

# Ban Logic を利用した MIS プロトコルの形式的セキュリティ解析

堀 良彰<sup>†</sup>

柳 壹善<sup>‡</sup>

櫻井 幸一<sup>†</sup>

<sup>†</sup>九州大学大学院システム情報科学研究院情報学部門

819-0395 福岡市西区元岡 744

財団法人九州先端科学技術研究所

814-0001 福岡市早良区百道浜 2 丁目 1-22 福岡 SRP センタービル 7 階

{hori, sakurai} AT inf.kyushu-u.ac.jp

<sup>‡</sup> 韓国聖書大 schools 情報科学部

大韓民國ソウル市蘆原区サンゲ洞

isyou AT bible.ac.kr

あらまし MIS プロトコルは、モバイル端末が基地局ルータと安全にかつ高速に接続を実現する目的でモバイルブロードバンド協会により策定された。MIS プロトコルは安全な無線 LAN アクセスプロトコルとして利用されている。本稿では、MIS プロトコルに対する形式的検証を試み、無線 LAN 環境における安全性について考察した。解析により、DoS 攻撃に対する脆弱性ならびにセッションキーの脆弱性を示し考察した。

## Formal Security Analysis with Ban Logic for MIS Protocols

Yoshiaki Hori<sup>†</sup>

Ilseun You<sup>‡</sup>

Kouichi Sakurai<sup>†</sup>

<sup>†</sup>Dept. of Informatics, Kyushu University

744 Motooka, Nishi-ku, Fukuoka 819-0395 Japan

Institute of Systems, Information Technologies and Nanotechnologies (ISIT)

Fukuoka SRP Center Building 7F, 2-1-22, Momochihama, Sawara-ku, Fukuoka, 814-0001, JAPAN

{hori, sakurai}@inf.kyushu-u.ac.jp

<sup>‡</sup>School of Information Science, Korean Bible University

205 Sanggye-Dong, Nowon-ku, Seoul, South Korea

isyou@bible.ac.kr

**Abstract** MIS protocol (MISP) and MISAUTH protocol were proposed by Mobile Broadband Association (MBA) in order to enable fast connection between a mobile node and a base router securely. Wireless LAN is one major application area of MISP and MISAUTH protocol can use for secure wireless LAN protocol. In this paper, we provide formal analysis of MISP in Wireless LAN environment and discuss its security. From the result of security analysis, we discuss about weakness the MIS protocols..

## 1 はじめに

無線 LAN における安全性と高速接続性を実現するために、モバイルブロード協会 (MBA: Mobile Broadband Association) では、MIS プロトコル [4] および MISAUTH プロトコル [5] の 2 つのセキュリティプロトコルを策定した。MIS プロトコル (MISP) は、モバイルノード ( $MN$ : Mobile Node) と基地局

ルータ ( $BR$ : Base Router) 間を接続するためのプロトコルであり、IP レイヤと接続メディア提供レイヤの間で機能する。一方、MISAUTH プロトコルは、 $BR$  が認証サーバ ( $AS$ : Authentication Server) と連携して、 $MN$  を認証するための機能を提供する。MIS プロトコルおよび MISAUTH プロトコルによって次の機能が提供される。(1) $BR$  から  $MN$  への接続情報広告。(2) $MN$  と  $BR$  との相互認証。

(3)  $MN$  と  $BR$  間のセッションキー共有。(4) 上位プロトコル層のための設定情報の交換。(5) パケットの認証と暗号化。これらの機能を提供するために、MISP では次の3つのセキュリティタイプを定義している。(1) NULL, (2) HMAC-MD5 / HMAC-MD5 / AES-CBC-128bit, (3) HMAC-MD5 / HMAC-MD5 / HMAC-MD5-128 bit である。2 番目のタイプは必須のものとされ、認証とセッションキー交換に HMAC-MD5 を利用し、データ暗号化に AES-CBC-128bit を使用するものである。これらの機能とセキュリティタイプにより、MISP は、無線 LAN 環境における中間者攻撃 (Man-in-the-middle)、偽基地局による攻撃、セッションハイジャック攻撃を防止することができる [6, 7]。さらに、MISP は  $MN$  と  $BR$  において、他の無線 LAN プロトコルと比較し、高速な接続確立を実現できる。それゆえ高速接続あるいはハンドオーバが必要なモバイル環境においては利点を有している。MISP のセキュリティおよびハンドオーバに関していくつかの研究が進められている [6, 7, 8]。文献 [7] では、IEEE802.11 と IEEE802.1X[2] を組み合わせたプロトコルと MISP を比較しており、ハンドオーバならびにセキュリティに関して MISP が優っていることを示している。文献 [6] では、セキュリティ機能に着目し、MISP の IEEE802.11i[3] との比較しながら定性的な解析を行っている。これらの研究では、MISP の形式的なセキュリティ解析は行われていない。形式的解析はセキュリティプロトコル自身の評価を厳密に行うためだけでなく、それらの欠点を解消するシステム設計ならびに新たなプロトコル設計のためにも重要である。

