Trustworthy Wireless Volunteer Computing using Markov Model and Firefly Algorithm

Farooque Hassan Kumbhar, Soo Young Shin*
farooque.kumbhar@gmail.com, * wdragon@kumoh.ac.kr

Kumoh National Institute of Technology, Gumi, South Korea.

Abstract

The volunteer computing (VC) paradigm provides extensive distributed cloud computing services to millions of devices in need. However, the true potential of VC can be achieved in the Internet of Things (IoT) networ k where devices are resource constraints and require nearby cloud services. We highlight the need for trustw orthiness to enable VC in IoTs and propose a Markov model-based paradigm for trustworthy wireless VC usi ng a firefly algorithm. In this paper, we introduce a fusion of VC and IoT and propose a distributed trustwort hiness management system using the Social Internet of Things.

Ⅰ. Introduction

Volunteer computing (VC) allows devices to share their idle computing resource like storage and processing with other devices in need. By doing so, VC makes available tons of resources and computing power in a connected network. A middle-ware creates a bridge between these volunteer service providers (SP) and service users (SU}[1]. A middle-ware is responsible for the contract (tasks, time, resources, scheduling, etc.) between SP and SU. However, more often these middle-wares require continuous communication with SP and SU for control and monitoring which can hinder network performance due to its centralized architecture. We believe that the volunteer resources for computing and storage offer massive computing advantage in the Internet of Things (IoT) environment, where devices are expected to communicate autonomously. The volunteer computing can take advantage of IoT distributed architecture and enable resource sharing, which also benefits IoTs [2].

There is a need for a distributed and autonomous agreement system, which can enable VC in IoT devices and provide a trustworthiness management system for an impartial give-and-take scenario. Moreover, to ensure safety and security, an autonomous trust management mechanism is also required. Social Internet of Things (SIoT) is a distributed paradigm that allows devices to establish relationships and manage trustworthiness[3]. The trust calculation process employs a function of the centrality of the device, previous experience, and peer opinion. We propose a distributed trustworthy paradigm to enable VC in the wireless environment of IoT. Each IoT device can communicate to a nearby device and request for cloud services[4]. We propose to establish an agreement between devices by maximizing trust towards SP, remaining storage, and energy of SP. We contribute to the novelty by identifying and tackling three major challenges: (a) distributed trust management using Social Internet of Things (SIoT), (b) selection of SP by SU using Firefly algorithm, and (c) state transition diagram to apply communications constraints using Markov Model. Considering the random and sporadic nature of device mobility in IoT and trust factor over continuous time, we believe that the Markov model can portray a better state transition system.

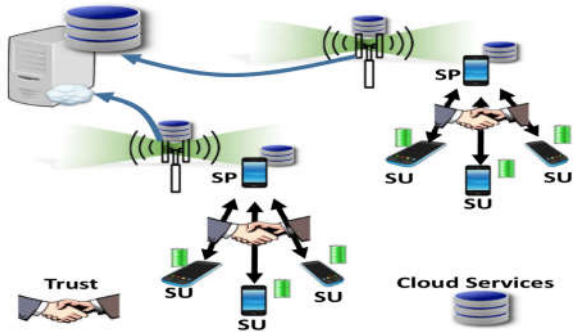


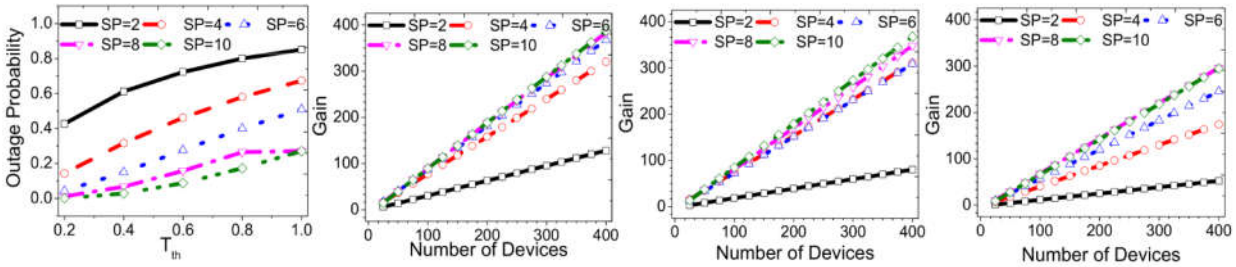
Figure 1 Proposed scheme for mobile cloud

