を埋込むことであり，それに用いられる技術を情報ハイディング技術と呼ぶ [7]．情報ハイディング技術は利用目的と応用形態により各種のものがあるが, ステガノグラフィ（通信秘匿 : Steganography）と電子透かし (Digital watermark) が代表的なものである [7]．その他にメッセージの送信者や受信者を不明にする匿名通信路（Anonymous channel），電子透かしの簡易版との言えるディジタル指紋 (Digital fingerprint) などがある [8].

ステガノグラフィは，通信の事実自体を秘密にしながら情報を伝送する技術である [7]．一般に，ある情報メディアに別の秘密情報を秘密裏に埋込むことにより実現する．この通信秘匿は，暗号を用いた通信（秘匿通信, 又は秘密通信）と異なる概念である. 秘匿通信は，秘密情報を伝送するために暗号によって情報を秘匿して通信を行うことである．一方，通信秘匿は，通信の事実自体，および伝送される秘密情報を秘匿して通信を行うことを意味している.

一方，電子透かしは，ある情報メディアに別の情報を埋込むことにより，著作権主張や情報改ざんの検知などの機能を実現する技術である [7]．電子透かしにおいては，別の情報が埋め込まれていること自体が知られても構わない．むしろ，電子透かしとして埋め込まれた情報が存在することを明確にして，その機能を達成する.

情報ハイディングでは，ある情報メディア（公開情報メディア）のどの部分に何をどのように隠しているのか, 第３者に不明とすることが一般的である．すなわち，利用目的と応用形態に依存した前提が特に設定されない限り，何が秘密情報か，秘密情報の処理アルゴリズム，埋込み手法などが未知なことを前提とする.

2.2 ステガノグラフィの概要

2.2.1 ステガノグラフィの概念

ステガノグラフィでは，ある情報メディアを媒体として，それを巧みに改変し，伝送したい秘密情報を当事者以外に秘密裏に伝送する手法である [7]．この通信自体を隠す点が暗号技術と異なっている．このため，伝送したい秘密情報は媒体となる情報メディア（データ）に埋め込まれる．ここで，埋め込まれる秘密情報は, 埋込み情報 (Embedded information) と呼ばれ，媒体となる情報メディアは，カバーデータ (Cover data) と呼ばれ，その結果として得られるデータは, ステゴデータ (Stego data) と呼ばれる [7]. ステガノグラフィでは，ステゴデータとカバーデータとの差を識別できないところに安全性の大半が依存している [8].

ステガノグラフィを用いた通信が毎回同じアルゴリズムで処理されると, ①第３者による通信の検知, ②当該通信相手以外の別の通信相手による通信を検知，などの危険性が増加する [7]．その対策としてステゴ鍵 (Stego-Key) と呼ばれるパラメータ処理が用いられる．この鍵は，通信相手ごと又は通信ごとに

適宜変更され，それを知らない当該通信相手以外の第３者が，通信を検出することを困難とする．さらに，通信が検知できたとしても，通信内容の取得をより困難とする[7]．ステガノグラフィの構成を Fig. 1 に示す．

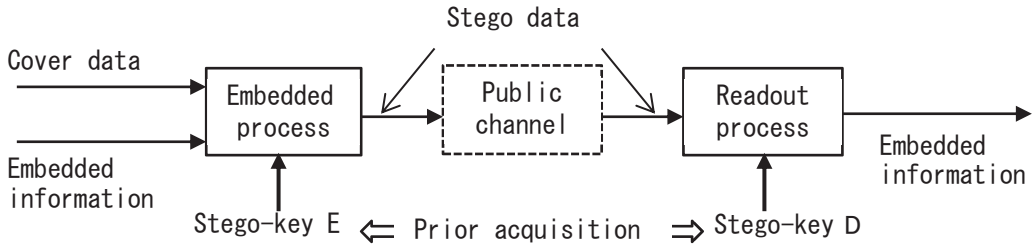

Fig. 1. Configuration of steganography.

2.2.2 ステガノグラフィが満たすべき性質

ステガノグラフィ技術においては，埋込み情報の検知又は存在推定がされないために，①通信検知困難性，②カバーデータの自然さ，などの性質が求められる．

通信検知困難性とは，通信秘匿を達成するために埋込み情報の検知が困難なことである．このための必要条件の一つとして，カバーデータの品質の保持がある[7]．品質が劣化すると埋込み情報の存在に気付く危険性が増加する．また，情報を埋め込んだステゴデータの自然さの保持も重要となる．ステゴデータが見かけ上カバーデータとほぼ同一でない場合，埋込み情報の存在に気付く危険性が増加する．

カバーデータの自然さについては，ステゴデータの伝送自体が検知されなくても，カバーデータが不自然であると，カバーデータ以外の情報が隠されているとの疑念を抱かせる危険性が増加する．カバーデータが実際に意味のある情報であることが望ましい．

2.2.3 ステゴ鍵の機能とステガノグラフィの分類

ステガノグラフィは，埋込みと読み出し処理に用いられるステゴ鍵の有無と性質によって，純ステガノグラフィ，共通鍵ステゴノグラフィなどに分類される[7]．純ステガノグラフィの場合，事前に鍵情報などの秘密情報を共有する必要はない．但し，当事者間で，埋込み情報の埋込み処理と読み出し処理について，共有しておく必要がある．

一方，共通鍵ステガノグラフィの場合，埋込み情報を埋込む処理 E と読み出し処理 D において用いられる鍵は共通で，$K_E=K_D=K$ である．事前に共有鍵，又は，共通ステゴ鍵 K を生成するための秘密情報を共有する必要がある．また，埋込む処理 E と読み出し処理 D も共有しておく必要がある．

