Secure Critical Data Reclamation Scheme for Isolated Clusters in IoT enabled WSN

Ata Ullah, Muhammad Azeem, Humaira Ashraf, NZ Jhanjhi, Lewis Nkenyereye*, Mamoona Humayun

Abstract—**Internet of Things (IoT) comprises of a huge number of connected devices that can communicate within the same network and across the networks. IoT enabled Wireless Sensor Networks (WSN) are getting growing interest due to its wide applicability in healthcare, patient monitoring, transportation, and surveillance. The main issue is that the network is mostly deployed in hostile environments where an attacker may physically destroy the CHs or other technical fault may occur. It isolates the cluster and causes loss of sensitive data from that region. This paper presents a Critical Data Reclamation (CDR) protocol that provides secure data transmission for isolated clusters. We present the data transfer, data aggregation algorithms for sensing nodes and data receiving and extraction at CH and sink. We performed extensive simulations using NS-2.35. Results prove the dominance of CDR in contrast to counterparts in terms of communication cost, energy consumption, and resilience.**

Keywords: Data aggregation, Gateway node, Inter-cluster keying, WSN, Internet of Things

I. Introduction

In IoT enabled Wireless Sensor Networks (WSN), number of low energy ordinary smart wireless devices can communicate with other devices and scope of these devices have specific diameter for data transmission. IoT enabled WSN connects huge amount of machines or devices and these devices also generate huge amount of data [1]. Sensors are widely deployed in remote locations to collect the data and then forward the collected data to the station (BS) for data processing. Multiple standardization organizations and industries still trying to make efforts for standardization and development of IoT enable WSNs but there is a need of comprehensive framework. Most significant challenges in the WSN are data transmission and data trafficking for traffic monitoring, activity monitoring, quality assurance and fire detection [2]. Security and reliability of the nodes is mandatory especially in real time continuous secure data transmission to the remote destination [3]. Sensing devices share data with collectors to aggregate data in a resource efficient and collaborative manner. In smart IoT, the mobile phones, Tabs and laptops establish keys securely communicate with smart sensing devices [4].

The main issue during data collection is that CH may be destroyed by attacker or some technical fault may occur. It blocks the data at sensing nodes. The critical data must be timely reached to Sink node especially for the real-time data in non-delay tolerant networks like secure healthcare data sharing for patients. Security of aggregated data is also quite essential. Member nodes cannot share the data with neighboring CH because keys are not established with neighboring clusters.

This paper presents a Critical Data Reclamation (CDR) protocol that ensures secure data transmission when CH is destroyed within a network. We utilize the gateway nodes that are located at the boundary of clusters and have established keys with both CH. Gateway nodes collect the compressed messages from the sensor nodes and share the aggregated data with neighboring CH to further transmit to sink or FoG servers. The main contribution of this paper are follows.

1) We explored the literature for data aggregation schemes.
2) A system model is presented for the data reclamation in case of CH failure. We present data transfer and data compression algorithms.
3) Next, we present the aggregated message formation at CH and share with the sink.
4) Finally, the message receiving mechanism is explored to extract the data at sink.

The rest of paper is organized as follows; Section II explores the literature review for data aggregation schemes. Sections III elaborates the proposed CDR protocol and related algorithms. Section IV discusses about results and analysis. Finally, Section V concludes our work and discusses about future work.

II. Related Work

We explored recent schemes that used key-based encryption and authentication for secure communication in WSN. The data aggregation scheme in [5] establishes a secure path for peer to peer intercommunication between sensing nodes and the smart aggregator nodes. Zhong et al. efficiently reduced energy consumption and delay for data transmission using signature based homomorphic encryption. Encrypting and filtering data to reduce energy consumption [6]. In [7], a secure information transfer mechanism is presented. It computes and analyzes the data produced by the sensors on the IoT devices. It transfers data to cloud or fog nodes as per topic of data.

Manuscript submitted on 26 December 2020 for review.

A. Ullah and M. Azeem are with Department of Computer Science, National University of Modern Languages (NUML), Islamabad 44000, Pakistan (e-mail: aullah@numl.edu.pk, muhammadazeem0493@gmail.com).

H. Ashraf is with Department of Computer Science and Software Engineering, International Islamic University Islamabad, Islamabad 44000, Pakistan. (email: humaira.ashraf@iiu.edu.pk)

N.Z Jhanjhi is with the School of Computer Science and Engineering, SCE, Taylor’s University, Malaysia. (email: noorzaman.jhanjhi@taylors.edu.my).

Lewis Nkenyereye is with Department of Computer and Information Security, Sejong University, 05006, Korea. (email: nkenyele@sejong.ac.kr)

Mamoona Humayun is with College of Computer Science, Jouf University, Al-Jouf, Saudi Arabia. (email: mahumayun@ju.edu.sa).