7ZD-06

IoTデバイス向け相互認証プロトコルEGPのための制限時間付き認証を用いた防御方法

公文慧彪† 木村成伴‡

筑波大学情報学群情報メディア創成学類† 筑波大学システム情報系情報工学域‡

1. はじめに

RFID (Radio Frequency Identification)技術は高速，非接触で情報をやり取りすることができ，ノード発見の技術としても注目されている．しかし，RFIDタグとRFIDリーダ間にはセキュリティ，プライバシー上の問題がある．そこでタグとリーダ間の相互認証プロトコルが重要になっている．この相互認証プロトコルは，認証の際にタグ側で使用できる計算コストによって，次の4つに分類することができる[1]．

(1) 重量級：ハッシュ関数や公開鍵暗号など
(2) 中量級：一方向ハッシュ関数や擬似乱数生成器などを含めることができる．
(3) 軽量級：動作が軽い関数をサポートしており，巡回冗長検査や軽量の擬似乱数生成器などを含めることができる．
(4) 超軽量級：ビット単位の演算のみをサポートする．

本論文で対象としているEGP [2]は超軽量級に分類される．

2. EGP (Extremely Good Privacy) Protocol

本章では，EGPの認証セッションについて説明する．

まずEGPの第iセッションにおけるタグとリーダのメモリ構成は次のようになる．

タグ：$(ID, IDS_i, IDS_{i-1}, K_i, K_{i-1})$

リーダ：

$(ID, (IDS_i, IDS_{i-1}, \dots, IDS_{i-(r-1)}), (K_i, K_{i-1}, \dots, K_{i-(r-1)}))$

ここで，IDはタグのID，Kは秘密鍵，IDSはそのセッションにおける擬似IDとなる．これらの内，秘密情報はK,IDSを指す．次に，EGPの秘密情報の暗号化で用いられる関数$P_x(m,n)$の説明に入る．

n,mはそれぞれlビット長のビット列である．

$$m = m_1 m_2 \dots m_l$$
$$m_i \in \{0,1\} \quad i=1,2,\cdots,l$$
$$n = n_1 n_2 \dots n_l$$
$$n_i \in \{0,1\} \quad i=1,2,\cdots,l$$

$P_x(m,n)$はnに基づくmの置換を意味する関数である．

(1) まず$n_i = 0$であるとき，m_iにあるビットはm_lに置かれる．
(2) 次のサイクルでは，$n_{i+1} = 0$なら，m_{i+1}のビットはm_{l-1}に置かれる．
(3) この処理を繰り返すと，新たな文字列m^*が得られる．この新しい文字列m^*とnでXORを取ったものが$P_x(m,n)$となる．

図1はEGPの第iセッションにおける認証のプロセスを示したものである．

(1) まずリーダ側がタグに通信開始の合図としてHelloを送信する．
(2) タグはHelloを受信すると，リーダにそのセッションのIDSを返答として返す．
(3) リーダはIDSを受信すると，乱数n1,n2を生成し，A,B,Cそれぞれを計算し，それらを連結させてタグに送信する．
(4) タグはA,B,Cを受信後，P_xの逆関数を用いてA,Bからn1,n2を抽出し，C'を計算する．受信したCとC'が一致している場合，タグはリーダを認証する．ここでタグはIDS,Kを更新する．
(5) その後タグはリーダにDを送信し，リーダはこれを受信後，D'を計算し，D=D'の時タグを認証する．ここでリーダはIDS,Kを更新する．

3. EGPにおける問題点と提案方式

先行研究[3]では前節のプロセス中において非同期攻撃,秘密漏洩攻撃を受けることが指摘されている．

(1) 非同期攻撃

EGPにおいて「同期状態」とは，タグのメモリ構成のIDS_i, IDS_{i-1}のどちらかが(Kにおいても同様)リーダのメモリ構成に入っていることを指す．つまり，非同期攻撃とはタグのメモリに格納されているIDS,Kのどちらともがリーダのメモリに

Defense Method with Limited Time Authentication for Mutual Authentication Protocol EGP for IoT Devices
† Keita Kumon, College of Media Arts, Science and Technology, School of Informatics, University of Tsukuba
‡ Shigetomo Kimura, Institute of Systems and Information Engineering, University of Tsukuba