2.3 ステゴグラフィに対する攻撃と守秘の特徴

2.3.1 ステゴ解析技術

ステガノグラフィによる通信を検知する技術は，ステゴ解析（ステガナリシス：Steganalysis）と呼ばれ，近年研究が始められつつある[7]．通信検出を行う行為を「攻撃」と呼ぶが，考えられる攻撃は利用可能な情報など，状況の相違に依存する．ステガノグラフィに対する主要な攻撃には，Stego-only Attack, Known Cover Attack, Chosen Stego Attack, Known Stego Attack などがある．

Stego-only Attack とは，攻撃対象データのみを解析して，埋込み情報の有無を判定する攻撃である．（暗号解読における暗号文攻撃に対応する概念である．）

Known Cover Attack とは，攻撃対象データと改変が加えられていないカバーデータがある状況において，それらを解析することで，埋込み情報の有無を判定する攻撃である．この場合，データの改変は容易に検知されるが，それが直ちに埋込み情報の検出

とはならない．単にステゴ解析者をかく乱する意味のない情報(雑音)が加えられている可能性もあり，埋込み情報の存在までは確認できない[7]．

Chosen Stego Attack とは，ステゴ作成アルゴリズム（埋込み方法）が分かっている状況で，攻撃対象データに埋込み情報が存在するかどうかを判定する攻撃である．(改変されないカバーデータは入手できないとしている．)

Known Stego Attack とは，ステゴデータ作成アルゴリズムが既知で，改変されないカバーデータが得られる状況において，埋込み情報の有無を判定する攻撃である．

上記のように攻撃レベルの分類ができるが，純ステガノグラフィなどは，Known Stego Attack に対して脆弱となると思われる．この攻撃に対しては，攻撃対象データの改変が容易に検出される．それゆえ，この攻撃に耐性を保持するには，その改変が単なるかく乱情報か，埋込み情報に起因するものかの判定を不可能にする必要がある．その一手段は，ステゴ鍵の活用によりステゴデータからの埋込み情報の解読を不能にすることである．

ここで、攻撃がより容易となる Known Stego Attack の前提がどのような状況で妥当になるかについては，議論の余地のあるところである．このため、攻撃の耐性の検討においては，検知が容易な前提のもとで攻撃耐性を議論するばかりでなく，より検知が難しい前提のもとでの攻撃法についても評価すべきである．

2.3.2 守秘における特徴と効用

(1) 暗号技術とステガノグラフィの役割

守秘性を保証する主要な技術は暗号技術であるが，暗号を用いた通信を公開通信路で行う場合，暗号文の存在は比較的容易に検知されるため，暗号解読等の攻撃を受け易い．一方，ステガノグラフィは，秘密情報を伝送する通信自体を秘匿する技術であり，攻撃対象とならないためのものであり，その守秘機能は暗号技術ほど堅固ではない．暗号とステガノグラフィは，併用可能な技術であり，ステガノグラフィは暗号技術の補完的な役割である．暗号による通信の存在を知られたくない場合や存在が明らかになることで攻撃対象となることを避ける機能を果たしている．ここに，ステガノグラフィの特徴がある．

(2) 守秘におけるステガノグラフィの効用

ステガノグラフィは，ある情報メディア（公開メディア）に秘密の情報が含まれているか否か，含まれる場合でも何を隠しているのか，どの部分に埋め込まれているか，どのように隠しているか，などを第３者に分からないようにするのが原則である．このような場合には，ステゴデータとカバーデータとの統計的な有意差の判定で埋込み情報の有無を判定することになる．なお，少数のステゴデータが，埋込み可能な膨大な数の情報メディアに含まれている一方，攻撃対象の効果的な選別法がない場合，総当たりでステゴ解析を行うと多大の労力を要することになる．この労力（コスト）とステゴ解析に成功した場合に得られる利得との兼ね合いが，ステゴ解析の攻撃の抑止力になっている．これが，ステガノグラフィの効用である．

(3) ステガノグラフィの課題

上記の場合には，ステガノグラフィが暗号解読等の攻撃に対する抑止となっている．しかし，その前提が成り立たず，攻撃対象データの絞り込みが効率的に行われ，攻撃が容易となる条件が揃っている場合には，ステガノグラフィの効用は大幅に損なわれる．したがって，ステガノグラフィでは，簡単に攻撃対象の絞り込みが行われないように注意を要する．また，Known Stego Attack に対しても，多少の耐性を持つことが望ましい．なお，ステゴ解析のコストが抑止力となっていると考えた場合，方式を複雑にすれば良いが，正規者のコストも多大となるのでは意味がない．攻撃により受ける損失よりも守秘コストが大きい場合，コスト面からは秘密情報を守る理由が不明確となる．したがって，正規者間で復号が容易である一方，盗聴者に困難な方式が求められる．すなわち，正規者のコストと盗聴者のコストの比が大きいことが重要となる．

３．無線信号秘匿

3.1 無線信号秘匿の概要

無線信号秘匿の基本概念は，情報メディアにおけるステガノグラフィ（通信秘匿）の概念を無線伝送メディアに適用しようとする試みである．無線信号秘匿では，ステガノグラフィにおけるカバーデータ，埋込み情報，ステゴデータに相当するものを，それぞれカバー信号，埋込み信号，ステゴ信号と呼ぶ．また，従来のステガノグラフィが情報メディアにおける情報処理に基づいていたのに対し，無線信号秘匿（無線ステガノグラフィ）は，伝送メディアにおける信号処理に基づいている．そこに，無線信号秘匿の新たな課題が発生するとともに，電波伝搬の多様性と複雑性に基づく新たな方式の可能性がある．

