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 helpers based on their influence and contribution. We also evaluate the offloading efficiency for our trust-based offloaders.

In the remainder of the paper, we briefly summarize the literature survey in Section 2. Section 3 and Section 4 present the system model and problem formulation with our contribution, respectively. Section 5 covers the proposed algorithm for offloading. Section 6 covers the simulation results. Finally, we conclude our work in Section 7.

BACKGROUND

We have gone through the latest optimal data offloading solutions in our literature survey. We have identified that there is a limited research focus on trust management for efficient data offloading. Hence, this aspect needs to be explored more with possible improvements. In this section, we survey the recent activities related to offloading based on trust.

Thilakarathna et al. (2013) and Thilakarathna et al. (2016) used distributed content storage and dissemination architecture to address the issue of trust and timeliness delivery of data for intelligent content replication. The research includes the forecast for trust prediction among nodes for social networking based mobile network. The results also establish the fact that it is not possible to consistently identify all the significant users to optimize delivery. This is because, the users are highly environment-dependent i.e., the networks are dynamic and keep evolving with time especially in vehicular networks. The work is dependent upon a community-based greedy method for content replication based on behavioral patterns of mobile users. The work also considers the minimization of both the content replication and the delivery delay. The community-based prediction is characterized by unconditional sharing with a fixed delivery deadline. The consumers need to download the full content at first to start the content dissemination as a propagator, which results in more delay for more substantial content. The energy costs are also ignored. This involves excessive network resource utilization and high computations due to the use of application-specific trust management.

Jung et al. (2013) and Zhang and Xu (1999) used a user-centric approach for hetergoneous networks based on Wi-Fi offloading model. Jung et al. (2013) proposed a higher per-user throughput offloading model, which show better results than the on-spot Wi-Fi offloading model. However, their work is based on the assumption that all the packet generation rates are the same for all users along with the packet sizes using the implementation of the dogleg path algorithm. Zhang and Xu (1999) suggested the need of identification of selfish nodes on the basis of social trust behavior. They used a reputation system on the basis of direct and indirect information shared individually and socially. Trust and security mechanism is considered significantly in mobile networks along with the aspects of mobility management and accounting to support offloading strategies (Rebecchi et al., 2014, Salam et al., 2018). Jedari et al. (2019) suggested the need of identification of selfish nodes based on the social tie behavior. They designed a malicious node detection module for the evaluation of truthfulness of watchdogs' nodes. They used a reputation system based on direct and indirect information shared individually and socially. This is achieved by the identification of a few nodes in the network as the watchdog nodes. This helps the model to have a longer detection time for data relaying with less communication overhead. It also acknowledges the mitigation in individual and social cooperation.

The relation between trust management and privacy protection is targeted by Pham and Yeo (2018) for VANETs. There is a proposal of Adaptive Likability and Recognition Scheme (ALRS) for revoking the selective nodes with some ability to recognize the identity and the trust level. The authors also used Adaptive Trust Management System (ATMS) to verify the data sent by other nodes and update their reputations. These systems use a policy of intersection between their list of link values in which every pair of vehicles exchange their identities confidentially and share a link value upon their first meeting. The results show accurate decisions towards the reported event and high detection rate of malicious nodes recognizing the wrong events. Oubabas et al. (2018) also derive a secure and stable clustering algorithm on the basis of hybrid mobility similarities and trust management schemes in Vehicular Ad hoc Networks (VANETs). The use of trust management systems in VANETs is also evaluated for addressing security attacks with optimum utilization of network bandwidth (Poongodi et al., 2019).

Salam et al. (2017) identify the significance of transitive relations in trust evaluation for data offloading in 5G networks using machine communications. They used social connectivity along with physical proximity for the transitive evaluation of trust criteria. The work focuses on the framework using graph formation followed by relay group formation for graph optimizations on the basis of their multiple mobile relay algorithms. However, they used the primary relay schemes based on the mutual trust among the devices limited to scenarios like stadiums, shopping malls, and exhibition centers. The authors proposed a data aggregation scheme for data offloading on the basis of extensive trust criteria, which diffuses the nuisance of a single point of failure in machine-type communications. This structure is based on a two-hop relay scheme, which is assumed to be non-interfering across the second hop.

The phenomenon of Home Router Sharing based on Trust (HORST) is also used for online social networks in Rebecchi et al. (2014) and Salam et al. (2018). The methodology involves a firmware for a home router along with an application. Seufert et al. (2013) proposed a trust-based third party application for home router sharing, which augments the caching approach of base station access points, one step ahead from online social networks. The HORST algorithm focuses on data offloading to Wi-Fi, content caching and content delivery. The authors identify the drawback of transitive trust-based derivations. They used personalized trust values of Wi-Fi access point owners with closer geographical distances. However, the content caching mechanism incurs additional costs, which accounts for the selfish and non-cooperative behavior of users (Weifeng et al., 2020).

