Basic Study of Group Secret Key Agreement Based on Mobile Propagation Characteristics － Part I : Problems of the Conventional Method and Suggestion of New Method in Star Connection －

Hideichi SASAOKA and Hisato IWAI*

(Received October 10, 2019)

Wireless physical layer security attracts attention as a kind of the information security that utilized radio propagation characteristics. A lot of studies of secret key agreement are performed as the main field, but there are relatively few studies of group secret key agreement. This Paper gave an outline of conventional method based on mobile propagation characteristics for star connection systems and clarified a problem of the technique to notify of difference of the series of RSSI. Then, this paper suggested a method to acquire multiple group secret key using a notice of the EX-OR of the series of two binary RSSI to solve a problem. This paper also suggested a method to acquire multiple group secret key by the key distribution using the notice of the EX-OR with the series of binary RSSI and the binary random number. These suggestion methods show that the update of the secret key becomes easy by utilizing multiple group secret key.

Key words : physical layer security, secret key agreement, group secret key, mobile propagation characteristics

キーワード：物理層セキュリティ，秘密鍵共有，グループ秘密鍵，移動伝搬特性

移動伝搬特性に基づくグループ秘密鍵共有の初期検討 —（その１）星型接続における従来方式の課題と新方式の提案 —

笹岡　秀一，　岩井　誠人

１．はじめに

近年，移動通信など無線通信の普及・発展が目覚しく，最近では第五世代移動通信システムの導入が進められている．ここで，無線通信は開かれた空間を介して電波を送受信するため，盗聴や不正アクセスの対策が重要であり，共通鍵暗号や公開鍵暗号などの暗号を用いるのが一般的である．なお，移動通信の場合，端末での処理演算量の関係で共通鍵暗号を用いるのが一般的である．ここで，共通鍵暗号は，鍵管理や鍵配送が必要となることが課題である．さらに，無線通信において共通鍵暗号による複数端末への同報秘密通信の需要や共通鍵によるグループ認証の需要があり，グループ秘密鍵の管理や配送が重要となる．ここで，グループ秘密鍵の配送は，複数端末に同一鍵を配送することで容易に実現できる．

これらの計算量的な複雑性を安全性の根拠とする

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6267, Fax: +81-774-65-6267, E-mail: hisaiwai@mail.doshisha.ac.jp

一般的な暗号技術と異なり，情報理論的な複雑性を安全性の根拠とする暗号技術も研究されている．これらには，雑音のある通信路（盗聴通信路）を用いた秘密鍵配送 [1]，相関情報に基づく鍵抽出（鍵生成）と鍵一致処理等により同一の秘密鍵を取得する秘密鍵共有 [2,3]などがある．また，複数端末に対する秘密鍵容量が検討されている [4]．さらに，グループ秘密鍵の生成アルゴリズムの検討も行われている [5]．しかし，これらは理論的研究が多く，実用的なものは少ない．

一方，より実用的なものとして，移動通信などの電波伝搬路特性を用いた秘密鍵生成が提案されている [6,7]．この秘密鍵共有は相関情報に基づく手法の一種とも捉えられるが，無線物理層セキュリティにおける秘密鍵生成と位置づけられる [8]．また，電波伝搬の可逆性と場所依存性を活用した効率的な秘密鍵生成に特徴がある．すなわち，電波伝搬の可逆性により正規者間で相関性の高い秘密鍵を共有する一方，マルチパス伝搬の場所依存性により盗聴者の情報推定を阻止している [9]．ここで，マルチパス伝搬が生じる移動通信路においては，様々な電波伝搬特性が秘密鍵生成に用いられている．例として，マルチトーン信号の位相差 [6,7]，無線伝送路のインパルス応答 [10]，振幅周波数特性の時変化 [11]，受信信号強度の時変化 [12,13]などの電波伝搬特性を用いた秘密鍵生成がある．また，室内通信環境など伝搬特性の時間変化が少ない場合を対象として，マルチパス伝搬の到来方向の偏りとアレーアンテナの指向性パターン変動とを活用して発生させた人工フェージングの受信信号強度を用いた秘密鍵生成がある [14,15]．これら手法は，秘密鍵の取得と更新が無線物理層の処理で比較的容易となることが特長である．

これらの秘密鍵共有は，送受一対での共有を対象としており，双方向の電波伝搬特性の測定に基づいて秘密鍵（秘密鍵候補）を生成する．また，生成された秘密鍵が不一致の場合，公開通信路を介した情報交換による鍵不一致解消やプライバシー増幅など秘密鍵共有プロトコルに基づいて正味の秘密鍵が共有される [16]．一方，グループ秘密鍵の取得は，無線端末の組合せを変えて一対の秘密鍵共有を複数回実施し，次に共有された秘密鍵を用いて従来の暗号技術で同一秘密鍵を複数端末に配送すれば実現可能である．しかし，上記の手法と異なる無線通信の特徴を活用した簡易な手法も考えられる．具体的には，全無線端末において相関の高い秘密情報を生成し，鍵生成と鍵一致処理等によりグループ鍵共有を行う手法がある．

この一例として，受信電界強度表示 (RSSI: Received Signal Strength Indicator) の時系列(RSSI 系列)を用いたグループ秘密鍵生成がある [17]．この論文では，星型（スター）接続と鎖型（チェイン）接続に対して秘密鍵生成の手順を提示している．ここで，星型構成においては，中継端末と移動端末間で双方向の RSSI 系列を測定した後，基準端末と対象端末との RSSI 系列の差分値を中継端末から全移動端末に通知することで，各無線端末で共通の秘密情報を生成する [17]．その秘密情報からグループ秘密鍵生成を行っている．また，グループ秘密鍵共有が理想的に行われた場合のグループ秘密鍵容量の理論的評価を行っている．その結果，星型接続の場合に良好な秘密鍵容量が確保できることを示している．なお，グループ秘密鍵の安全性は，双方向の RSSI 系列の安全性を根拠としており，通知情報（RSSI 系列の差分値）を用いた盗聴者の攻撃を想定していない．