3.1.1 無線信号秘匿の概念

無線信号秘匿では，通常の情報で変調された無線通信信号をカバー信号とし，秘密情報で変調された埋込み信号をカバー信号に埋込み，ステゴ信号とする．正規者 A（送信側）では，アンテナ送信前に埋込み処理が行われ，ステゴ信号が送信される．また，正規者 B（受信側）では，カバー信号や埋込み処理内容が既知などの前提の下で，ステゴ信号から埋込み信号が分離され，埋込み信号から秘密情報が抽出される．ここで，無線信号秘匿がある処理内容で実施され，同一処理が繰り返されると，ステゴ解析に余計な情報を与えることになる．また，秘密にしていた処理内容が公開になった場合，ステゴ解析が格段に容易となる．このため，処理手法は基本的に変更しないで処理内容を変更するため，ステゴ鍵を用いてパラメータ依存処理を行う．このステゴ鍵によりステゴ解析に対する耐性を確保する．

3.1.2 無線信号秘匿の課題

盗聴者は，利用可能な情報に基づいてステゴ解析を実施する．ステゴ解析では，はじめにカバー信号の情報を得ることを試みる．カバー信号は，通常の情報で変調された信号であり，一般に盗聴者もカバー信号の復調によりその情報を取得できるとするのが妥当である．ここで，その情報がアナログ情報の場合，伝送路での雑音，歪み，埋込み信号の影響により，元の情報を忠実に取り出すことが難しい．

一方，現在，主流であるディジタル通信の場合，受信雑音があまり大きくなければ，元の情報をほぼ正確に得ることが分かる．なお，不一致部分は誤りビットとなる．このとき，変調諸元（変調パラメータ）と電波伝搬特性等が盗聴者に既知であれば，カバー信号も容易にほぼ正確に得られることになる．ここで議論を一般化するために，受信カバー信号を再生可能成分と再生困難成分に分割して考える．上記は，再生困難成分と受信雑音が十分に小さい場合である．この状況は，ステゴ解析における Known Cover Attack に相当し，埋込み情報が検出される可能性が高くなる．これは，通常のステガノグラフィと異なり，無線信号秘匿に特徴的な課題である．

この解決には，検知されない程度のダミー信号（かく乱信号）を付加し，さらにそのダミー信号に埋込み信号を隠すことが必要となる．ここで，ダミー信号は盗聴者に未知であるが，正規受信者には未知の場合と既知の場合が考えられる．なお，既知の場合には，その情報を別途，事前に秘密裏に共有する必要がある．

3.1.3 無線信号秘匿の基本構成

Fig. 2 に無線信号秘匿の基本構成を示す．送信側では，カバー信号，ダミー信号，埋込み信号を合成して送信する．なお，信号合成には線形と非線形な手法があるが，非線形合成の方が受信側での信号分離が複雑となる．また，ステゴ解析への耐性が増加する．以下では，簡単のために線形合成を想定して，受信側での処理を説明する．

受信側では，初めにステゴ信号を復調して得たカバー情報に基づき，変調諸元と電波伝搬特性情報から受信カバー信号（再生可能成分）を再生する．次に，ステゴ信号から受信カバー信号を取り除き，残留信号を得る．

この残留信号には，受信カバー信号の再生困難成分（受信カバー信号の残差成分），受信機雑音，ダミー信号，埋込み信号が含まれる．この信号より埋込み情報の抽出処理を行い，埋込み情報を得る．ここ

で,埋込み情報の抽出処理は,埋込み信号の生成法,ダミー信号の生成法,ダミー信号の既知・未知の別,受信信号の残差成分の構成などに依存するので，具体的な手法は個々の場合に検討すべき課題である.

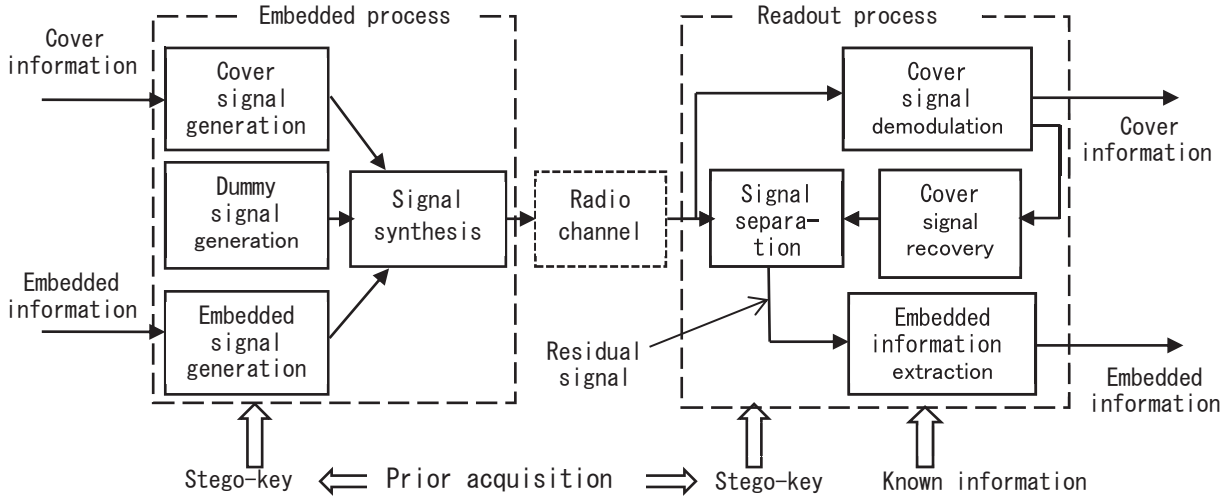

Fig. 2. Basic configuration of radio signal hiding.