Yu et al. (2019) used the derivation of interactive quality features, which is dependent on the degree of the nodes and the total number of connections. They applied an attenuation function for weighing interaction feedback-based mechanism. The dependency of relationship information feedback nodes can be biased. The trust degree evaluation is also dependent on the feedback-based mechanism. However, some of the terminal nodes across graphs are also crucial despite of being loosely coupled with the original source of the transmission. The performance factor needs additional addressing than link reliability to enable better adaptation towards service level agreements for critical data transmission (Sharma and Kumar, 2019). The assumption restriction of parallel links in the network graph and data bifurcation helps in identifying a suitable network model.

The use of Communication Things Network (CTN) has been offered a secure mechanism for extracting and sharing digital information to develop smart appliances for better productivity (Rathee et al., 2019). Haseeb et al. (2020) have proposed an IoT-based WSN framework as an application for smart agriculture based on several design leveling techniques. They have proposed an energy efficient and secure IoT-based WSN framework application for smart agriculture. Their work is dependent on factors such as residual energy, signal-to-noise ratio constraints, and the distance between base station and the IoT device. The proposed framework depends on the usage of secret keys for secure data transmission. However, this work lacks the performance analysis in IoT-based network or intelligent transportation system. Balamurgan and Satheesh (2017) have demonstrated the integration of IoT with Raspberry pi and sensors to monitor soil pressure, temperature, and humidity of fields for improving the efficiency of agriculture. The results demonstrate reduced man power and electrical energy usage.

It can be concluded from the above work that the use of trust and security mechanism has been considered significantly along with the aspects of mobility management and accountability to support offloading strategies in infrastructure-based mobile networks. The community-based prediction is characterized by unconditional sharing with a fixed delivery deadline. The consumers have to download the full content at first to start the content dissemination as a propagator, which results in longer delay for a larger content in general. The energy costs are also ignored. This involves excessive resource utilization in the network and high computations due to the use of application specific trust management, which renders additional load. The contribution of trustworthy offloaders is significant which needs to be explored more. From the above analysis of existing literature, it can be concluded that in real world applications, the information of social attribute identification of the destination nodes does not have integrity. It also has limited adaptability of dynamic behavior of nodes and their network structures. The social aspect of such structures is limited to certain parameters and the trust identification is also partial. Also, the communication is trust-oriented, but limited to the communication range in WSNs. Some sub-networks have social relations derived on the basis of real scenarios, which consider the static relationships independent of quantified social relationships in agricultural networks.

MAIN FOCUS OF THE ARTICLE

The main concern in this paper is to model a realistic behavior of the users in opportunistic network by considering the opinion based trust of the users. The users may or may not be completely connected. We enable bidirectional opportunistic communication using IoT devices.

Issues, Controversies and Problems

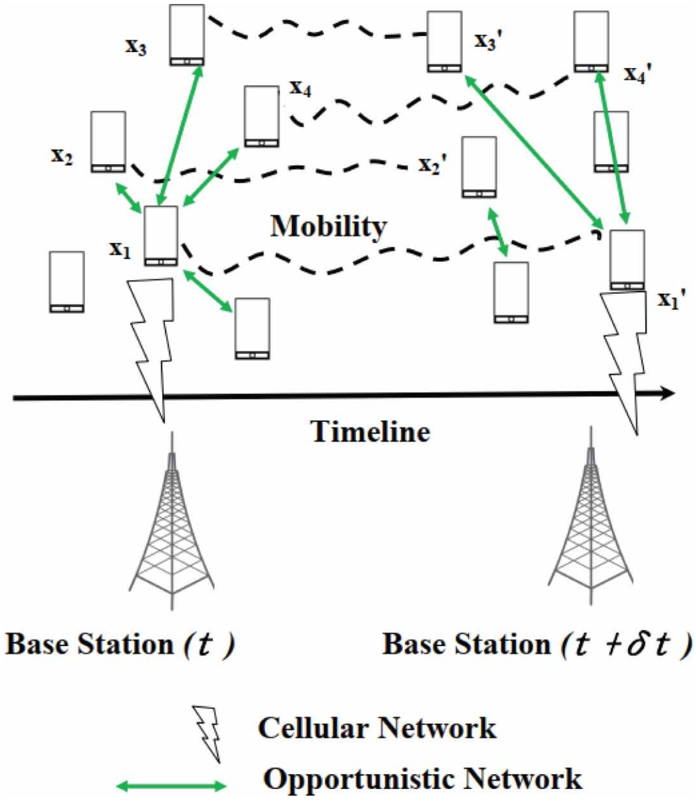
As stated in (Malliaros et al., 2016), time is an important aspect for describing the dynamic property of any trust relationship. So, we propose our model having mobile characteristics in an opportunistic network. Such a continuously evolving model enables us to view the network at different time frames. Our observation model is more realistic because of its dynamic behavior and is analyzed to derive opinion heuristics, using graph properties that change with time. Our system model considers the mobile users randomly distributed in limited geographical proximity, as shown in Figure 1. We demonstrate few mobile users namely x_1, x_2, $x_{3,}$ and x_4, at time instance t, which change their position to x'_1, x'_2, x'_3 and x'_4 at time instance $t + \delta t$. The new position for users x'_1 and x'_2 as shown in the diagram, shows that the user x_1 is still connected to the base station at instance $t + \delta t$, however the user x_2 falls within the proximity of x_1 after the same time interval. In such an opportunistic sub-network, we conceptualize the users x_3 and x_4 to be more trustworthy for the user $x_{1,}$ than the user x_2 during a fixed time interval δt.