一方，上記のグループ秘密鍵生成 [17]に対して，RSSI 系列の差分値の和を用いた攻撃法が指摘され，盗聴者への情報漏洩により秘密鍵容量が大幅に低下することが示されている [18]．また，その対策としてアナログの差分値を通知する手法の替わりに，ディジタル化したビットの排他的論理を通知する手法が提案されている [18]．この改良方式は，盗聴者への情報漏洩が皆無となるため，秘密鍵容量の向上の可能性が示されている．しかし，グループ秘密鍵共有の手順とその結果得られるグループ秘密鍵容量の理論特性が示されていない．

本論文では，はじめに電波伝搬特性を用いた既存のグループ秘密鍵生成の概要とその課題を示す．次に，単一のグループ秘密鍵しか生成しない従来方式の課題を解決するために，複数のグループ秘密鍵を生成する方式を提案する．提案方式の一つは，双方

向の RSSI 系列の測定に基づいて一対の２値 RSSI 系列を複数生成した後で，２値 RSSI 系列の間の排他的論理和を複数端末へ通知することにより，複数のグループ秘密鍵を取得する手法である. 別の提案は，２値乱数と２値 RSSI 系列との排他的論理和の通知により，２値乱数と複数の秘密鍵をグループ秘密鍵として取得する手法である．これらの複数のグループ秘密鍵を取得する提案方式の概要とそのグループ鍵更新への応用を示すとともに，未実施の課題にも言及する．

２．従来のグループ秘密鍵共有の概要と課題

2.1 RSSI 系列の差分値の通知による従来方式

2.1.1 従来方式の概要

ここでは，電波伝搬特性を用いたグループ秘密鍵共有のうちで，中継端末と移動端末の星型接続を対象とし, RSSI 系列の差分値の通知を用いた方式 [17]の概要を説明する．

はじめに, Fig. 1 に示す中継端末 (Ryan) と二つの移動端末 (Alice, Bob) の構成に対して，移動端末間の秘密鍵生成の基本手順を示す [17]．基本手順では，はじめに双方向の RSSI 系列を測定する．次に，中継端末より移動端末 Bob に RSSI 系列の差分値を通知し，移動端末で秘密情報を取得した後で鍵抽出を行い，秘密鍵を生成する [17].

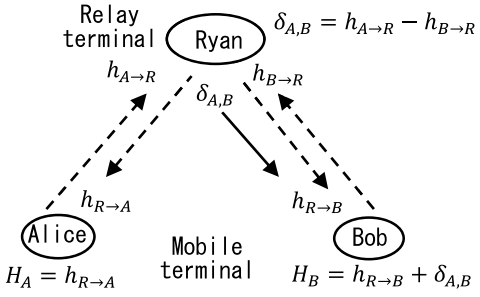

Fig. 1. Principal of secret key generation using relay terminal.

Fig. 1 において，測定された双方向の RSSI 系列 $h_{A\to R}, h_{R\to A}, h_{B\to R}, h_{R\to B}$ には，可逆性に起因する共通の RSSI 成分と雑音成分が含まれており，

$$\begin{aligned} h_{A\to R} &= h_A + n_{R,A} \quad h_{R\to A} = h_A + n_{A,R} \\ h_{B\to R} &= h_B + n_{R,B} \quad h_{R\to B} = h_B + n_{B,R} \end{aligned} \tag{1}$$

と表される．また，RSSI 系列の差分値 $\delta_{A,B}$ と移動端末で生成される秘密情報 H_A, H_B は，

$$\delta_{A,B} = h_A - h_B + n_{R,A} - n_{R,B} \tag{2}$$

$$\begin{aligned} H_A &= h_A + n_{A,R} \\ H_B &= h_A + n_{R,A} - n_{R,B} + n_{B,R} \end{aligned} \tag{3}$$

と表される．ここで，雑音成分が小さければ，十分に相関の高い秘密情報となる．また，この秘密情報に対して鍵抽出を行うと，鍵不一致が少ない秘密鍵を生成できる．ここで，秘密鍵が一致しない場合には，公開通信路を介した情報交換による鍵不一致解消とプライバシー増幅など秘密鍵共有プロトコルに基づいて正味の秘密鍵が共有される [16]．また，秘密鍵共有の処理が理想的に行われた場合の秘密鍵容量の理論式が示されている [2].

次に，この基本手順を単一の中継端末と多数移動端末間の星型接続に適用した場合のグループ鍵生成の手順 [17]を Fig. 2 に示す．図では RSSI 系列の測定の部分の表示を省略し, RSSI 系列の差分値の通知と秘密情報の取得を主に表示している．この秘密情報に対して鍵抽出を行い，秘密鍵を生成する．

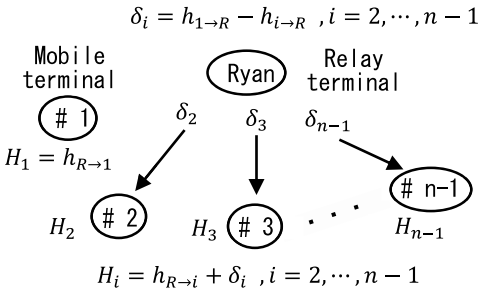

Fig. 2. System configuration of conventional group key generation via star connection.

