1X-08

軽量暗号と秘密分散によるデータ共有方式

小林聖哉† 宮崎敏明†

†会津大学コンピュータ理工学部

1. はじめに

近年、センサや医療機器などの IoT デバイスの利活用が急速に進んでいる。それに伴って、ハードウェアリソースが限られた IoT デバイスにおけるセキュリティ対策の研究も盛んになってきた。IoT デバイスでは、メモリ使用量や消費電力を抑えつつデータを保護することが求められる。本稿では、センサなどの IoT デバイスのデータを集約する中継サーバ（エッジノード）を分散配置し、IoT デバイスと中継サーバ間の通信を軽量暗号で、かつ、中継ノード同士の通信を秘密分散法で保護し、しかも複数の経路を用いてデータを送ることで、広域に分散配置された IoT デバイスの軽量かつ安全なデータ共有方式を提案する。

2. 提案システム

図 1 に提案システムの概要を示す。提案システムは、総計N台の中継サーバ集合$\{1,\cdots,N\}$からなり、それらは互いにネットワークで接続されている。そのうちの 1 つの中継サーバを$x|1 \le x \le N$とする。個々の中継サーバは、近傍の IoT デバイス（以下、単にデバイス）からのデータを集約し、データを送信・受信できる 1 つのエンドユーザとして振る舞う。また、他中継サーバを経由して、自分の配下のデバイスへ要求されたデータを、そのデータを要求したエンドユーザに送信する役割を担う。例えば、図 1 において、右端のエンドユーザが中継サーバxにデータ取得要求を発すると、その要求を受信した中継サーバxは、データを持つデバイスに要求を出し、当該データを受け取る。この時、対象デバイスと中継サーバx間の通信は、後述する軽量暗号を用いて保護する。データを受け取った中継サーバxは秘密分散法を用いて当該データを分割し、複数経路を用いて、エンドユーザにデータを届ける。詳細を以下に述べる。

2.1. 軽量暗号の適用

ハードウェアリソースが限られたデバイスに従来の暗号化アルゴリズムを適用すると、その処理が重いために、本来のデバイス動作に支障をきたす可能性があり、望ましくない。近年、そのようなデバイスに適用可能な、より低コストで高速な軽量暗号法が研究されている[1]。本稿では、軽量暗号法の 1 つである SPECK 暗号[2]を適用する。SPECK 暗号は、RFID (Radio Frequency Identification)などメモリサイズが小さいデバイスにも実装可能で動作が高速であり、しかも、使用できるメモリが限られていても性能低下が小さいことが知られている共通鍵を用いた軽量暗号方式である。デバイスは、通信に際しエンドユーザと共通鍵を共有する必要がある。ここでは、共有鍵は既存プロトコルを用いて事前に共有されていると仮定する。デバイスは、その共通鍵を用いてデータを暗号化し、最寄りの中継サーバへ送る。データを受け取った中継サーバは、次に示す秘密分散法による複数経路配送法を用いて当該データを、それを要求したエンドユーザに配送する。

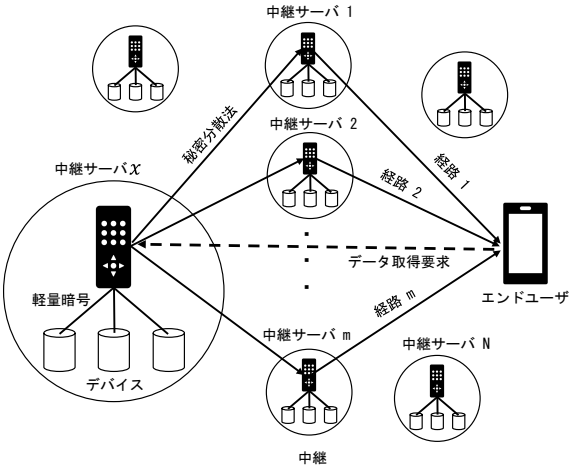

図1 提案システム

2.2. 秘密分散法による複数経路配送

中継サーバ間のデータ配送には、シャミアの秘密分散法[4][5]を用いる。秘密分散法では、データをm個のシェアと呼ぶ部分データに分割し、そのうちのk個（このkを閾値と呼ぶ）以上のシェアを得れば元のデータが復元できる。換言すれば、$k-1$個以下のシェアからは元のデータを復元できない。このシャミアの秘密分散法を適用することで、データ送信時に悪意のある攻撃者から通信を盗聴されデータを復元されることを困難にする。

Data sharing using lightweight encryption and secret sharing scheme
Seiya Kobayashi†, and Toshiaki Miyazaki†
†School of Computer Science and Engineering, The University of Aizu

