通信方式の特性に応じた経路による秘密分散の実現法

1200306　小野田 祐稀　【 ネットワーク信号処理研究室 】

1　はじめに

ハウス農業では温度や湿度，土壌水分量などのセンサデータを集め，ネットワークを通じて遠隔地で分析をすることで農作業の効率化を図り，技術の継承に利用することができる．しかし，通信の際にデータを盗聴されると，その農家の栽培手法に関わる重要な情報が漏えいする危険性があるため，通信内容を秘匿化する必要がある．通信内容を秘匿化する方法として (k,n) しきい値秘密分散法が挙げられるが，実際に使用するネットワークの通信方式の特性に応じて，秘密分散をどのように実現するか考慮する必要がある．

本稿では，通信方式の 1 つである LoRa を使用したネットワーク環境を想定して，ネットワークの仕組みと，秘密分散によりシェアを作成するまでの実現法について示す．

2　LoRa を使用したネットワーク

LoRa を使用したネットワークの仕組みを示す．$k=3$,$n=5$ とした時，シェアを作成する送信元端末が 1 台と分散先となる受信端末が 5 台あり，それぞれの端末に個別の ID を設定する．LoRa を使用したネットワークでは，通信先の ID は 1 台までしか設定することができないので，1 対 n 通信を行う場合は通信先の ID の再設定を行い通信相手を変える必要がある．送信元端末は，受信したデータを $m$bit ずつ f 個に分割し，分割したデータそれぞれに対して (3,5) しきい値秘密分散を行うことで $f*5$ 個のシェアを作成する．シェア $w_{i,j}(i=1,2,\cdots,f,\ j=1,2,\cdots,5)$ の j の値と受信端末の ID を対応させ，受信端末へ 1 台につき f 個ずつ順に送信する．

3　秘密分散の演算方法

送信元端末が 128Byte のデータを受信したときの秘密分散の演算方法を示す．コンピュータは内部処理を 2 進数で行っていることを意識して，$GF(2^m)$ 上で演算を行う [1]．送信元端末が受信したデータを S とする．データを 4bit ずつ分割する場合，分割したデータを $S_i(i=1,2,\cdots,256)$ とする．S_i について (3,5) しきい値秘密分散をそれぞれ行う. 既約多項式を $p(x)=x^4+x+1$ として，解を α とする．これより $GF(2^4)$ の元のうち，0 を除く $\alpha^0,\alpha^1,\alpha^2,\cdots,\alpha^{14}$ の値を求める．$GF(2^4)$ の元 $-\{0\}$ の集合より異なる 5 個の元を選んだ $x=\{\alpha^0,\alpha^1,\alpha^2,\alpha^3,\alpha^4\}$ から $5*3$ の vandermonde 行列 X を作成する．この時，乗法は元 α^i と α^j の積が指数法則を用いて

$$\alpha^k * \alpha^l = \alpha^{k+l} \tag{1}$$

となることを利用して，$k+l$ を 2^m-1 で剰余をとることで計算結果を求める．

$$X=\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha^1 & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \\ 1 & \alpha^3 & \alpha^6 \\ 1 & \alpha^4 & \alpha^8 \end{pmatrix} \tag{2}$$

また，分割したデータ S_i と $GF(2^4)$ の元 $-\{0\}$ の集合よりランダムに 2 個の元を選んだ $R=\{r_{i,1},r_{i,2}\}$ よりベクトル a_i を作成する．この時，S_i はべき表現に変換する．

$$a_i=\begin{pmatrix} S_i \\ r_{i,1} \\ r_{i,2} \end{pmatrix} \tag{3}$$

そして，X と a_i の乗算より求まる値 $w_{i,1},w_{i,2},\cdots,w_{i,5}$ をシェアと呼ぶ．この時，加法はべき表現を 2 進数値に変換し，排他的論理和をとる．

$$Xa_i=\begin{pmatrix} S_i+r_{i,1}+r_{i,2} \\ S_i+\alpha^1*r_{i,1}+\alpha^2*r_{i,2} \\ S_i+\alpha^2*r_{i,1}+\alpha^4*r_{i,2} \\ S_i+\alpha^3*r_{i,1}+\alpha^6*r_{i,2} \\ S_i+\alpha^4*r_{i,1}+\alpha^8*r_{i,2} \end{pmatrix} = \begin{pmatrix} w_{i,1} \\ w_{i,2} \\ w_{i,3} \\ w_{i,4} \\ w_{i,5} \end{pmatrix} \tag{4}$$

4　まとめ

送信元端末が受信したデータを $m$bit ずつ分割し，$GF(2^m)$ 上で演算を行ってシェアを作成することで，CPU が扱えるデータサイズに配慮した計算処理ができる. そして，作成したシェアをどのように送受信するか，復元処理をどのように行うか考慮することで秘密分散の流れができる．また，第三者によってシェアが漏えいし改ざんされる可能性や，端末になりすまされる可能性など，実現法において問題が起こる条件及び解決法を考慮することで，ハウスから遠隔地までシェアを送受信するための安全な経路を確保することができる．

参考文献

[1] 嶋岡哲夫，”秘密分散における効率的かつ高速な計算処理”，平成 13 年度高知工科大学学士学位論文,Mar. 2002.