次に，生成した複数の秘密鍵に対して，グループ秘密鍵共有プロトコルに基づいて正味の秘密鍵が共有される．ここで，この処理が理想的に実施された場合のグループ秘密鍵が理論検討されている [17]．その結果によると，グループ秘密鍵容量 S_{star} は，

$$S_{star} = \log\left\{1 + \frac{1/(n-1)}{(1+\gamma_m{}^{-1})^2 - 1}\right\} \tag{4}$$

と表される [17]．ここで，γ_m は伝送路の信号対雑音電力比である．

従来方式のグループ秘密鍵容量特性の評価は，理論式に基づいて行われている．しかし，具体的に秘密鍵を一致させる手法（秘密鍵共有の手法）は明記されていない．その結果，計算機シミュレーションによる特性評価がない．また，鍵不一致率特性等の実験結果が一部示されているのみである．

2.1.2 従来方式の課題

従来方式の課題の一つは，通知される RSSI 系列の差分値の傍受に伴う秘密鍵の盗聴の危険性が未検討であることである．これに対して，RSSI 系列の差分値 δ_i の傍受に基づく攻撃法が指摘されている [18]．その攻撃法では，RSSI 系列の差分値の和

$$D_\delta = \frac{1}{n-2}\sum_{i=2}^{n-1}\delta_i = h_{1\to R} - \frac{1}{n-2}\sum_{i=2}^{n-1}h_{R\to i} \quad (5)$$

を求める．次に，D_δ とその平均値 $\overline{D_\delta}$ との偏差を盗聴者が推定する秘密情報 H_E とすると，

$$H_E = h_{R\to 1} - \overline{h_{R\to 1}} + \frac{1}{n-2}\sum_{i=2}^{n-1}\left(h_{i\to R} - \overline{h_{\iota\to R}}\right) \quad (6)$$

となる．ここで，移動端末の数が増加するに従い，

$$H_E \cong h_{R\to 1} - \overline{h_{R\to 1}} \quad (7)$$

となることが示されている [18]．さらに，計算機シミュレーションの結果，盗聴者への秘密鍵情報の漏洩により秘密鍵容量が大幅に低下することが示されている [18]．

別の課題は，RSSI 系列の差分値の通知の仕方に関するものである．すなわち，Fig. 1 に示すように両方でなく一方に通知している．また，Fig. 2 に示すように一つの差分値を一つの移動端末にのみ通知している．この理由は，複数端末に通知して複数の秘密情報を生成しても，簡単な手法と安全性が同じであるとしている [18]．しかし，複数端末への通知により複数のグループ秘密鍵の取得できる利点が考慮されていない．

2.2 ディジタル化 RSSI 系列を用いた改良方式

2.2.1 改良方式の概要

上記の従来方式は，RSSI 系列の差分値 δ_i の傍受に基づく攻撃に脆弱であるが，その対策として改良方式が提案されている [18]．改良方式では，RSSI 系列を量子化・符号化し，符号化された RSSI 系列 $(\boldsymbol{h}^{\Delta}_{R\to i},\ \boldsymbol{h}^{\Delta}_{i\to R})$ のビットごとの排他的論理和 $\boldsymbol{\delta}^{\Delta}_i$ を求めて通知する．ここで，符号化ビット数を L とすると，

$$\boldsymbol{h}^{\Delta}_{R\to i} = \left(h^{(L)}_{R\to i}, h^{(L-1)}_{R\to i}, \cdots, h^{(0)}_{R\to i}\right) \quad (8)$$

$$\boldsymbol{h}^{\Delta}_{i\to R} = \left(h^{(L)}_{i\to R}, h^{(L-1)}_{i\to R}, \cdots, h^{(0)}_{i\to R}\right) \quad (9)$$

$$\begin{aligned}\boldsymbol{\delta}^{\Delta}_i &= \boldsymbol{h}^{\Delta}_{1\to R} \oplus \boldsymbol{h}^{\Delta}_{i\to R} \\ &= \left(h^{(L)}_{1\to R} \oplus h^{(L)}_{i\to R}, \cdots, h^{(0)}_{1\to R} \oplus h^{(0)}_{i\to R}\right)\end{aligned} \quad (10)$$

と表される．また，生成される秘密鍵は，

$$\boldsymbol{K}^{\Delta}_i = \boldsymbol{h}^{\Delta}_{R\to i} \oplus \boldsymbol{\delta}^{\Delta}_i \quad (11)$$

と表される [18]．この改良方式は，$\boldsymbol{\delta}^{\Delta}_i$ の傍受に基づく攻撃に耐性があることが示されている [18]．

改良方式の評価においては，従来方式と改良方式の比較に重点が置かれており，二つの端末間の鍵不一致率と秘密鍵容量の信号対雑音比に対する特性が計算機シミュレーションにより求められている．また，従来方式と比較して十分良好な特性であることが示されている [18]．

2.2.2 改良方式の課題

改良方式においては，中継端末と移動端末の対向での秘密鍵容量の理論式を検討しているが，正確なグループ秘密鍵容量の理論式の導出も行っていない．また，全端末で生成された秘密鍵に対して，鍵不一致解消アルゴリズムなどグループ秘密鍵共有プロトコルの検討を行っていない．このため，計算機シミュレーションによりグループ秘密鍵容量の評価が未着手となっている．

３．複数のグループ秘密鍵を取得する新方式

3.1 ２値 RSSI 系列を用いる新方式の概要

3.1.1 システムの構成とグループ秘密鍵の生成

提案方式は，RSSI 系列の差分値の代わりに符号化した RSSI 系列間のビットごとの排他的論理和を用いる方式に準じるが，その排他的論理和を全ての複数移動端末に通知する点が異なっている．また，移動端末の他に中継端末も含めてのグループ秘密鍵の取得を対象とする．なお，以下では説明の簡単化のために，符号化した多ビットの RSSI 系列でなく２値化した１ビット RSSI 系列（以後，２値 RSSI 系列と呼ぶ）を用いる．

はじめに，Fig. 3 に中継端末 (Ryan) と二つの移動端末 (Alice, Bob) の構成に対して，複数のグループ

秘密鍵を取得する基本手順を示す．図では，双方向の RSSI 系列の測定により一対の２値 RSSI 系列 $k_{A\to R}, k_{R\to A}$ および $k_{B\to R}, k_{R\to B}$ を生成し，２値 RSSI 系列の排他的論理和 X_{AB} を Alice と Bob 通知する．図に示すように $X_{AB} = k_{A\to R} \oplus k_{B\to R}$ である．また，Ryan, Alice, Bob で生成される秘密鍵 K_R, K_A, K_B は，

$$\begin{aligned} K_R &= (k_{A\to R}, k_{B\to R}) \\ K_A &= (k_{R\to A}, k_{R\to A} \oplus X_{AB}) \\ K_B &= (k_{R\to B} \oplus X_{AB}, k_{R\to B}) \end{aligned} \tag{12}$$

である．この秘密鍵は，鍵一致処理（鍵共有）を行う前の鍵であり，以下では秘密鍵候補と呼ぶ．

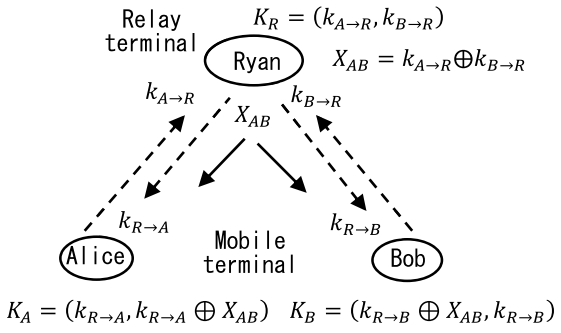

Fig. 3. Principal of new group key generation via star connection.

