Trust-Based Opportunistic Network Offloaders for Smart Agriculture

Prince Sharma, Jaypee University of Information Technology, Waknaghat, India

Shailendra Shukla, Motilal Nehru National Institute of Technology Allahabad, India

Amol Vasudeva, Jaypee University of Information Technology, Waknaghat, India

ABSTRACT

With the enormous use of internet of things-based devices for enabling smart agriculture, there is a significant need for efficient systems in order to improve agricultural practices. It can help efficiently to develop optimal web-based information system using the data of field monitoring. But, the collection of such data in the presence of connectivity disruptions poses new challenges for users. This paper targets to determine such offloaders with less infrastructural costs to enable smart agriculture based on network heuristics. Although, few works contribute to the trust established, most of them are applicable only for static networks. This paper explores a trust-based solution for mobile data offloading. This paper identifies the need and impact of trust determination using the trust model algorithm. The proposed algorithm outperforms the hybrid trust-based mobility aware clustering algorithm for trust-based offloaders with up to 13% better offloading potential saving a minimum of 8 pJ energy per user with just 25% contributors with 50% lesser time delay.

KEYWORDS

Data Sharing, Internet of Things, Opportunistic Networks, Smart Agriculture, Target Set Selection, Trust

INTRODUCTION

The use of smart agriculture techniques provides a promising solution for crop monitoring and environmental data gathering, while addressing the challenges of less human resources, climate change, and economic barriers etc. The use of mobile phones along with IoT based devices, which aim to connect the physical devices to the internet can significantly contribute to the development of smart agriculture and farming techniques (Awada et al., 2003). The lack of benefit from data sharing by the farmers has been identified as the major drawback in leveraging the advantages of digital agriculture. Big data and precision agriculture are believed to impact the farm economy over a longer period. This may narrow down the labor requirements and specialized trends in such fields. The societal returns to the rural alleviations are more important than the digital agricultural startups for their possible success (Chaterji et al., 2020). A very few of the research works has experimentally shown the use of IoT devices (Elijah et al., 2018) to develop web-based information systems (Balamurugan and Satheesh, 2017). The idea is to collect the data efficiently and automatically in the challenging context of the network connectivity and architecture. Although, some updates and applications can tolerate delays and disruptions in data, it is always beneficial to use the converging trend of Wireless Sensor Networks (WSNs) (Ray, 2017) and Opportunistic Networks (Han et al., 2011) to reduce these delays and data disruptions. Thus, when we deal with the contribution of social network analysis

DOI: 10.4018/IJAEIS.20210101.oa3

for the determination of opportunistic communication in networks, there is a similar application of opportunistic networks in agriculture also. This enables us to replace traditional agricultural practices with more efficient mechanisms enabling smart agriculture (Heble et al., 2018). The contribution of smart agriculture practices can be well exploited when implemented for various phases of farming (Ray, 2017). This may help all the contributors in the agricultural network including all producers and consumers. In recent years, due to increase in the information and communication technologies as well as IoT-based technologies, the mobile network operators have been suffering from the problem of traffic explosion (Genghua et al., 2019). The exponential growth in global mobile traffic is likely to push the current cellular network to its limit (Salam et al., 2017). According to the annual internet report Cisco (2020), about 66% of the global population is expected to be connected by three times the number of devices using Internet Protocol (IP) networks by the year 2023. The significant side effect of this expected phenomenon is the overloading on 4G/5G cellular network and creating a bottleneck in transmission (Rebecchi et al., 2014). Thus, it is indeed imperative to handle massive traffic using novel architectures and feasible protocols. Due to expensive investments, it becomes impractical to extend cellular networks' infrastructure to process this data traffic (Gao et al., 2013). Hence, to address the massive traffic and expensive infrastructure, it is required to switch to mobile data traffic offloading solutions (Awada et al., 2010) via technology like femtocells (Han et al., 2011), Bluetooth (Han et al., 2011; Wang et al., 2015), WiFi (Jung et al., 2013), or D2D communications (Weifing et al., 2020).

Although, there have been solutions (Rebecchi et al., 2014), but most of them have an unrealistic model like using either static graphic analysis (Thilakarathna et al., 2016) or monotonic behavior of Internet Service Provider (ISP) (Salam et al., 2018) or the Access Points (AP) (Yu et al., 2019). The researchers have shown that opportunistic mobile data offloading (Jedari et al., 2018; Thilakarathna et al., 2013; Yu et al., 2019) can provide a feasible solution for data offloading. The major limitation of the existing opportunistic mobile data offloading is that all the nodes willing to participate in data offloading are the honest nodes. One of the solutions for these limitations is to use trust determination and incentive for the network nodes. In most of the modeling schemes, the existing trust determination (Yu et al., 2019; Zhang et al., 1999) is difficult to be applied due to the limitations of energy (Zhuo et al., 2011), frequent association/disassociation (Rebecchi et al., 2014), dynamic graph (Oubabas et al., 2018), buffer space of nodes (Zhuo et al., 2015), or their interest in incentives (Kang et al., 2015). The implementations in the above literature require all nodes to cooperate (Yu et al., 2019) to forward the information. This may lead to the problem of evaluating the trust timely (Huang et al., 2004) and precisely. There are equal chances of nodes to leave the connected domain due to their dynamic behavior. The authority assignment for trust evaluation is also partially based on the model used for comparisons as given in Jedari et al. (2019). As far as the utilization of network's node degree is concerned, the degree of nodes keeps on changing due to the continuously evolving pattern of the network. The degree of the network can only be assured once the network transforms to its final state; else not. Most of the network modeling and its analysis afterward is done over static networks (Jung et al., 2013, Thilakarathna et al., 2013, Thilakarathna et al., 2016, Zhou et al., 2018), which is unrealistic. Also, the degree of nodes in the network may reflect malicious behavior as stated in (Jedari et al., 2019; Rebecchi, 2014). Such a situation arises in social networks when some terminal node exhibits the property of structural holes in a network.

The major contribution in this work is the identification of reliable, optimal off-loaders as the target set selection problem and a trust-based solution for data offloading. This paper incorporates the phenomenon of opinion-based trust with higher time delay tolerance. We target the dynamic behavior of network graphs. The proposed model considers the dynamic behavior that evolves with the changing time. We study the significance of random trust modeling mechanism for dynamically evolving networks. The goal is to derive the trust for such potential offloaders for their true or false behavior based on heuristic opinion dynamics. It helps in the determination of high or low trustworthy