本稿では、BAN-logic により MISP を形式的に解析する。BAN-logic はよく知られた手法で、セキュリティプロトコルの検証に用いられる [9]。また、この解析結果により得られた脆弱性に関するの対抗手段について議論を行う。

本稿の構成は次の通りである。2 節では、MIS プロトコルの概要を述べる。3 節では、BAN-logic を用いたセキュリティ解析について述べる。最後の 4 節を本稿のまとめとする。

## 2 MIS プロトコル概要

MIS プロトコル (MISP) は、 $MN$ 、 $BR$  の 2 者間のプロトコルを定義している。MISP の主要目的は、 $MN$  と  $BR$  間において安全な通信を提供すること

である。このため、 $MN$  と  $BR$  は相互認証を実施する。特に、MISAUTH プロトコル [5] を合わせて用いることで、 $BR$  は  $MN$  の認証を  $AS$  に依存させることができるさらに、MISP は、 $MN$  および  $BR$  の 2 者間、暗号化および  $MN$  のパケットの認証のために安全にセッションキーを共有させる。本節では、本プロトコルの詳細を述べる。

### 2.1 記法と前提

図 1 に、本稿における記法を示す。各  $MN$  の利

|              |                                  |
|--------------|----------------------------------|
| $MN, BR, AS$ | モバイルノード, 基地局ルータ, 認証サーバ           |
| $secType$    | セキュリティタイプ, 認証・鍵配送・暗号化アルゴリズム      |
| $secTypes$   | セキュリティタイプのリスト                    |
| $H(M)$       | メッセージ $M$ の一方方向ハッシュ値             |
| $HMAC(K, M)$ | メッセージ $M$ , 鍵 $K$ により得られる HMAC 値 |
| $ID_X$       | $X$ の識別子                         |
| $P_{MN}$     | $MN$ 利用者のパスワード                   |
| $MA_X$       | $X$ の MAC アドレス                   |
| $K_{AB}$     | $AS$ と $BR$ の共有秘密鍵               |
| $SK$         | $MN$ と $BR$ のセッション鍵              |
| $lt$         | $SK$ の生存時間                       |
| $ts$         | タイムスタンプ                          |
| $ $          | 接続記号                             |
| $\oplus$     | 排他的論理和演算                         |