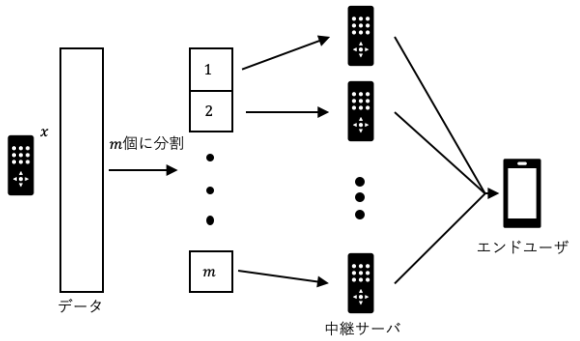

図2 複数経路を用いた秘密分散通信

次に、中継サーバxからエンドユーザへの通信方法を図 2 に示す。中継サーバxは、軽量暗号化後のデータを、シャミアの秘密分散法を用いて、適当な閾値kを定め、m個のシェアに分割する。次に N個の中継サーバからm個を選び、各中継サーバにシェアとエンドユーザの情報を送信する。分割されたデータを受信した中継サーバはデータをエンドユーザに送信する。なお、中継サーバxからエンドユーザに至る各経路の形成は、別途行うものとする。上述したように、複数経路を経由してデータを送ることで、複数の経路を監視しなければデータを復元することは困難となり、悪意のある攻撃者からデータを守ることができる。

3. 実験・評価

本システムでは、中継サーバがデバイスから受け取った軽量暗号化後のデータを復号する必要がないので、デバイスと中継サーバ間の通信に関しては SPECK 暗号単体の性能に依存する。文献[1]によれば、SPECK 暗号は、最も普及している共通鍵暗号アルゴリズム AES より処理量が小さいため、消費電力を抑えることができ、しかも、他の軽量暗号に比べて少ないメモリサイズ（最小 ROM サイズ 71 バイト）で実装が可能である。また、文献[3]によれば、2018 年 1 月時点で約 70 の論文で SPECK 軽量暗号の安全性についての議論がなされているが、決定的な攻撃法は見つかっていない。

次に、中継サーバxからエンドユーザへの秘密分散法を用いた通信をネットワークシミュレータ ns-3[6]を用いて評価した。ここでは、全体の中継ノード数Nを$N = 16$、各経路のデータ転送速度(10 MB/s)、その伝播遅延(10 ms)、および元データサイズ(10 MB)を固定した。また、どの経路も、１つの中継ノードを経由してエンドユーザに接続されているとした。経路数はシェア数mと同じとし、さらに閾値kも$k = m$として、経路数を変えながら、全データをエンドユーザが受信しデータを復号できるまでの時間を評価した。加えて、当該中継サーバとエンドユーザが直接通信した場合

表1 評価結果

経路数(=シェア数) m	閾値 k	送信時間(ms)
0	−	1771
2	2	1793
4	4	1822
8	8	1860
16	16	1897

（経由する中継ノード数を０個とした場合）の、遅延も参考として計測した。表１に評価結果を示す。シャミアの秘密分散法では、シェア数mが増えると、各シェアを合計したサイズは元データのサイズより大きくなり復号にかかる時間も増える。そのため、表１から分かるように、シェア数mの増加に伴い元データ全体の送信時間は大きくなる。しかし、その増加量は、$m = 16$でも、秘密分散通信を使用しない場合($m = 0$)に比べ、126ms であり、エンドユーザに大きな負荷をかけることなく秘密分散法によるデータの保護が可能なことがわかる。さらに、シェアに分割された１つ１つのデータは元のデータサイズより小さいため、それぞれの経路にかかる負担は小さくなる利点がある。

4. おわりに

IoT ネットワークにおいて、軽量暗号 SPECK とシャミアの秘密分散法を用いたデータ共有方式を提案した。本提案方式では、軽量暗号と秘密分散法によるデータの二重保護と、データ配送時に複数の経路を用いて配送することで、通信の盗聴によるデータ漏洩のリスクを軽減し、かつ、各経路への負担を減らすことができる。

今後は、各中継サーバの負荷状況を加味した配送経路決定法の開発と、実機 IoT エッジノードへの実装を目指す。

謝辞

本研究の一部は、総務省戦略的情報通信研究開発推進制度（SCOPE No.162302008）の支援を受けて実施したものである。

参考文献

[1] “CRYPTREC 暗号技術ガイドライン（軽量暗号）,” http://www.cryptrec.go.jp/report/cryptrec-gl-0001-2016-j.pdf
[2] R. Beaulieu, S. Treatman-Clark, D. Shors, B. Weeks, J. Smith, and L. Wingers, "The SIMON and SPECK lightweight block ciphers," IEEE 52nd ACM/EDAC/IEEE Design Automation Conference (DAC), 2015. DOI: 10.1145/2744769.2747946
[3] R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, “Notes on the design and analysis of Simon and Speck”, 2018-1-19, https://eprint.iacr.org/2017/560.pdf
[4] A. Shamir, “How to share a secret,” Communications of the ACM,vo. 22, no. 11, pp. 612-613, 1979. DOI: 10.1145/359168.359176
[5] 保坂範和, 多田美奈子, 加藤岳久, “秘密分散法とその応用,” 東芝レビュー, vol. 62, no. 7, pp.23-26, 2007.
[6] “ns-3 Network Simulator,” https://www.nsnam.org/