3.1.4 盗聴者による攻撃のモデル

上記（Fig. 2）の無線信号秘匿に対する盗聴者による攻撃（ステゴ解析）のモデルを Fig. 3 に示す．ここで，ステゴ信号の存在を確認する攻撃は，受信側で実施される．この攻撃は，はじめに受信信号がステゴ信号である可能性を判別すること，すなわち攻撃対象の選別から始められる．このため，受信信号がカバー信号として不自然でないかが試験される．具体的には，カバー情報の品質（ビット誤り率など）が劣化していないか，受信信号の特性がカバー信号と比べて不自然でないか，などを調べる．次に，正規受信者と同様にカバー信号を復調して，受信カバー信号を再生することで，残留信号に対して埋込み信号を検出するための攻撃を行う．この攻撃には，各種の信号解析（スペクトル解析，振幅分布解析，相関解析など）が考えられる．埋込み信号が検出，又は疑わしい信号が検出されたら，埋込み情報の解読を実施する．そして，埋込み情報が得られたことで,埋込み信号の存在と埋込み情報が明らかとなる.

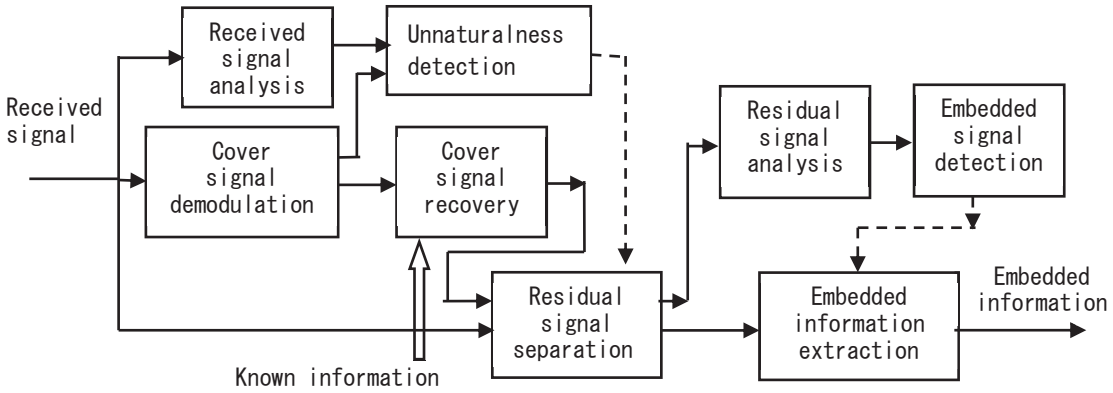

Fig. 3. System model of eavesdropper attack (steganalysis).

3.2 複数アンテナを用いた無線信号秘匿

上記の単一アンテナを用いた無線信号秘匿では，正規者と盗聴者の伝送品質の差別化が難しく，ステゴ解析に耐える条件設定が難しいと考えられる．一方，複数アンテナを用いた方式では，空間での信号重畳の効果を用いて，正規者と盗聴者の伝送品質の差別化の可能性が増加すると期待できる．そこで，複数アンテナを用いた無線信号秘匿の構成を検討した．

複数の送受信アンテナを用いる無線通信は，MIMO などで広くに用いられている．そのため，無線信号秘匿の目的で MIMO と類似のシステムを使用しても，直ちに無線信号秘匿の意図を悟られることはない．そこで，送受一系統の無線信号秘匿の構成を複数の送受信アンテナを使用した場合に拡張する．ここで，カバー信号は，通常の MIMO システムで伝送される信号と同様なものが望ましい．

3.2.1 送受信アンテナ２対を用いた構成例

送受信アンテナ２対を用いた無線信号秘匿の構成例を Fig. 4 に示す．送信側の埋込み処理部では，２系統のカバー信号，ダミー信号，埋込み信号を合成して，２系統のステゴ信号を得る．カバー信号はそのまま信号合成に入力するが，ダミー信号と埋込み信号は，両方の成分が含まれるように線