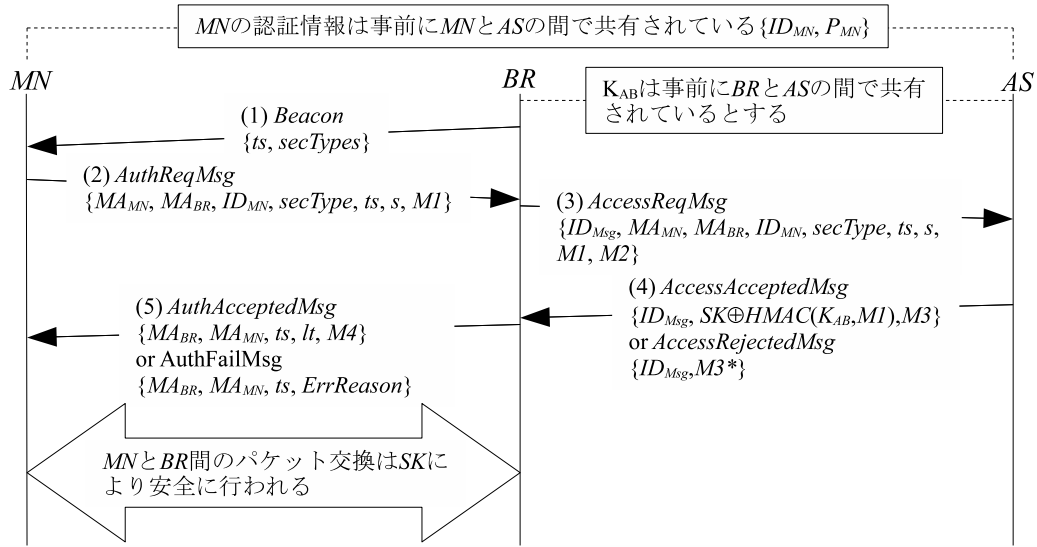
図 1: 記法

用者は、 $AS$  に登録されており、 $AS$  は利用者のアカウント情報である  $ID_{MN}$  および  $P_{MN}$  を安全に管理できていると仮定する。 $MN$  の識別子は  $ID_{MN}$  は、*Network Access Identifier (NAI)*[11] となっており、 $MN$  の認証において要求される。それゆえ、 $BR$  に代わり、 $AS$  は  $MN$  およびパスワード  $P_{MN}$  を検証する。この認証機能の実現のために、 $BR$  と  $AS$  は事前に共有秘密鍵  $K_{AB}$  を設定しておく必要がある。また、 $BR$  と  $AS$  間は RADIUS による通信を行う。それに加え、 $BR$  と  $AS$  との間では時刻同期がなされていると仮定する。

### 2.2 プロトコルシーケンス

MIS プロトコルと MISAUTH プロトコルを適用した際の  $MN$ 、 $BR$ 、 $AS$  の 3 者間のプロトコルを図 2 に示す。

- (1) 各  $BR$  は定期的に *Beacon* メッセージをブロードキャストにより送信する。 $MN$  は、チャンネルスキャンによりこれを受信する。もし  $MN$  が複数の  $BR$  からのビーコンメッセージを受



secTypeは次の3つうちいずれかである (2) は必須, 1), 2) はオプション )  
 1) Null, 2) HMAC-MD5/HMAC-MD5/AES-CBC-128bit, 3) HMAC-MD5/HMAC-MD5/HMAC-MD5-128bit  
 例) もし、2)が選択された場合、次のアルゴリズムが適用される。  
 (i) 認証: HMAC-MD5, (ii) セッション鍵配送: HMAC-MD5, (iii) 暗号化: AES-CBC-128bit  
 $ts$ : タイムスタンプ,  $ID_{Msg}$ : メッセージ識別子  
 $SK = HMAC(P_{MN}, s)$  (ここで  $s$  は MN によりランダムに生成されるシード)  
 $M1 = HMAC(P_{MN}, H(MA_{MN}|MA_{BR}|ID_{MN}|secType|ts|s)))$ ,  $H()$  は MD5 が用いられる  
 $M2 = HMAC(K_{AB}, MA_{MN}|MA_{BR}|ID_{MN}|secType|ts|s|M1)$   
 $M3 = HMAC(K_{AB}, ID_{Msg}|SK \oplus HMAC(K_{AB}, M1))$ ,  $M3^* = HMAC(K_{AB}, ID_{Msg})$   
 $M4 = HMAC(SK, H(MA_{BR}|MA_{MN}|ts|lt))$   
 $ErrReason$ : 認証失敗時の理由

図 2: MIS プロトコルおよび MISAUTH プロトコル

信した場合は、適当なひとつを選択する。MN は、*AuthReqMsg* メッセージ送出によってセッションを開始する。このメッセージを作成するために、MN はビーコンメッセージに格納されている有効なセキュリティタイプから希望のものを選択する。本稿では、MISPにおいて必須とされている type 2 (HMAC-MD5 / HMAC-MD5 / AES-CBC-128) を選択する場合について取り上げる。その後 MN はシード  $s$  ランダムに生成する。最後に、MN は  $M1$  を  $P_{MN}$  によって計算する。

- (2) *AuthReqMsg* メッセージ到着後 BR は最初に受信した  $ts$  がフレッシュであることを確認し、それが最新の *Beacon* メッセージに格納されたものと比較する。検証できた場合、共有秘密鍵  $K_{AB}$  を用いて  $M2$  を計算し、*AccessReqMsg* メッセージを AS に送る。検証できない場合は、*AuthFailMsg* メッセージが MN に返される。