図に示す一対の２値 RSSI 系列には，雑音がない場合に中継端末と各移動端末との対向で取得される同一の秘密鍵（以下，個別秘密鍵と呼ぶ）k_A, k_B と雑音に起因する不一致成分 $d_{R,A}, d_{A,R}, d_{R,B}, d_{B,R}$ が含まれており，

$$\begin{aligned} k_{A\to R} &= k_A \oplus d_{R,A} \quad k_{R\to A} = k_A \oplus d_{A,R} \\ k_{B\to R} &= k_B \oplus d_{R,B} \quad k_{R\to B} = k_B \oplus d_{B,R} \end{aligned} \tag{13}$$

と表される．また，X_{AB} は，

$$X_{AB} = k_A \oplus k_B \oplus d_{R,A} \oplus d_{R,B} \tag{14}$$

と表される．さらに，各無線端末で生成される秘密鍵候補は，

$$\begin{aligned} K_R &= \left(k_A \oplus d_{R,A},\ k_B \oplus d_{R,B}\right) \\ K_A &= \left(k_A \oplus d_{A,R},\ k_A \oplus d_{A,R} \oplus d_{R,A} \oplus d_{R,B}\right) \\ K_B &= \left(k_B \oplus d_{B,R} \oplus d_{R,A} \oplus d_{R,B},\ k_B \oplus d_{B,R}\right) \end{aligned} \tag{15}$$

と表される．

ここで，一対の２値 RSSI 系列が個別秘密鍵に一致する場合，即ち，$d_{R,A} = d_{A,R} = d_{R,B} = d_{B,R} = 0$ となる場合には，

$$K_R = K_A = K_B = (k_A, k_B) \tag{16}$$

となり，複数のグループ秘密鍵が共有され．また，不一致成分がある場合にも，グループ秘密鍵に対して鍵不一致解消を行うと，グループ秘密鍵共有が行われる．このグループ秘密鍵共有は，対向の秘密鍵共有で得られる個別秘密鍵 (k_A, k_B) を全無線端末で共有することと捉えられる．

3.1.2 グループ秘密鍵の正味の秘密鍵容量

この方式では，個別秘密鍵 k_{A} と k_{B} がグループ秘密鍵となるので，X_{AB} の通知によりグループ秘密鍵容量が見かけ上で増加する．そこで，通知情報 X_{AB} を盗聴局が知った条件の下での正味の秘密鍵容量を検討する．ここで，簡単のために一対の２値 RSSI 系列に不一致成分がなく，個別秘密鍵に一致するとする．なお，既に述べたように一対の２値 RSSI 系列が不一致である場合には，秘密鍵共有の手順を用いてグループ秘密鍵共有を実現することになるが，以下では簡単のために，「なお，・・・」の記述を省略する．

この場合，式(16)が成り立つので条件付き相互情報量は，$I(K_{\mathrm{A}}; K_{\mathrm{B}}; K_R | X_{\mathrm{AB}}) = H(K_{\mathrm{A}} | X_{\mathrm{AB}})$ となり．さらに，

$$\begin{aligned} H(K_{\mathrm{A}} | X_{\mathrm{AB}}) &= H(k_{\mathrm{A}}, k_{\mathrm{B}} | X_{\mathrm{AB}}) \\ &= H(k_{\mathrm{B}} | X_{\mathrm{AB}}) + H(k_A | k_{\mathrm{B}}, X_{\mathrm{AB}}) \end{aligned} \tag{17}$$

となる．ここで，$k_{\mathrm{A}} = X_{AB} \oplus k_B$ が k_{B} と X_{AB} から一意的に決定されるため，$H(k_{\mathrm{A}} | k_{\mathrm{B}}, X_{\mathrm{AB}}) = 0$ となることを用いると，

$$H(K_A | X_{\mathrm{AB}}) = H(k_{\mathrm{B}} | X_{AB}) \le H(k_{\mathrm{B}}) \tag{18}$$

となる．式(18)と同様な式が k_{B} を k_{A} に置き換えても成り立つ．この結果をまとめると，

$$I(K_{\mathrm{A}}; K_{\mathrm{B}}; K_R | X_{\mathrm{AB}}) \le min\big(H(k_A), H(k_B)\big) \tag{19}$$

となる．式(18)から条件付き相互情報量の上限が，k_{A} と k_{B} のエントロピーの最小値で抑えられることが分かる．このため，k_{A} と k_{B} のエントロピーが最大となるように，(0,1)の発生頻度に偏りがないことが望ましい．以上から最終的な（単一の）グループ鍵共有は，k_{A} または k_{B} の個別秘密鍵を選択することで取得される．

3.2 複数のグループ秘密鍵への拡張と応用

3.2.1 多数移動端末への拡張

ここでは，複数とグループ秘密鍵を取得する手法の多数移動端末への拡張を示す．Fig. 4 に移動端末の数が３の場合の星型接続を示す．図において２値 RSSI 系列の表示を省略し，通知情報を主に表示している．ここで，通知情報は，

$$X_{AB} = k_{A\to R} \oplus k_{B\to R},\ X_{AC} = k_{B\to R} \oplus k_{C\to R} \tag{20}$$