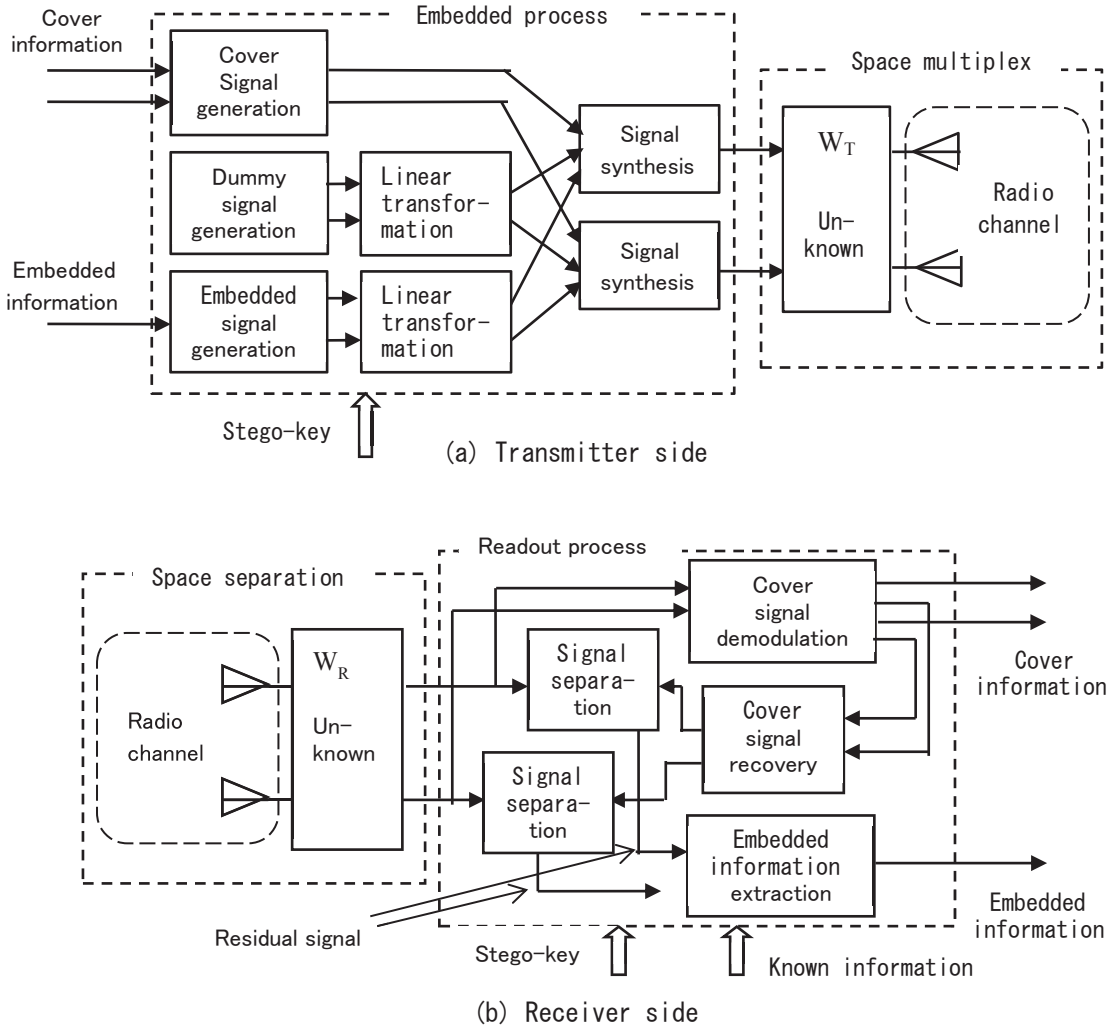

Fig. 4. System configuration of radio signal hiding using two pair antenna.

形変換して信号合成に入力する．埋込み信号は本来１系統でよいが,埋込み信号を何らかの信号処理(線形又は非線形）で二つに分割して，２系統で一つの信号とする場合も想定している．

２系統のステゴ信号は，重みづけ処理が行われたあと，2系列の送信アンテナから送信される.また，空間において信号の重畳が行われる．一方，受信側では，受信アンテナで受信されたあと，重みづけ処理が行われて,２系統のステゴ信号が取り出される．ここでは,送信側と受信側のアンテナの重みづけは，送信側の２系列の合成信号が受信側でそれぞれ分離されるように設定されるものとする．

受信側の読出し処理部では，１系統の場合と同様な処理が２系統のステゴ信号に対して実施される．２系統の残留信号（受信信号の残差成分，受信機雑音，ダミー信号，埋込み信号）から埋込み情報の抽出処理を行い，埋込み情報が得られる．ここで，２系統の残留信号からの埋込み情報の抽出処理は，埋込み信号の生成法，ダミー信号の生成法，線形変換法，受信信号の残差成分などに依存するので，具体的な手法は個々の場合に検討すべき課題である．

3.2.2 盗聴者による攻撃のモデル

上記（Fig. 4）の無線信号秘匿に対する盗聴者による攻撃のモデルを Fig. 5 に示す. 攻撃のモデルは Fig. 3 の攻撃モデルと共通点が多い．始めに，受信信号がステゴ信号である可能性を判別するために，受信信号がカバー信号として不自然でないかが試験される．その前提として，２系統の送信信号がそれぞれ分離されて受信されることが望ましい．ここで, Fig. 4 の送信重み等が未知の場合に，盗聴者はブラインドで空間フィルタリングによる信号分離を実施することになる．このブラインドの信号分離が正確に実施できれば，以下は２系統の受信信号に対して攻撃を行うことになる．なお，信号分離が不完全となると，それ以降の攻撃の困難さが増加する．

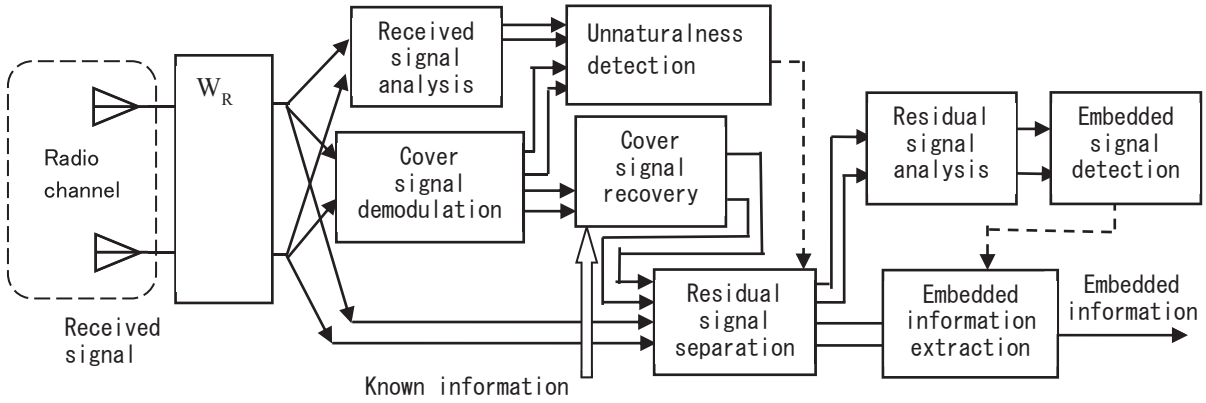

Fig. 5. System model of eavesdropper attack in the case of two cover signal.

