Form 3

Abstract of Thesis

Name (EI KHAING WIN)	
Title	Study on Reliable and Secure Multi-receiver Data Delivery for Internet of Things (Internet of Things のための高信頼かつ安全なデータ同報配信手法に関する研究)

Abstract of Thesis

In the emerging Internet of Things (IoT) technology, the sensors take an essential role in sensing and monitoring. To make IoT applications more responsive and solve some privacy constraints, the sensed data are stored, processed, and analyzed at the edge of the network instead of the cloud servers. For example, in healthcare applications, the body sensor data of a patient must be analyzed on the smartphone of a caregiver instead of a cloud server to give point-of-care efficiently. Furthermore, the sensed data are delivered to multiple receivers as continuous stream data in general. For example, the body sensor data of a patient are delivered to doctor, nurse, and other caregivers continuously for different kind of cares. One important issue to be treated in such data delivery is how to recover data losses for the reasons of unstable communications, insufficient processing powers, and so on. The existing data stream recovery schemes increase the communication loads on the sender or storage usages on the receivers though most of the edge devices have limited network bandwidth or storage. The other issue is the protection of sensitive data such as heartbeat data or location data in the healthcare applications from leakage to unintended receivers or malicious attackers. Though there exist multi-receiver encryption schemes for the data protection, they do not consider some security properties, which are necessary for IoT applications such as source authentication and replay attack prevention. Moreover, the existing schemes require high computational cost, which is not suitable for resource-constrained edge devices.

To achieve reliable and secure multi-receiver data delivery for IoT, this thesis proposes a novel recovery stream delivery scheme and multi-receiver encryption scheme for treating these issues.

This thesis consists of five chapters. Chapter 1 explains the research background, research issues, objectives and the content of this research.

Chapter 2 proposes a synchronized recovery stream merging (SRSM) scheme which focuses on the sensor data stream multicast delivery that can recover lost data. Two methods of the SRSM scheme for IoT applications are proposed in this chapter. The first one is latency-aware synchronized recovery stream merging (SRSM-L) method, which is suitable for applications that can tolerate some latency to fetch the lost data. The second one is bandwidth dependent synchronized recovery stream merging (SRSM-B) method, which is suitable for IoT applications where the senders have limited network bandwidth. The proposed methods reduce the total bandwidth required by the sender without requiring large buffer storage on receivers.

Chapter 3 proposes a lightweight certificate-less multi-receiver encryption scheme to cope with the data protection issue. The proposed scheme avoids pairing operations that introduce high computational costs to achieve multi-receiver encryption with source authentication and replay attack prevention. Compared with the existing schemes, the proposed scheme is better regarding computational cost and security properties.

Chapter 4 describes a combined design and implementation of the schemes proposed in Chapter 2 and 3. An extension of the SRSM scheme with a limited number of receivers (SRSM-R) method is proposed to reduce key renewal computation cost, which is inevitable to encrypt sensor data stream in the SRSM scheme when there are access policy changes. Although there is a trade-off between the key renewal time and the bandwidth usage, the simulation experiments showed that the key renewal time could be reduced with smaller additional bandwidth in the SRSM-R method.

Finally, the conclusion and the future work of the research are described in Chapter 5.

様式 7

論文審査の結果の要旨及び担当者

氏　名　（　EI KHAING WIN　）		
	（職）	氏　名
論文審査担当者	主 査　教授	下條　真司
	副 査　教授	藤原　融
	副 査　教授	鬼塚　真
	副 査　教授	原　隆浩
	副 査　教授	松下　康之

論文審査の結果の要旨

提出された論文では、IoTのための重要な課題である高信頼かつ安全なデータ同報配信を達成するために，回復ストリーム配信方式と同報暗号方式を新たに提案している。IoT環境において、健康管理や介助行為のように即応性が求められる場合、ネットワークの末端（エッジ）にあって通信経路が短い計算機を活用することが考えられる。さらに、IoT環境においてセンシングされたデータは、連続的なデータ（ストリームデータ）として複数の受信者に配信されことがある。既存の方式では、多くの計算資源や通信資源が必要でIoTに不向きであった。本論文では、IoTのこれらの特徴に着目し、以下の研究成果について述べている。

主な成果としては、まず、通信失敗や処理能力不足などの理由により欠損したデータを回復するセンサデータストリーム同報配信方式であるSynchronized Recovery Stream Merging (SRSM)方式を考案し、IoT環境に応じた2種類の手法を提案している。一つは欠損データの回復に遅れを許容できる場合に適しているLatency-aware Synchronized Recovery Stream Merging (SRSM-L)手法である。二つめは送信側のネットワーク帯域が制限されている場合に適しているBandwidth dependent Synchronized Recovery Stream Merging (SRSM-B)手法である。シミュレーションにより、これらの提案手法が受信側に必要なバッファ容量を抑えつつ送信側に求められるネットワーク帯域を削減できることを示している。

さらに、機密データを意図しない受信者や悪意のある攻撃者から保護するデータ保護の課題に対して、低負荷な非証明書同報暗号方式を提案している。提案方式では、配信元認証と反射攻撃防止が可能な同報暗号を低負荷に実現するためにペアリング操作を省略している。既存方式と比べて提案方式は計算負荷とセキュリティ特性の面で優れていることを示している。また、上記のSRSM方式と非証明書同報暗号方式を統合した方式の設計と実装を行っている。統合に伴って、アクセスポリシーが変化すると求められる鍵更新負荷を軽減するSRSM scheme with a limited number of Receivers (SRSM-R)手法へとSRSM方式を拡張している。鍵更新時間と利用するネットワーク帯域の間にトレードオフがあるものの、SRSM-R手法では利用ネットワーク帯域の増加を抑えて鍵更新時間を削減できることをシミュレーション実験で確認している。

本論文は、IoTのための重要な課題である高信頼かつ安全なデータ同報配信を達成するために、回復ストリーム配信方式と同報暗号方式を新たに提案し、実験とシミュレーションによりそれらが有効であることを示している。IoT環境におけるデータ同報配信技術の向上に大きく貢献し、重要な成果を挙げた研究として、情報科学に寄与するところが大きい。よって、本論文は博士（情報科学）の学位論文として価値のあるものと認める。