- (3) *AccessReqMsg* メッセージ到着後 AS は本メッセージ中の  $ts$ 、 $M1$ 、 $M2$  を検証する。それらが検証できた場合、つまり MN が認証された場合、サーバはセッションキー  $SK$  を生成する。そして、それを  $HMAC(K_{AB}, M1)$  を用いて排他的論理和を取ることで暗号化する。最後に、AS は BR に対して  $M3$  で保護された *AccessAcceptedMsg* メッセージを送信する。MN が不正である場合、AS は BR に対して、 $M3$  で保護された *AccessRejectedMsg* メッセージを送出する。

- (4) *AccessAcceptedMsg* メッセージまたは *AccessRejectedMsg* メッセージが到着した時、BR は  $M3$  (または  $M3^*$ ) を検証する。 $M3$  が正当であれば、つまり MN が正当であれば、MN に *AuthSuccessMsg* メッセージが送られる。この目的のため、BR は  $K_{AB}$  を用いて  $SK$  を回復し、この鍵を利用して  $M4$  を計算する。同時に、 $SK$  の生存時間 (lifetime)  $lt$  を決定する。

もし、 $M3$  が不正であるか、 $M3^*$  が正当であるならば、 $AuthFailMsg$  は  $MN$  に送られる。

- (5)  $AuthSuccessMsg$  到着後、 $MN$  は  $SK$  を用いて  $M4$  を検証する。 $M4$  が有効であれば、認証は成功し  $BR$  との間で  $SK$  の共有が実施される。この点において、 $BR$  は  $MN$  によって認証される。その後、 $MN$  と  $BR$  間のセッションは  $SK$  によって認証および暗号化がおこなわれる。このセッションキーの生存期間  $lt$  が満了する前に、 $MN$  はセッションキーの更新を行う。

### 3 セキュリティ解析

本節では BAN-logic[9] を用いた MISP の形式的な解析について述べる。BAN-logic はこれまでにさまざまなセキュリティプロトコルの検証に採用されており、特にセキュリティプロトコルの脆弱性を発見するのに有用である。

#### 3.1 BAN-logic

BAN-logic は次のステップから構成されている [9]。(1) プロトコルの理想化 (idealization)。(2) 初期状態を仮定する。(3) プロトコルの各ステップ毎に推論を行い、結果を得るまで繰り返す。BAN-logic の記法とルールを図 3 および図 4 に示す。

|                                     |                                                   |
|-------------------------------------|---------------------------------------------------|
| $P \equiv X$                        | $P$ は $X$ を信じる                                    |
| $P \triangleleft X$                 | $P$ は $X$ を受け取った                                  |
| $P \vdash X$                        | $P$ はかつて $X$ を送った                                 |
| $P \models X$                       | $P$ は $X$ を宣言できる                                  |
| $\#(X)$                             | $X$ はfreshである                                     |
| $P \stackrel{K}{\leftrightarrow} Q$ | $P$ と $Q$ は共有鍵 $K$ で通信する                          |
| $\{X\}_K$                           | 鍵 $K$ で暗号化されている $X$                               |
| $+ \{M\}_K$                         | $= (M, \{H(M)\}_K)$<br>ここで $H(\cdot)$ は一方方向ハッシュ関数 |

図 3: BAN-logic の記法

BAN-logic では、HMAC(Hashed Message Authentication Code) または MAC(Message Authentication Code) 操作のための記法がない [10] ため、本稿では、HMAC 操作のために記法  $\{H(M)\}_K$  を用い

|                                                                                                                               |                                                                                                  |
|-------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| R1: Message-Meaning Rule<br>$\frac{P \equiv P \stackrel{K}{\leftrightarrow} Q, P \triangleleft \{X\}_K}{P \equiv Q \vdash X}$ | R2: Nonce-Verification Rule<br>$\frac{P \equiv \#(X), P \equiv Q \vdash X}{P \equiv Q \equiv X}$ |
| R3: Jurisdiction Rule<br>$\frac{P \equiv Q \models X, P \equiv Q \equiv X}{P \equiv X}$                                       | R4: Hash Rule<br>$\frac{P \equiv Q \vdash H(X), P \triangleleft X}{P \equiv Q \vdash X}$         |
| R5: Other Rules<br>$\frac{P \equiv \#(X)}{P \equiv \#(X, Y)} \quad \frac{P \equiv (X, Y)}{P \equiv X}$                        |                                                                                                  |