3.2.3 複数アンテナを用いた構成の一般化

複数の送受信アンテナを用いて一般化した無線信号秘匿の構成を Fig. 6 に示す.

送信側の埋込み処理部では，複数のカバー信号，複数のダミー信号，複数の埋込み信号が合成され，複数のステゴ信号が出力される．次に，アンテナ・伝搬部（空間重畳・分離部）では，重みづけ（線形合成）されたステゴ信号が複数アンテナから送信され，空間で重畳される．また，複数アンテナで受信された信号に重みづけが行われ，空間重畳され信号の分離が行われる．複数のステゴ信号となる．受信側の読み出し処理部では，複数系統のカバー信号復調・再生と残留信号の分離が行われたあと，埋込み情報の抽出が行われる．Fig. 6 に示す無線信号秘匿に対する盗聴者の攻撃モデルは，Fig. 5 に示す攻撃モデルと同様である．しかし，アンテナ本数が増加すると，複数系統の送信信号に対してブラインドで空間フィルタリングを行い，それぞれを分離して受

信することがより困難となる．

3.2.4 複数アンテナを用いた無線信号秘匿の特徴

単一アンテナを用いた無線信号秘匿の場合，3.3節に示す「無線信号秘匿が満たすべき性質」を実現するための条件が厳しく，信号電力の設定などに余裕が小さい．しかし，複数アンテナを用いたシステムでは，ステゴ信号とカバー信号との差異を検知されない設定，ダミー信号が検知されない設定，埋込み信号が満たすべき条件などを比較的無理なく実現できる．特に，複数カバー信号が存在する場合，受信側で複数カバー信号を十分に分離できないと，受信信号の不自然さの検出，残留信号の分離，残留信号解析が不十分となる．このため，ダミー信号や埋込み信号の検出性能が劣化するので，その分だけダミー信号や埋込み信号の電力を大きく設定することが可能となり，埋込み信号の伝送性能の向上にも役立つ．

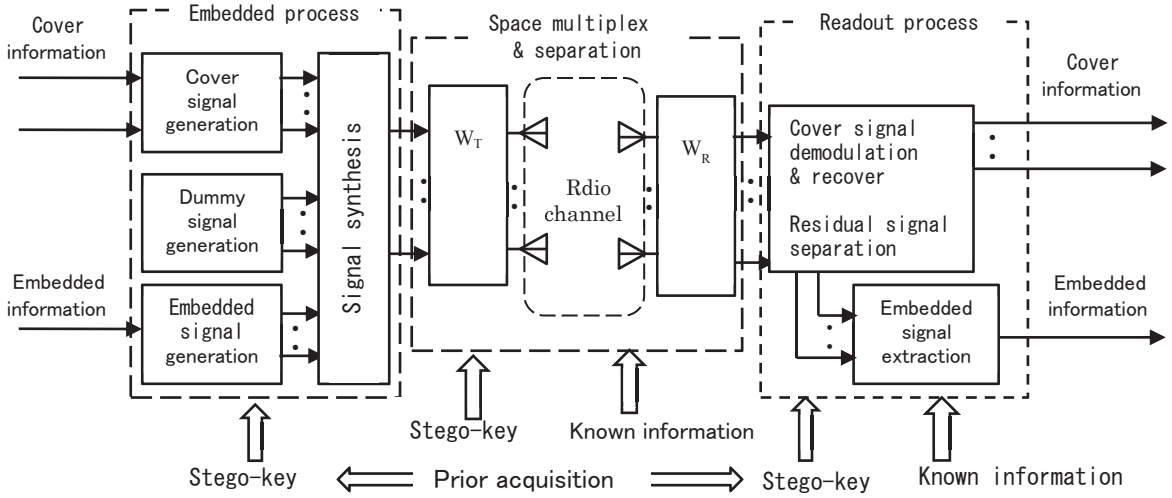

Fig. 6. System configuration of radio signal hiding using multiple antennas.

3.3 無線信号秘匿が満たすべき性質

無線信号秘匿において，カバー信号で伝送される情報（カバー情報）がごく自然なものであること，変調方式や伝送方式がごく一般的なものであることを前提とする．したがって，カバー信号自体から無線信号秘匿の存在を検知されないとする．その場合に，無線信号秘匿が満たすべき性質は，①ステゴ信号がカバー信号との差異により検知されないこと，②カバー信号を再生して得られる残留信号からダミー信号が検知されないこと，③残留信号から埋込み信号が検知されないこと，④埋込み信号の存在を想定した攻撃(埋込み情報の抽出)に耐性があること，などである．

3.3.1 ステゴ信号が検知されない設定

カバー信号との差異によってステゴ信号が検知又は推定されないためには，①ステゴ信号のカバー情報の品質（ビット誤り率など）に劣化がないこと，②ステゴ信号の波形が不自然でないこと，が必要となる．また，ステゴ信号とカバー信号の差異がどの程度まで検知されないかは，カバー信号の再現精度に依存している．