と表される．また，各端末で生成される秘密鍵は，

$$\begin{aligned} K_R &= (k_{A\to R},\ k_{B\to R},\ k_{C\to R}) \\ K_A &= (k_{R\to A},\ k_{R\to A} \oplus X_{AB},\ k_{R\to A} \oplus X_{AC}) \\ K_B &= (k_{R\to B} \oplus X_{AB},\ k_{R\to B},\ k_{R\to B} \oplus X_{AB} \oplus X_{AC}) \\ K_C &= (k_{R\to C} \oplus X_{AC},\ k_{R\to C} \oplus X_{AB} \oplus X_{AC},\ k_{R\to C}) \end{aligned} \tag{21}$$

となる．ここで，一対の２値 RSSI 系列が個別秘密鍵に一致する場合には，

$$K_R = K_A = K_B = K_C = (k_A, k_B, k_C) \tag{22}$$

となり，３種類の個別秘密鍵が全無線端末で取得され，グループ秘密鍵となる．

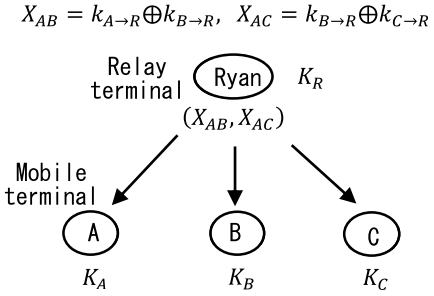

Fig. 4. System configuration of new group key generation via star connection in the case of three mobile terminals.

次に，グループ秘密鍵の正味の秘密鍵容量について検討する．一対の２値 RSSI 系列が個別秘密鍵に一致する場合，上記の 3.1.2 項と同様な導出に基づいて，条件付相互情報量は，

$$\begin{aligned} &\mathrm{I}(K_A; K_B; K_C; K_R | X_{AB}, X_{BC}) \\ &\quad \le min\big(H(k_A), H(k_B), H(k_C)\big) \end{aligned} \tag{23}$$

となる．式(23)は，式(19)を拡張したものである．

さらに，多数移動端末へ拡張した場合にも同様な手順でグループ秘密鍵共有が行える．

3.2.2 複数のグループ秘密鍵の取得の応用と利点

複数のグループ秘密鍵の取得の応用は，個々の秘密鍵の使い捨て使用を容易とすることである．従来方式では，グループ秘密鍵が単一であるので，安全性の維持等から秘密鍵を更新する場合，RSSI 系列の再測定が必要となる．しかし，提案方式では，複数のグループ秘密鍵を順次使用することで，RSSI 系列の再測定の頻度を軽減できる．

複数のグループ秘密鍵の取得の別の応用は，新規端末の追加や既存端末の排除などのグループ秘密鍵の更新を容易とすることである．はじめに，Fig. 5 に示すように，中継端末と移動端末 (A, B, C) に対してグループ秘密鍵の初期設定が完了した後で，新規端末 (G) が追加される場合を検討する．ここで，新規端末は通知情報 (X_{AB}, X_{AC}) を未知とする．新規端末と中継端末間で一対の２値 RSSI 系列を生成した後で，新たな通知情報 $X_{AG} = k_{A\to R} \oplus k_{G\to R}$ が全移動端末に通知される．ここで，一対の２値 RSSI 系列が個別秘密鍵と一致する場合には，

$$\begin{aligned} K_R = K_A = K_B = K_C &= (k_A, k_B, k_C, k_G) \\ K_G &= (k_{AR}, k_{GR}) \end{aligned} \tag{24}$$

となり，複数種類のグループ秘密鍵が取得される．式(24)から　個別秘密鍵 (k_{AR}, k_{GR}) を全無線端末のグループ秘密鍵として使用できる．

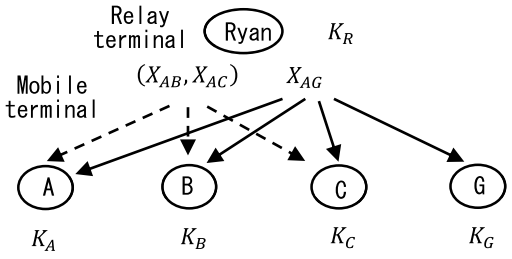

Fig. 5. Principle of the key setting for the new appearance mobile terminal in group secret key agreement.

次に，既存移動端末の排除を新規追加端末に対して行う場合，Fig. 5 で移動端末 (G) を例にとると，個別秘密鍵 (k_{BR}, k_{CR}) を使用することで，中継端末と移動端末 (A, B, C) 内でのグループ秘密鍵として使用できる．一方，初期の既存移動端末の排除は，その端末を排除した RSSI 系列の再測定が必要となる．

3.3 新方式の未実施の課題

上記では，複数のグループ秘密鍵を取得する新方式について，システム構成と複数のグループ秘密鍵生成の原理，多数移動端末への拡張，グループ秘密鍵の秘密鍵容量の上限，グループ秘密鍵の更新への応用，などについて示した．

しかし，秘密鍵容量の理論検討や計算機シミュレーションによる特性評価は未実施であり，今後の課題である．具体的には，一対の２値 RSSI 系列の鍵不一致率がグループ秘密鍵容量に関係しており，その部分の検討が必要となる．また，グループ秘密鍵容量の理論式の導出も必要となる．一方，グループ秘密鍵の共有において鍵不一致解消アルゴリズムの検討が必要である．また，この手法に基づいてグループ秘密鍵共有を実施することで，シミュレーションによるグループ秘密鍵容量特性の評価が可能となる．

４．秘密鍵配送を用いたグループ秘密鍵生成

4.1 秘密鍵配送によるグループ秘密鍵生成の概要

4.1.1 システム構成とグループ鍵生成の原理

はじめに，Fig. 6 に中継端末と二つの移動端末 (Alice, Bob) の構成に対して，２値乱数（秘密鍵）の配送によるグループ秘密鍵生成の基本手順を示す. 図において一対の２値 RSSI 系列の取得は, 3.1.1 項の Fig. 3 と同様である．次に，中継端末で２値乱数 g_R を発生させ，２値 RSSI 系列との排他的論理和 (X_A, X_B) を通知情報とする．また，各端末で生成される秘密鍵候補は,

$$\begin{aligned} K_R &= (g_R, k_{A\to R}, k_{B\to R}) \\ K_A &= (X_A \oplus k_{R\to A}, k_{R\to A}, X_A \oplus X_B \oplus k_{R\to A}) \\ K_B &= (X_B \oplus k_{R\to B}, X_A \oplus X_B \oplus k_{R\to B}, k_{R\to B}) \end{aligned} \tag{25}$$