図 4: BAN-logic の基本ルール

る。HMAC の利用に関する拡張ルール E1 について図 5 に示す。

|                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| E1: Extended Rule<br>$\boxed{\frac{P \equiv P \stackrel{K}{\leftrightarrow} Q, P \triangleleft + \{H(M)\}_K}{P \equiv Q \vdash M}}$                                                                                                                                                             |
| Proof)<br>(i) $P \equiv P \stackrel{K}{\leftrightarrow} Q, P \triangleleft + \{H(M)\}_K$<br>(ii) $P \equiv P \stackrel{K}{\leftrightarrow} Q, P \triangleleft M, P \triangleleft \{H(M)\}_K$<br>(iii) $P \equiv Q \vdash H(M), P \triangleleft M$ [by R1]<br>(iv) $P \equiv Q \vdash M$ [by R4] |

図 5: HMAC のための BAN-logic 拡張ルール

#### 3.2 形式的解析

MISP の解析を行うにあたり、次のゴールを設定する。

- G1:  $BR \equiv MN \stackrel{SK}{\leftrightarrow} BR$   
G2:  $BR \equiv MN \equiv MN \stackrel{SK}{\leftrightarrow} BR$   
G3:  $MN \equiv MN \stackrel{SK}{\leftrightarrow} BR$   
G4:  $MN \equiv BR \equiv MN \stackrel{SK}{\leftrightarrow} BR$

これらは、 $MN$  と  $BR$  の双方が共有しているセッションキーについて信じているという状態を意味しており、これは  $MN$  と  $BR$  が相互に認証されていることを示す。それゆえ、もし、このゴール状態を満足できていれば、MISP により  $MN$  と  $BR$  間で相互認証が実現できセッションキーの交換が正しく行われたことを確認できる。

最初のステップとして、MISP を理想形に変換する (図 6)。理想形では、公開されている (秘密で

|                                                                                                                                                                                       |                          |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| (3-AccessReqMsg) $BR \rightarrow AS : +\{ID_{Msg}, +\{ts, MN \xleftrightarrow{SK} BR\}_{P_{MN}}\}_{K_{AB}}$                                                                           | * Authentication Success |
| (4-AccessAcceptedMsg) $AS \rightarrow BR : +\{ID_{Msg}, \#(MN \xleftrightarrow{SK} BR), MN \vdash MN \xleftrightarrow{SK} BR, \{ts, MN \xleftrightarrow{SK} BR\}_{K_{AB}}\}_{K_{AB}}$ |                          |
| (5-AuthSuccessMsg) $BR \rightarrow MN : +\{ts, MN \xleftrightarrow{SK} BR\}_{SK}$                                                                                                     |                          |
| (4-AccessRejectedMsg) $AS \rightarrow BR : +\{ID_{Msg}\}_{K_{AB}}$                                                                                                                    | * Authentication Fail    |

図 6: MIS プロトコルの理想形

ない) メッセージやいくつかの変数は本解析に影響しないため取り除かれている。また、認証要求メッセージ *AuthReqMsg* は削除している。アクセス許可メッセージ *AccessAcceptedMsg* の記述は *SK* がフレッシュであることと、それが一度だけ *MN* から送られたものであることも示している。これは、*AS* は *SK* を信じている場合のみメッセージを送ることによる。*AS* はシード *s* を使って *SK* を導出するため、*s* は *SK* で置き換えられている。

解析のために、次を仮定する。

- A1:  $AS \equiv AS \xleftrightarrow{K_{AB}} BR$
- A2:  $AS \equiv \#(ts)$
- A3:  $AS \equiv AS \xleftrightarrow{P_{MN}} MN$
- A4:  $BR \equiv AS \xleftrightarrow{K_{AB}} BR$
- A5:  $BR \equiv \#(ID_{Msg})$
- A6:  $BR \equiv AS \vdash MN \vdash MN \xleftrightarrow{SK} BR$
- A7:  $BR \equiv AS \vdash \#(MN \xleftrightarrow{SK} BR)$
- A8:  $BR \equiv \#(ts)$
- A9:  $BR \equiv AS \vdash MN \xleftrightarrow{SK} BR$
- A10:  $MN \equiv MN \xleftrightarrow{SK} BR$
- A11:  $MN \equiv \#(MN \xleftrightarrow{SK} BR)$
- \*H1:  $MN \equiv Beacon$
- H2:  $AS \equiv MN \vdash MN \xleftrightarrow{SK} BR$