(1) カバー情報のビット誤り率

カバー信号のみの場合に比べステゴ信号の場合では，ダミー信号と埋込み信号の影響により，カバー情報のビット誤り率が多少とも必ず劣化する．ここで，カバー信号のみの場合に対して，カバー情報のビット誤り率がある範囲にある場合には，ステゴ信号の場合のビット誤り率の劣化をその範囲に収まるように設定すれば良い．

一方，カバー信号のみの場合のビット誤り率が盗

聴者に既知と仮定する場合，ビット誤り率の僅かな差も長時間測定すれば必ず検出される．しかし，その場合でもステゴ信号がある有限区間に限定されているとすると，短区間で測定されたビット誤り率には統計的なばらつきがある．そして，ビット誤り率の分布の重なり部分が多くなると，ビット誤り率に有意な差が検出できるかが問題となる．

(2) ステゴ信号の自然さ

送信されるカバー信号は，既知の変調諸元により発生した信号である．このため，信号波形（アイパターンを含む)，フェーザ (信号軌跡, 信号点配置)，スペクトル（電力スペクトル）および統計分布（振幅分布など）が変調諸元に依存した形状となる．受信カバー信号は，伝送路歪み，受信機雑音の影響を受け,送信されたカバー信号とは若干異なってくる．しかし，受信信号の形状と送信カバー信号の形状との相違がある範囲を超えると，ステゴ信号の存在が検知又は推測される．なお，相違が検知される範囲は，測定時間にも依存するので，個々に検討する必要がある．

3.3.2 ダミー信号が検知されない設定

(1) 残留信号からのダミー信号の検知

カバー信号（ディジタル変調波）の復調によりカバー情報が得られた場合，変調諸元と電波伝搬特性（振幅，位相，遅延歪み）が正確に分かれば，受信カバー信号のレプリカが比較的容易に得られる．この結果，受信カバー信号の再生困難部分（受信カバー信号の残差成分），受信雑音，ダミー信号，埋込み信号の和である残留信号が得られる．このため，残留信号からダミー信号が検知されないことが重要となる．ここで，受信カバー信号の残差成分が支配的でない場合には，受信雑音とダミー信号との識別が難しくなるように，ダミー信号を雑音的な信号とすることが重要となる．一方，受信カバー信号の残差成分が支配的な場合は，その成分に対して識別が難しい程度にダミー信号の電力を増加させて設定することが可能となる．また，ダミー信号に隠す埋込み信号の電力を増加させることも可能となる．

(2) カバー信号の再現の阻害要因

ステゴ信号の自然さ，又は残留信号の自然さの判断基準は，受信カバー信号の再現精度と関係している．以下に，受信カバー信号の再現精度を劣化させる要因を示す．

①伝送路歪み，干渉，受信雑音などによりカバー信号の復調時にビット誤りが発生すると，カバー信号の復調情報が元の送信カバー情報と不一致となる．このため，復調情報からは，不完全な送信カバー信号しか再生できない．

②伝送路歪み，干渉，受信雑音の影響により受信カバー信号の振幅・位相の再生が不完全となると，たとえ①の項目がほぼ完全であったとしても，受信カバー信号の再生が不完全となる．

③伝送路歪み（遅延歪み）の推定が困難の場合，又は，雑音，干渉の影響で推定誤差が発生する場合には，たとえ①，②の項目がほぼ完全であったとしても，受信カバー信号の再生が不完全となる．

④たとえ，①，②，③の項目がほぼ完全であったとしても，送信増幅器で非線形増幅が行われ，その非線形特性が未知の場合，非線形歪みも含めた受信カバー信号の再生は難しい．

3.3.3 埋込み信号が満たすべき条件

埋込み信号が満たすべき条件は，盗聴者にダミー信号が検知されても，埋込み信号自体を検知されないことである．その一方，正規者はダミー信号等で隠された埋込み信号から埋込み情報を誤りなく取り出せることである．

ここで，仮に埋込み信号の存在が推測されても，埋込み情報までは解読されないと，埋込み信号の存在が確認されたことにならない．そこで，埋込み情報が解読されないことも重要となる．このため，埋込みアルゴリズムが非公開の場合に，埋込みアルゴリズムが何らかの手法で解読されないことが必要である．一方，埋込みアルゴリズムが既知の場合に，埋込み情報の解読の攻撃に対して耐性をもつことが重要である．これには，埋込み情報の守秘のためステゴ鍵が有効に機能する必要がある．

3.4 無線信号秘匿におけるステゴ鍵

ステガノグラフィにおいて盗聴者に最も有利なステゴ解析である Known Stego Attack に対しても耐性を持たせるためには,ステゴ鍵の使用が必須である.ここでは,ステゴ鍵の共有法と用途について概説する.

3.4.1 ステゴ鍵の共有法

(1) 無線信号秘匿におけるステゴ鍵の特徴

ステゴグラフィにおけるステゴ鍵は,ディジタルの鍵で暗号鍵と同様な機能を持つものである.また,鍵の共有は,情報セキュリティ技術の一種である鍵配送の手法等で実現される.一方,無線信号秘匿における鍵は,埋込み情報の情報処理(例えば,暗号化)の他に,埋込み信号の信号処理に関するものが考えられる.後者の場合に,アナログ的な情報で信号処理を行うとすると,アナログ情報がステゴ鍵の機能を果たすことになる.また,無線信号秘匿の場合には,無線の特徴を生かした鍵共有法(例えば,電波伝搬特性を活用した鍵共有法)も選択肢である.