となる．

ここで，一対の２値 RSSI 系列が個別秘密鍵と一致する場合には,

$$K_R = K_A = K_B = (g_R, k_A, k_B) \tag{26}$$

となり, グループ秘密鍵が取得される. この結果は, 通知情報の数が 3.1.1 項の Fig. 3 に比べて一つ増加して２となるが，中継端末で発生させた２値乱数 g_R の他に個別秘密鍵 k_A, k_B の計３種の秘密鍵を全端末で取得できることを示している．

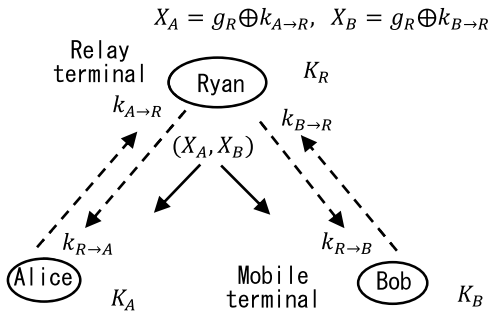

Fig. 6. Principle of group secret key agreement using the secret key distribution.

次に, 盗聴者が通知情報 (X_A, X_B) を知った条件の下での正味のグループ秘密鍵容量を求める．簡単のため，一対の２値 RSSI 系列が個別秘密鍵に一致する場合には, 式(25)が成り立つので, 条件付相互情報量が，$I(K_A; K_B; K_R | X_A, X_B) = H(K_A | X_A, X_B)$ となる．また，$X_A = g_R \oplus k_A, X_B = g_R \oplus k_B$ となる．この結果,

$$\begin{aligned} H(K_\mathrm{A} | X_\mathrm{A}, X_B) &= H(g_R, k_\mathrm{A}, k_\mathrm{B} | X_\mathrm{A}, X_B) \\ &= H(g_R | X_\mathrm{A}, X_B) + H(k_A, k_\mathrm{B} | X_\mathrm{A}, X_B, g_R) \end{aligned} \tag{27}$$

となる．ここで，X_A, X_B, g_R から k_A, k_B が，一意的に決定され，$H(k_A, k_\mathrm{B} | X_\mathrm{A}, X_B, g_R) = 0$ となることを用いると,

$$H(K_\mathrm{A} | X_\mathrm{A}, X_B) = H(g_R | X_\mathrm{A}, X_B) \le H(g_R) \tag{28}$$

となる．式(28)と同様な式が g_R を k_A, k_B に置き換えても成り立つ．この結果をまとめると,

$$\begin{aligned} &I(K_A; K_B; K_R | X_A, X_B) \\ &\quad \le min\big(H(k_A), H(k_B), H(g_R)\big) \end{aligned} \tag{29}$$

となる．

4.1.2 多数移動端末への拡張

秘密鍵の配送によるグループ秘密鍵生成の多数端末への拡張を検討する．Fig. 7 に移動端末の数が３の場合の星型接続を示す．図において２値 RSSI 系列の表示を省略し，通知情報を主に表示している．ここで，通知情報は,

$$\begin{aligned} &X_A = g_R \oplus k_{A\to R}, X_B = g_R \oplus k_{B\to R} \\ &X_C = g_R \oplus k_{C\to R} \end{aligned} \tag{30}$$

と表される．また，各端末で生成される秘密鍵候補

は，

$$K_R = (g_R, k_{AR}, k_{BR}, k_{CR})$$
$$k_A = (X_A \oplus k_{AR}, k_{AR}, X_A \oplus X_B \oplus k_{AR}, X_A \oplus X_C \oplus k_{AR})$$
$$k_B = (X_B \oplus k_{BR}, X_A \oplus X_B \oplus k_{BR}, k_{BR}, X_B \oplus X_C \oplus k_{BR})$$
$$k_C = (X_C \oplus k_{CR}, X_A \oplus X_C \oplus k_{CR}, X_B \oplus X_c \oplus k_{CR}, k_{CR}) \quad (31)$$

となる．

ここで，一対の２値 RSSI 系列が個別秘密鍵に一致する場合には，

$$K_R = K_A = K_B = K_C = (g_R, k_A, k_B, k_C) \quad (32)$$

となり，複数のグループ秘密鍵が取得される．式(32)は，式(25)の拡張である．また，グループ秘密鍵の正味の秘密鍵容量を示す条件付相互情報量は，

$$I(K_A; K_B; K_C; K_R | X_A, X_B, X_C) \leq min\big(H(k_A), H(k_B), H(k_C), H(g_R)\big) \quad (33)$$

となる．

さらに，多数移動端末に拡張した場合にも同様な手順でグループ秘密鍵の共有が行える．

$X_A = g_R \oplus k_{A\to R},\ X_B = g_R \oplus k_{B\to R}, X_C = g_R \oplus k_{C\to R}$

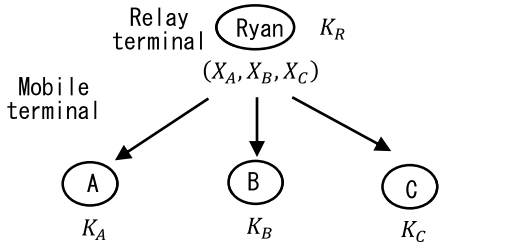

Fig. 7. System configuration of group secret key generation using the secret key distribution.