厳密に言えば、*MN* はビーコンメッセージ *Beacon* を受信するのみであり、メッセージ中の情報を信用することはできない。すなわち、MISP はこの点においてそもそも問題がある。しかしながら、他のセキュリティ面の欠点を見つけるために、以下においては、*MN* は *Beacon* 中の情報を信じると仮定する (仮定 H1)。

理想形および仮定から、MISP の検証を試みる。(3-AccessReqMsg) より、次を導出する。

- (1a)  $AS \equiv BR \vdash (ID_{Msg}, +\{ts, MN \xleftrightarrow{SK} BR\}_{P_{MN}})$  [by A1, E1]
- (1b)  $AS \equiv \#(ID_{Msg}, +\{ts, MN \xleftrightarrow{SK} BR\}_{P_{MN}})$  [by A2, R5]
- (1c)  $AS \equiv BR \equiv (ID_{Msg}, +\{ts, MN \xleftrightarrow{SK} BR\}_{P_{MN}})$  [by (1a), (1b), R2]
- (1d)  $AS \equiv BR \equiv ID_{Msg}$  [by (1c), R5]
- (1e)  $AS \equiv MN \vdash (ts, MN \xleftrightarrow{SK} BR)$  [by A3, E1]
- (1f)  $AS \equiv \#(ts, MN \xleftrightarrow{SK} BR)$  [by A2, R5]
- (1g)  $AS \equiv MN \equiv (ts, MN \xleftrightarrow{SK} BR)$  [by (1e), (1f), R2]
- (1h)  $AS \equiv MN \equiv MN \xleftrightarrow{SK} BR$  [by (1g), R5]

(1d) により、*AS* は *AccessReqMsg* および *BR* を信頼することができる。また、(1g) は *AS* が *MN* の正当性を確信させる。しかしながら、(1g) から導出された (1h) は *AS* が、*MN* が *SK* を信じていることのみを信じていることを示す。この解析により、*AS* は、*MN* が *SK* を宣言できると信じる必要がある。

不幸なことに、たとえシード *s* がフレッシュであっても、保証がないため、*MN* は *SK* を宣言できるとはいえない。それゆえ、残りの解析においては、仮定として H2 を加え、次式を導出する。

- (1i)  $AS \equiv MN \xleftrightarrow{SK} BR$  [by (1h), H2, R3]

(4-AccessAcceptedMsg) から、次式を導出する。

- (2a)  $BR \equiv AS \equiv ID_{Msg}$  [by A4, E1, A5, R5, R2, R5]
- (2b)  $BR \equiv AS \equiv \#(MN \xleftrightarrow{SK} BR)$  [by A4, E1, A5, R5, R2, R5]
- (2c)  $BR \equiv AS \equiv MN \vdash MN \xleftrightarrow{SK} BR$  [by A4, E1, A5, R5, R2, R5]
- (2d)  $BR \equiv MN \vdash MN \xleftrightarrow{SK} BR$  [by (2c), A6, R3]
- (2e)  $BR \equiv \#(MN \xleftrightarrow{SK} BR)$  [by (2b), A7, R3]
- (2f)  $BR \equiv MN \equiv MN \xleftrightarrow{SK} BR$  [by (2d), (2e), R2]
- (2g)  $BR \equiv AS \equiv MN \xleftrightarrow{SK} BR$  [by A4, R1, A8, R5, R2, R5]
- (2h)  $BR \equiv MN \xleftrightarrow{SK} BR$  [by (2g), A9, R3]

(2a) により、*BR* は、*AccessAcceptedMsg* メッセージと *AS* を認証できる。また、(2f) と (2h) は、*BR* の *SK* を確かにし、ゴール G1 と G2 を満足する。