(2) ステゴ鍵の共有法

ディジタル鍵の共有法としては,従来からある鍵配送の手法を用いる方法,又は鍵情報を暗号化により伝送する方法がある.また,電波を用いた秘密鍵共有法や秘密情報伝送を用いる方法が考えられる.

アナログ鍵の共有は,一般の情報セキュリティ技術に不向きである.一方,電波を用いる秘密鍵共有では,ディジタル鍵を生成する前に共有されたアナログ情報からアナログ鍵が得られる.このアナログ秘密情報は,電波伝搬路の可逆性と場所依存性に基づいて取得することができる.なお,具体的なアナログ鍵(鍵の内容と取得方法)については,その用途に応じて個々に検討する必要がある.

3.4.2 ステゴ鍵の用途

ディジタルのステゴ鍵は,埋込み情報の情報処理,又は埋込み信号の信号処理に用いられる.

一方,アナログのステゴ鍵は,埋込み信号の信号処理に用いられる.また,ステゴ鍵の概念から多少離れるが,埋込み信号の埋込み区間を指定する情報の共有も場合により有効である.

(1) 埋込み情報の情報処理

ステゴ鍵を埋込み情報の情報処理に用いる簡単な例は,ステゴ鍵による埋込み情報の暗号化やスクランブルなどである.この他に,ステゴ鍵に基づく,①複数の情報処理アルゴリズムの選択,②情報処理の初期値の設定,③複数の情報処理パラメータの選択,などが考えられる.

(2) 埋込み信号の信号処理

ディジタルのステゴ鍵を埋込み信号の信号処理に用いる一例としては,スペクトル拡散変調における PN 符号の段数・種類の選択と初期値の設定がある.その他に,①複数の信号処理アルゴリズム(例えば,変調方式)の選択,②複数の信号処理パラメータの選択,などが考えられる.

一方,アナログのステゴ鍵を埋込み信号の信号処理に用いる一例としては,電波伝搬の伝送路歪みから抽出したアナログ情報を用いる,①送信側での伝送路歪みの事前補償,②受信側での伝送路歪み補償などが考えられる.

(3) 埋込み区間の選択

ステガノグラフィの場合と同様に,無線信号秘匿においても埋込み信号の埋込み区間が,第三者に不明であることが前提である.ここで,埋込み区間が秘密であってもそれの設定が固定されると,安全性が低下する懸念がある.そこで,埋込み区間を可変にすることが望ましいが,そのためには,正規者間で埋込み区間(一般に複数区間)の情報を共有・更新する必要がある.このような埋込み区間の選択は,上記の情報処理や信号処理と趣が異なり,むしろ無線信号秘匿システムの運用法である.そこで,このような運用法を不規則・間欠運用(仮称)と呼ぶことにする.この不規則・間欠運用により,各種の攻撃(ステゴ解析)が困難となることが予想される.なお,不規則・間欠運用により埋込み信号の有無が検知されないためには,埋込み信号のオン・オフを

行わず，埋込み情報をオン・オフしてオフ区間にダミー情報を送信する手法も考えられる．

不規則・間欠運用は，無線信号秘匿の安全性向上の効果的な手法と考えられるが，技術的な課題は正規者の送受信間で埋込み区間の情報を共有して，如何にタイミングの同期を取るかである．不規則・間欠運用を可能とする同期情報の共有法は，システム構成や電波伝搬特性などにも依存し，今後の個々に検討すべき課題である．

4．まとめ

無線信号秘匿の概念とその課題，システム構成と攻撃のモデル，無線信号秘匿のための所要条件などについて網羅的に検討した．特に，複数アンテナを用いた無線信号秘匿を提案し，ステゴ信号の検知を困難とする所要条件の実現が容易となることを示した．さらに，守秘のためのステゴ鍵の役割と機能について検討した．

本論文の対象外とした非線形な信号合成を用いた無線信号秘匿の検討は，今後の課題である．また，特定の無線信号秘匿方式を対象とし，具体的なステゴ解析や攻撃法を想定した場合の定量的な特性評価も今後の課題である．

参考文献

1) J. E. Hershey, A. A. Hassan and R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management”, *IEEE Trans. Communi.*, **43**, 3-6 (1995).

2) A. A. Hassan, W. E. Stark, J. E. Hershey and S. Chennakeshu, “Cryptographic Key Agreement for Mobile Radio”, *Digital Signal Processing*, **6**, 207-212 (1996).

3) H. Koorapaty, A. A. Hassan and S. Chennakeshu, “Secure Information Transmission for Mobile Radio”, *IEEE Communication Leters*, **4**, 52-55 (2000).

4) 笹岡秀一，“電波を用いた無線通信セキュリティ技術”，電子通信学会技術研究報告，WBS2010-**51**，31-36 (2011)．

5) 北野隆康，岩井誠人，笹岡秀一，“ディジタル移動通信における直移設拡散信号の埋込みによる無線ステガノグラフィ方式”，同志社大学理工学研究報告，**52**，127-134 (2011)．

6) 北野隆康，岩井誠人，笹岡秀一，“OFDM 移動通信における周波数拡散信号の埋込みによる無線ステガノグラフィ方式”，電子情報通信学会論文誌 B，**92**，2-10 (2009)．

7) 電子情報通信学会編，情報セキュリティハンドブック，（オーム社，東京，2004），pp. 255-267.

8) 松井甲子雄，岩切宗利，情報ハイディングの基礎，（森北出版，東京，2004），pp. 1-13.