4.2 秘密鍵の配送による新方式の応用と利点

4.2.1 サブグループ化への応用

秘密鍵の配送によるグループ秘密鍵生成では，中継端末で秘密鍵（２値乱数）を発生させるが，２値乱数を複数使用することで，別々のグループ秘密鍵を共有する複数の移動端末のグループ（サブグループ）を形成できる．

二つのサブグループ (α, β) に対する秘密鍵の配送によるグループ秘密鍵生成の基本手順を Fig. 8 示す．はじめに，一対の２値 RSSI 系列を取得する．次に，中継端末で２種類の２値乱数 (g_α, g_β) を発生させ，各サブグループの２値 RSSI 系列との排他的論理和を通知情報とする．また，各端末で生成される秘密鍵は，

$$K_R = (g_\alpha, g_\beta, k_{\alpha1\to R}, k_{\alpha2\to R}, k_{\beta1\to R}, k_{\beta2\to R})$$
$$K_{\alpha1} = (X_{\alpha1} \oplus k_{R\to\alpha1}, k_{R\to\alpha1}, X_{\alpha1} \oplus X_{\alpha2} \oplus k_{R\to\alpha1})$$
$$K_{\alpha2} = (X_{\alpha2} \oplus k_{R\to\alpha2}, X_{\alpha1} \oplus X_{\alpha2} \oplus k_{R\to\alpha2}, k_{R\to\alpha2})$$
$$K_{\beta1} = (X_{\beta1} \oplus k_{R\to\beta1}, k_{R\to\beta1}, X_{\beta1} \oplus X_{\beta2} \oplus k_{R\to\beta1})$$
$$K_{\beta2} = (X_{\beta2} \oplus k_{R\to\beta2}, X_{\beta1} \oplus X_{\beta2} \oplus k_{R\to\beta2}, k_{R\to\beta2}) \quad (34)$$

である．

$X_{\alpha1} = g_\alpha \oplus k_{\alpha1\to R},\ X_{\alpha2} = g_\alpha \oplus k_{\alpha2\to R}$
$X_{\beta1} = g_\beta \oplus k_{\beta1\to R},\ X_{\beta2} = g_\beta \oplus k_{\beta2\to R}$

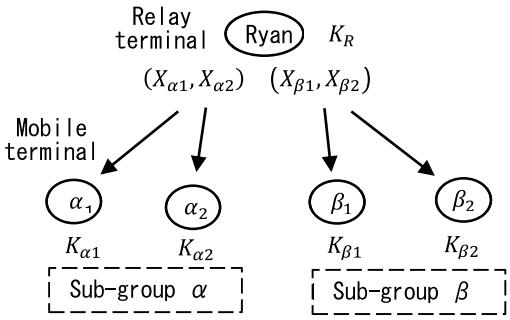

Fig. 8. Principal of sub-group secret key generation using the secret key distribution.

ここで，一対の２値 RSSI 系列が個別秘密鍵に一致する場合には，

$$K_R = (g_\alpha, g_\beta, k_{\alpha1}, k_{\alpha2}, k_{\beta1}, k_{\beta2})$$
$$K_{\alpha1} = K_{\alpha2} = (g_\alpha, k_{\alpha1}, k_{\alpha2}) \quad (35)$$
$$K_{\beta1} = K_{\beta2} = (g_\beta, k_{\beta1}, k_{\beta2})$$

となり，サブグループ秘密鍵が取得される．

次に，サブグループ秘密鍵のグループ外に対する秘密性を維持しながら，全グループに共通な秘密鍵を生成する手法を検討する．中継端末で２値乱数 g_0 を生成し，全グループに共通な秘密鍵とする．この秘密鍵を簡易に共有するには，通知情報 $(X_{\alpha0}, X_{\beta0})$ を，

$$X_{\alpha0} = g_0 \oplus g_\alpha, X_{\beta0} = g_0 \oplus g_\beta \quad (36)$$

とすればよい．しかし，この手法を用いると両方のサブグループ (α, β) で g_0 が取得されるため，容易に (g_α, g_β) が共有され，その結果として各サブ

グループ鍵も取得され,

$$K_R = K_{\alpha 1} = K_{\alpha 2} = K_{\beta 1} = K_{\beta 2} = (g_0, g_\alpha, g_\beta, k_{\alpha 1}, k_{\alpha 2}, k_{\beta 1}, k_{\beta 2}) \quad (37)$$

となる．このように，個々のサブグループ鍵の秘密性が維持できない.

この問題を解決する一方法は，式(36)において (g_α, g_β) をそのまま使用するのでなく，何らかの線形変換

$$X_{\alpha 0} = g_0 \oplus f_\alpha(g_\alpha), X_{\beta 0} = g_0 \oplus f_\beta(g_\beta) \quad (38)$$

を行うことである. また, 各サブグループにおいて, $f_\alpha(g_\alpha)$, $f_\beta(g_\beta)$ を作成し，g_0 を求める．ここで, $f_\alpha(g_\alpha)$, $f_\beta(g_\beta)$ が一方向性の変換であれば，サブグループαでは g_β を求めることが難しく，逆に，サブグループβでは g_α を求めることが難しい．このため，サブグループ秘密鍵の秘密性が維持できる.

4.2.2 グループ秘密鍵の更新

秘密鍵の配送によりグループ秘密鍵を生成する方式では，サブグループ毎に複数の秘密鍵を生成できるので，秘密鍵の更新のための RSSI 系列の再測定の頻度を低下できる．また，3.2.2 項に示す複数のグループ秘密鍵の生成の場合と同様に，新規端末の追加や既存端末の削除などのグループ秘密鍵の更新が容易である.

Fig. 7 の構成で, 新規端末 (G) の追加の場合には, 新規端末と中継端末間で一対の２値 RSSI 系列を生成した後で，$X_G = g_R \oplus k_{G \to R}$ を全移動端末に通知する．ここで, 一対の２値 RSSI 系列が個別秘密鍵に一致する場合には,

$$K_R = K_A = K_B = K_C = (g_R, k_A, k_B, k_C, k_G) \quad K_G = (g_R, k_G) \quad (39)$$

となる．式(39)から，新たなグループ秘密鍵である $K_G = (g_R, k_G)$ を全無線端末のグループ秘密鍵として使用できる.