(5-AuthSuccessMsg) から、次式を導出する。

- (3a)  $MN \equiv BR \vdash (ts, MN \xleftrightarrow{SK} BR)$  [by A10, E1]  
 (3b)  $MN \equiv \#(ts, MN \xleftrightarrow{SK} BR)$  [by A11, R5]  
 (3c)  $MN \equiv BR \equiv MN \xleftrightarrow{SK} BR$  [by (3a), (3b), R2, R5]

(3b) により、 $MN$  は *AuthSuccessMsg* メッセージが正当で  $BR$  を信頼できることが保証される。さらに、(3c) は  $MN$  が  $BR$  が  $SK$  を信じていることを、信じさせることができる。これにより G4 を満足する。

まとめると、式 (2f),(2h),(3c) により、H1 および H2 が仮定できる場合に限り、MISP は先に挙げたゴールを満足することができる。言い方を換えれば、MISP は H1 ならびに H2 を保証しないところに問題がある。

$MN$  が認証に失敗した場合について考える。この場合、 $AS$  は *AccessAcceptedMsg* の代わりに *AccessRejectedMsg* を送信する。

(6-*AccessRejectedMsg*) より、

- (4a)  $BR \equiv AS \vdash ID_{Msg}$  [by A4, R1]  
 (4b)  $BR \equiv AS \equiv ID_{Msg}$  [by A5, R2]

(4b) より、 $BR$  は *AccessRejectedMsg* メッセージを認証する。また  $AS$  も同様である。これは、 $BR$  が *AuthFailMsg* メッセージ送出を引き起こす。しかしながら、メッセージは保護されていないため、 $MN$  はメッセージをができるだけであるそれゆえ、メッセージについての信頼がないためプロトコルは完了しない。これにより、認証が失敗した場合、MISP は正しくない。

## 4 まとめ

本稿では、高速認証を実現する MIS プロトコルについて無線 LAN 環境における安全性について形式的手法を用いて解析した。BAN-logic を適用することで、安全確保のための2つの条件を求めた。ひとつは、 $MN$  が  $BR$  のビーコンメッセージを信じることができる。もうひとつは、 $MN$  と  $BR$  間で秘密鍵が共有されていることを  $MN$  が宣言できそれを  $AS$  が信じれることである。この2つを仮定できた場合、 $BR$  と  $MN$  は安全に相互に認証され、秘密鍵を共有できる。実際のシステム実装においては、これらの2つの条件を仮定できるような実装が求められる。

## 謝辞

本研究は、日本学術振興会論博プログラムの支援を受けた。

## 参考文献

- [1] ANSI/IEEE Std 802.11, "Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.
- [2] IEEE Std 802.1X-2001, "Port-Based Network Access Control," 2001.
- [3] IEEE Std 802.11i-2004, "Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," July 2004.
- [4] Mobile Broadband Association, "MIS Protocol (MISP) Specification Ver. 1.02," MBA Standard 0201, <http://www.mbassoc.org>, April 2004.
- [5] Mobile Broadband Association, "MISAUTH Protocol Specifications Ver. 1.02," MBA Standard 0301, <http://www.mbassoc.org>, June 2004.
- [6] Y. Hori and K. Sakurai, "Security Analysis of MIS Protocol on Wireless LAN comparison with IEEE802.11i," Proceedings of the 3rd international conference on Mobile technology, applications & systems, ACM International Conference Proceeding Series, Vol. 270, Article No. 11, 2006.
- [7] H. Morioka, H. Mano, M. Ohmori, C. Jogakuen and M. Ohta, "MIS Protocol for Secure Connection and Fast Handover on Wireless LAN," the 20th International Conference on Advanced Information Networking and Applications, Vol. 1, pp. 533-540, April 2006.
- [8] K. Fujikawa, H. Nakano, M. Ohta, M. Hirabaru, H. Mano, K. Ikeda, "A Fast Authentication System for Secure Wireless Internet Services," IPSJ Technical Report, 2001-DPS-107, (March 2002) (in Japanese).
- [9] M. Burrows, M. Abadi and R. Needham, "A Logic of Authentication," ACM Trans. Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.
- [10] D. Trcek, "MAC Based Lightweight Protocols for Strong Authentication and Key Exchange," Journal of Information Science and Engineering, vol. 21, pp. 753-765, July 2005.
- [11] B. Aboba, M. Beadles "The Network Access Identifier," IETF RFC 2486, Jan. 1999.