Ⅱ. Trust Establishment and SP Selection

Let a directed graph for IoT network is G={V,E}, where $V = \{v_1, v_2, \dots, v_n\}$ is the set of n nodes. An edge $e_{i,j}$ is a physical wireless direct communication link between v_i and v_j. We propose that given G={V,E}, trust between IoT device can be quantified and assigned to each edge. We calculate the trustworthiness of a nearby device $\tau_{i,j}$ [0,1], utilizing $R_{i,j}$, $O_{i,j}^{dir}$ and $O_{i,j}^{ind}$. Mathematically[3]:

$$\tau_{i,j} = (1-\alpha-\beta)R_{i,j} + \alpha O_{i,j}^{dir} + \beta O_{i,j}^{ind} \quad (1)$$

where $R_{i,j}$ [0,1] indicates the centrality of node v_j, as viewed from v_j and previous direct and indirect (common peer opinion) transaction experience is represented by $O_{i,j}^{dir}$ [0,1] and $O_{i,j}^{ind}$ [0,1] [3]. The α and β (=0.33) are the weights for the above weighted sum equation. Given that each SP (j) has a certain amount of energy (E_j) and storage capacity($S_j = \left(1 - \frac{1}{S_{avbl}}\right)^{S_{rqrd}}$ where S_{avbl} is available storage in SP and S_{rqrd} is storage required by SU), we formalize a utility



(a) Unavailability of SP (b) Capacity gain when $\tau_{th} = 0.25$ (c) Capacity gain when $\tau_{th} = 0.50$ (d) Capacity gain when $\tau_{th} = 0.75$

Figure 2 Performance evaluation of the proposed scheme with different SPs, τ_{th}, and number of devices

Algorithm 1 SP selection using metaheuristic fitness function based Firefly Algorithm

```
Initialize i=0, SP=0; f_max=0;
P_0 = {p_1, p_2, ..., p_λ}
while j < λ do
    if τ_i,j > τ_th then
        Calculate f(j)= α * τ_i,j + β * S_j + γ * E_j
        if f(j) > f_max then
            f_max = f(j)
            SP=j
            j++
        end if
    else
        f(j) = 0
    end if
end while
```

function considering trust, energy and storage. A device can identify the utility function of a SP by making use of a weighted sum equation as given below:

$$f(j) = \theta * \tau_{i,j} + \psi * S_j + \gamma * E_j \quad (2)$$

where θ, ψ and γ are weights to control the tendency towards any specific utility function parameter. The energy (E_j) of a SP is the remaining battery power. Algorithm 1 outlines proposed firefly algorithm where a SU device receives a set of SP offers $P_0 = \{p_1, p_2, \ldots, p_\lambda\}$. The SU evaluates each offer by calculating $f(j)$ if the trust ($\tau_{i,j}$ using Equation 1) towards the SP is higher than a threshold ($\tau_{i,j} > \tau_{th}$). A traverse operation assesses through all $f(j)$ to identify the one with highest $f(j)$, i.e. f_{max}. Given that the mobility has a major impact on the proposed scheme, we formalize four Markov model-based states, i.e. S1: A SP is within communication range, S2: A SP is not in the range, S3: A SP is within communication range and has data to process or store, S4: A SP is not in the range and has data to process or store. The proposed Markov model is used to identify the service outage in the mobile offloading process.

Ⅲ. Performance Evaluation and Conclusion

We perform a Monte Carlo based simulation in our c++ simulator to evaluate the performance of the proposed scheme. We populate an area of 1 km^2 with 400 devices where each device is assigned a storage value, energy, and a file to store. The device communicates with devices in proximity to estimate trust for each other. A random selection assigns 2 to 10 SP in each scenario which broadcasts their offer to nearby devices. Fig 2a shows that the number of SP has a great effect on the outage probability, calculated using the Markov model states. The unavailability of an SP also increases with the increase in the $\tau_{th}$from 0.2 to 1. Fig. 2b, Fig. 2c, and Fig. 2d show the capacity gain achieved by the proposed scheme when τ_{th} = 0.25, 0.5 and 0.75, respectively. The increase in the number of devices increases density which subsequently utilizes more SP resources and provides high capacity gain. However, it should be noted that the SP is assumed to have enough capacity. The proposed scheme innovates by introducing trust-based SP selection in a mobile wireless volunteer computing. The SP device comes forward and offers various cloud services to nearby SU devices. However, the SU doesn't blindly use the service and calculates trust $\tau_{i,j}$ for each offer. Moreover, each offer is also evaluated based on the proposed utility function of storage and energy. The proposed firefly algorithm pairs each SU with the most suitable SP to achieve high gain and minimum outage.

ACKNOWLEDGMENT

This work was supported by Korea Research Fellowship Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science and ICT (2019H1D3A1A01102978).

References

[1] Muhammad Nouman Durrani, Jawwad A. Shamsi: `Volunteer computing: requirements, challenges, and solutions', Journal of Network and Computer Applications, 2014, 39 (1), pp. 369-380

[4]. Murk, A. W. Malik, I. Mahmood, N. Ahmed, and Z. Anwar, "Big Data in Motion: A Vehicle-Assisted Urban Computing Framework for Smart Cities," IEEE Access, vol. 7, pp. 55951-55965, 2019

[3]. F. H. Kumbhar, N. Saxena, A. Roy, Reliable Relay Autonomous Social D2D Paradigm for 5G LoS Communications, IEEE Communications Letters, vol.21, no.7, pp.1593-1596, 2017

[4]. A. Amjid, A. Khan, and M. A. Shah, "VANET-Based Volunteer Computing (VBVC): A Computational Paradigm for Future Autonomous Vehicles," IEEE Access, vol. 8, pp. 71763-71774, 2020.