次に，既存の移動端末の排除を新規追加の移動端末に対して行う場合，全無線端末のグループ秘密鍵 K_G の使用を取りやめ, 個別秘密鍵 (k_A, k_B, k_C) を使用することで，中継端末と移動端末 (A, B, C) 内でのグループ秘密鍵として使用できる．一方，初期の移動端末の排除の場合には，その端末を排除した RSSI 系列の再測定が必要となる.

一方，サブグループ化を行うことで，新規の移動端末の追加と既存の移動端末の排除が，サブグループ毎で行えるので，更新処理の対象となるサブグループが一部に限定される場合に，更新の利便性が向上する．たとえば，新規追加の移動端末を一括して新たなサブグループに収容すれば，新規追加の移動端末の排除が他のサブグループに影響を及ぼさないので，対応が容易となる．また，初期の移動端末の排除についても, 排除する移動端末数が少ない場合, 対象となるサブグループの移動端末に対してのみ RSSI 系列の再測定を実施すればよいので, 省力化が図れる.

4.3 未実施の課題

上記では, 秘密鍵の配送によりグループ秘密鍵を生成する方式について，システム構成とグループ秘密鍵生成の原理，多数移動端末への拡張，グループ秘密鍵の全体の秘密鍵容量の上限，サブグループ化とその応用，グループ秘密鍵の更新法，などについて示した.

しかし, 3.3 節に示したように秘密鍵容量の理論検討や計算機シミュレーションによる特性評価は未実施であり，今後の課題である.

５．まとめ

本論文では，電波伝搬特性を用いた既存のグループ秘密鍵生成方式として, 星型接続において RSSI 系列の差分値の通知による秘密鍵生成方式とディジタル化 RSSI 系列を用いた改良方式の概要を示すと共にその課題を明らかにした．また，単一のグループ秘密鍵しか生成しない従来方式の課題を解決するために, ２値 RSSI 系列の排他的論理和の通知を用い, 複数のグループ秘密鍵を取得する方式を提案した．また，別の方式として，秘密鍵の配送を用いて，複数のグループ秘密鍵を取得する方式を提案した．これらの提案方式の概要を示す共に，複数のグループ秘密鍵の活用の可能性を検討し，グループ秘密鍵の更新に利点があることを明らかにした．また，未検討な課題として，グループ秘密鍵の鍵不一致解消の手順の提示とシミュレーションによる特性評価があることに言及した.

グループ秘密鍵共有における鍵不一致解消の手順の検討は今後の課題である．また，今回は星型接続におけるグループ秘密鍵共有を対象としたが，鎖型接続におけるグループ秘密鍵共有の検討は今後の検討課題である．

参考文献

1) A. D. Wyner, “The Wired-tap Channel”, *Bell Sys. Tech. J.*, **54**, 1355-1387 (1975).
2) U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information”, *IEEE Trans. Inform. Theory*, **39**[3], 733-742 (1993).
3) U. M. Maurer, and S. Wolf, “Unconditional Secure Key Agreement and the Intrinsic Conditional Information”, *IEEE Trans. Inform. Theory*, **45**[2], 499-514 (1999).
4) I. Csiszar, and P. Narayan, “Secret Capacities for Multiple Terminals”, *IEEE Trans. Inform. Theory,* **50**[12], 3047-3061 (2004).
5) C. Ye, and A. Reznik, “Group Secret Key Generation Algorithms”, *Proc. IEEE Int’l Symp. Inform. Theory* (*ISIT*), 2596-2600 (2007).
6) J. E. Hershy, A. A. Hassan, and R. Yarlagadda, “Unconditional Cryptographic Keying Variable Management”, *IEEE Trans. Communi.*, **43**[1],3-6 (1995).
7) A. A. Hassan, W. E. Stark, J. E. Hershey, and S. Chennakeshu, “Cryptographic Key Agreement for Mobile Radio”, *Digital Signal Processing*, **6**, 207-212 (2000).
8) K. Zeng, “Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities”, *IEEE Comm. Magazine*, **53**[6],33-39 (2015).
9) 岩井誠人, 笹岡秀一, “電波伝搬特性を活用した秘密情報の伝送・共有技術”, 信学論(B), **90**[9], 770-783 (2007).
10) S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, “Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel”, *Proc. ACM MobiCom*, 128-139 (2008).
11) 北浦明人，笹岡秀一，“陸上移動通信における OFDM の伝送路特性に基づく秘密鍵共有方式”，信学論(A)，**87**[10]，1320-1328 (2004).
12) B. Azimi-sadjadi, A. Kiayias, A. Mercado, and B. Yener, “Robust Key Generation from Signal Envelopes in Wireless Networks”, *Proc. ACM conf. Computer and Comm. Security* (*CCS*), 401-410 (2007).
13) S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, “On Effectiveness of Secret Key Extraction from Wireless Signal Strength in Real Environment”, *Proc. ACM MobiCom*, 321-332 (2009).
14) 青野智之, 樋口啓介, 大平孝, 小宮山牧児, 笹岡秀一, “エスパアンテナを用いた IEEE802.15.4 無線秘密鍵共有システム”，信学論(B)，**88**[9]，1801-1812 (2005).
15) T. Aono, K. Higuchi, T. Ohira, T. Komiyama, and H. Sasaoka, “Wireless Secret Key Generation Exploiting Reactance-domain Scalar Response of Multipath Fading Channel”, *IEEE Trans. Antenna Propag.,* **53**[11], 3776-3784 (2005).
16) C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized Privacy Amplification”, *IEEE Trans. Inform. Theory*, **41**[6], 1915-1923 (1995).
17) H. L. J. Yang, Y. Wang, Y. Chen, and C. E. Koksal, “Group Secret Key Generation via Received Signal Strength: Protocols, Achievable Rates, and Implementation”, *IEEE Trans. Mobile Computing*, **13**[12], 2820-2835 (2014).
18) 黒柳啓太，笹岡秀一，岩井誠人，“RSSI 差分情報の通知によるグループ秘密鍵共有における盗聴により漏洩する情報量の評価”, 信学論(B), **102**[11], 1-9(2019).