A Matrix-Based Pair-Wise Key Establishment for Secure and Energy Efficient WSN-Assisted IoT

Anurag Shukla Shukla, NIT Raipur, Raipur, India
Sarsij Tripathi, NIT Raipur, Raipur, India

ABSTRACT
The Internet of Things (IoT) is getting the reputation as one of the most optimistic networking paradigms that is reducing the gap between the cyber world and physical world. Most of the participating nodes in IoT network are sensors, which are limited in terms of resource such as energy, computation power, memory and so on. In IoT network, nodes communicate with each other via wireless medium, which makes the IoT network vulnerable to many security threats including eavesdropping. The IoT network is deployed in a large area and work on 24/7 hours, so an energy efficient scheme is one of the major issues in IoT. To achieve secure and energy efficient network, this article contributes: (1) A hierarchical topology for IoT network deployment; (2) symmetric matrix-based pair-wise key generation for secure communication; (3) A secure and energy efficient secure routing algorithm for the proposed model.

KEYWORDS
Deployment Knowledge, Energy Consumption, Hierarchical Clustering, Internet of Things (IoT), Matrix, Pair-Wise Key

1. INTRODUCTION
Internet of things (IoT), which connects the physical world with cyber world of communication and computation, is changed the way of interaction by the sensors, actuators, embedded devices and managing the real world around us. It is not integration of one standalone device rather many objects participate in IoT network. IoT includes many applications such as environment monitoring, traffic management system, smart parking and home automation, have large impacts on social life. Thus, many of us see the IoT as an essential solution to understand and automate the real-world physical processes in real time.

The implementation of IoT networks brings some challenges. The deployment of IoT networks is achieved in large area as compare to wireless sensor network, so traditional WSN’s techniques cannot be applied directly (Atzori, Iera & Morabito, 2010). In IoT networks, to satisfy user queries, sensor nodes sense the data in continuous way or communicate to each other. Many of the objects participate in IoT network; this makes large energy consumption in network. So, efficient energy communication is required to extend the network lifetimes (Sun & Coyle, 2012; Huang, Meng, Gong, Liu & Duan, 2014; Rani et al., 2015; Georgiou, Xavier-de-Souza, & Eder, 2017). The network nodes communicate to each other via wireless medium and generate data, which is sent via wireless medium to the targeted location. The data transmission via wireless medium causes many security

DOI: 10.4018/IJISP.201907010106

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
vulnerability issues under various cyber attacks. For example, attacker can eavesdrop or modify the data, interrupt the service, and even capture network nodes. To countermeasure these attacks in IoT network, many security techniques have been proposed that include key management technology (Wander, Gura, Eberle, Gupta, & Shantz, 2005; Ren, Zeng, & Lou, 2006), secure routing technology (Khan, Alrajeh, & Loo, 2012; Galuba et al., 2010) and intrusion detection technology (Lauf, Peters, & Robinson, 2010; Pham, 2011).

The realizations of secure and energy efficient routing and the analysis of energy cost of Blom’s scheme and modified Blom’s scheme into energy efficient routing protocol with optimal Relay node (RN) selection is the main objective of this work. Earlier many techniques have been proposed for efficient energy WSN such as: exact, hierarchy, ad-hoc, but these techniques do not include the node arrangements as in energy efficient IOT network. In this work, we adopt an efficient topology for IoT network deployment. First, IoT nodes are deployed in hierarchical framework, which supports the scalability features and would be extensible as well. Finally, at the end cluster-based energy efficient routing protocol is used for data transmission. Rani (2015) & Huang (2014) consider energy as a one parameter for optimization where as in this work we integrate the matrix-based pair-wise scheme for key generation (Blom, 1984; Sukumar, 2013) in the ME-CBCCP routing protocol to make the network secure. We make an analysis on energy depletion of proposed framework due to additional communication cost for pairwise key generation between nodes. The research work can be summarized as follows:

1. In this work, we deploy the network nodes in hierarchical cluster framework. This topology support scalability and can be extensible up to any level. The communication among the nodes in inter cluster or intra cluster are taken place according to some well-defined communication rules so that cluster load can be distributed, and network lifetime can be increased.
2. A secure and energy efficient communication problem is considered in this work. In this propose framework to achieve security, Base Station (BS) distribute secret symmetric matrixes to the cluster heads before the network deployments. Normal nodes (NNs) in local cluster can establish pair-wise key to the other neighbor NNs and can communicate to each other via corresponding relay nodes (RNs). We will discuss in detail in upcoming section that how the NNs can generate the key via private matrix.
3. The experiments have been performed with standard parameters on random deployment network and cost of energy is compared with energy efficient routing without security, energy efficient routing with bloom’s scheme and modified bloom’s scheme.

The remaining paper is structured as follows: WSN routing protocols related work overview is given in Section 2. Section 3 covers description of system framework. A matrix base pair-wise scheme for secure communication and their application in minimum energy consumption routing algorithm is presented in Section 4 and in section 5 performance evaluation has been done followed by conclusion in last section.

2. RELATED WORK

A lot of work have been carried out in past for energy efficient communication in deployed network to support green IoT network (Al-Fagih, 2013; Ehsan, 2012; Liu, 2012) and earlier secure communication techniques have been proposed based on matrix-based pair-wise key generation (Du, Deng, Han, & Varshney,2006; Zhang, Xu, Xiang, & Huang, 2013). But we found that very few work have been reported for secure routing protocol via concerning sensor nodes energy in the network. This opens the area with carry out research in this direction.
Efficient Routing Protocol for Location Privacy Preserving in Internet of Things
www.igi-global.com/article/efficient-routing-protocol-for-location-privacy-preserving-in-internet-of-things/218847?camid=4v1a

Applied Cryptography in Electronic Commerce
www.igi-global.com/chapter/applied-cryptography-electronic-commerce/46243?camid=4v1a