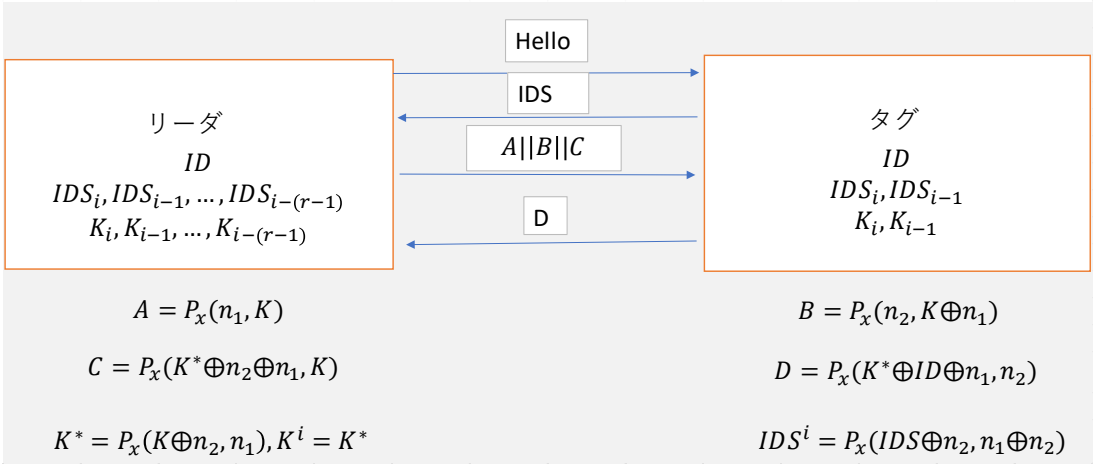

図 1 EGP の認証プロセス

格納されておらず，同期が取れない状態にされてしまい，認証ができなくなってしまうようになるという攻撃である．

(2) 秘密漏洩攻撃
秘密漏洩攻撃とは，EGP における秘密情報である IDS,K が攻撃者に漏洩してしまうことである．これらは攻撃者が各セッションの A,B,C,D を学習し，P_xの逆関数を用いて確率的に K が推定できてしまうということである．

これらの問題を踏まえて以下の方法を提案する．タグとリーダは事前共有秘密値として素数 p を有する．
(1) リーダはタグに Hello を送信する．
(2) タグは IDS を返す．
(3) リーダは素数 q を生成し，n=p*q を用いてメッセージ A',B'を作成し，タグに送信する．
(4) タグは A'から n を生成し，n を p で割った値が整数の時，B'を自身でも計算し送られてきたものと自身で計算したものが等しい場合はリーダを認証する．(4)ではタグの偽造防止のために制限時間を設ける．
(5) タグはリーダを認証後，C'を計算し，リーダへ送る．
(6) リーダはC'が届くと，自身でもC'を計算し等しい場合はタグを認証する．このときリーダは IDS,K を更新し，秘密情報の更新を知らせるメッセージ M をタグに送り，タグは受信後 IDS,K を更新する．

この提案方式によってまず IDS,K は両者の認証が完了した後に更新されるため，敵対者によって意図的に更新が阻害されるということがない．
また素因数分解を用いた認証を行うことによって認証メカニズムが悪意のあるものに知られていたとしても秘密情報の漏洩を防ぐことができる．

4. まとめ

本論文では，EGP プロトコルのセキュリティ上の問題を改善するため，素因数分解とセッションに制限時間を設けることを提案した．
但し，メッセージ A'，B'，C'，M は まだ暫定的なものなので，今後計算方法決定していく必要がある．共有秘密値 p はセッションによらず一定の値なので，時間経過に伴い，漏洩する恐れがあるので，定期的に更新するなどの対策が必要である．また，提案方式の計算量を評価し，実際の RFID タグで運用できるか，検証することも今後の課題とする．

参考文献

[1] **Christopher Bolan.** A Review of the Electronic Product Code Standards for RFID Technology. Proceedings of the Seventh International Network Conference (INC2008), pp. 171-178, 2008.
[2] **Madiha Khalid, Umar Mujahid , Najam-ul-Islam Muhammad.** Ultralightweight RFID Authentication Protocols for Low-Cost Passive RFID Tags. Security and Communication Networks, Vol. 2019, Article ID 3295616, Hindawi, 2019.
[3] **Amir Masoud Rahmani, Mokhtar Mohammadi and et. al,** Questioning the Security of Three Recent Authentication and Key Agreement Protocols. IEEE Access, Vol. 9, pp. 98204-98217, 2021.