We consider an ISP having several Access Points (APs) complementing for data offering. For each of these APs, we have a set of N users who are willing to act as helpers H in mobile data offloading, such that $H = \left\{x_1, x_2, x_3, ..., x_N\right\}$ at any instance of time t. Instead of considering all of the users as helpers, our proposed model considers only a limited set of users as helpers, which behave non-maliciously, i.e., on the basis of their trust values. These are referred to as optimal helpers H'. We determine H' on the trust basis so that the data gets offloaded only by M users, such that $H' \subseteq H$. Helpers may act positively or maliciously in a network. With a change in the time δt, the structure and behavior of the network changes and we observe a new graph with different functioning capabilities.

We have assumed that our opportunistic network is able to suit similar interest-based users more than the different interests based mobile users. However, the entire network, when visualized as a social network, also makes it suitable for dissimilar interest-based users. We have limited the use of our implementation for similar interest-based users so that it is able to deliver the smaller data size information perfectly better than any other network with maximum offloading offered by the trust derived matrix. We have considered only the positive trust based derivations and combined the neutral or negative trust derivations together. This is because the positive trust values are assumed to form a more reliable sub network than the non trust-based network.

We have also assumed that users tend to be selfish for enabling cooperation in the set and thus emerge to become trustworthy or non-trustworthy on the basis of their utility. In such a model, the users become more or less useful based on their contribution in the network for long run. We propose this model from the point of view of the ISP in collaboration with the subgroup leaders for their local

Figure 1. System Model for Trust-based Opportunistic Network



opinion-based neighborhood trust. This also helps to exclude the non-trustworthy associations. Our system model attributes to the association frequency of a node for being associated with specific set of neighbors. Hence, such a node with higher frequency of similar associations is automatically rewarded more than the one with fewer number of associations or dissimilar set of neighbors. In our system model, we prefer to use the term '*reward*' as getting positive opinion association and thus becoming more trustworthy whereas '*distrust*' refers to negative or zero opinion correspondence. Considering the constraint of social network participation, we aim to focus on a more realistic association of nodes across a conference dataset from Haggle project. Along with the dynamic network generation, we characterize the network nodes on the basis of the trust values based function derived by the neighboring nodes for each node. It adds to the dependence factor of the nodes, comprising within the network. This is attributed to the adjacency matrices of the nodes, with their neighbors. The significance of a node to its neighbors is used to evaluate the neighborhood opinion, where the opinion of a user is evaluated on the basis of similarity index of the neighbors and their ranking for the user (Zhang et al., 1999). Hence, our model lays the foundation of trust derivation for each node on the basis of bidirectional opinion dynamics, i.e., from users towards the helpers as well as from helpers towards ISP or APs, thereby finalizing the target set for optimal data offloading.

Definitions

In order to properly model the network and our algorithm, we will be using some frequently used terms in this paper. We define these terms as below:

- **Helpers:** All set of users who are finally selected as optimal data offloaders with favorable parameters on the basis of our proposed algorithm are being termed as Helpers in our work. In general, these are the optimal users with certain characteristics based on trust values.
- **Community:** In our work, we determine the trust values into three categories namely being positive, negative or null. Each of these subsets of users is termed as separate community, where a particular user is identified to be belonging to a particular community on the basis of magnitude of its trust value.
- **Homophily:** It is the property by virtue of which we may co-relate the behavior of a particular user to be same or different to some other user. All positive community users are expected to be more homologous than the negative or neutral community users.

PROPOSED ALGORITHM

In this section, we propose Trust Model Algorithm (TMA) to derive the optimal target set for final offloaders identification. Our algorithm uses the property of higher trust values in the opportunistic network. It considers the dynamic properties of the network. TMA uses the changing opinion on trust between users and the entire network. This helps us to exclude the less stable users and use the best users according to their potential. The list of symbols and notations used in the algorithm are listed in Table 1.

Trust Model Algorithm

TMA focuses on overall opinions of such helpers in the graph to derive direct trust values. Secondarily, indirect trust is dependent on the adjacency matrix based associations. The overall trust function values are used to derive final set of trustworthy users as Target Set (TS). We consider the Target Set Selection (TSS) problem based on positive or negative trust in a network, this is responsible for distrust of the helpers. We have considered all the strong and weak ties as edges in the network. This helps us to identify the triadic closures in the graph. We identify stable and unstable combinations of triads in terms of signed networks in our algorithm. Our algorithm relies on two significant parameters direct and indirect trust, for evaluating their contribution in a successful network or sub-network. In our algorithm, we evaluate direct trust ψ_1 using opinion θ_1 (Malliaros et al., 2016).

We consider the higher impact of helpers embedded in a network that is directly proportional to its trust value. For the evaluation of indirect trust ψ_2, we use the adjacency matrix for neighbor identification. This helps our algorithm to identify the pattern of homophily in the network. Our algorithm does not rely upon the degree of nodes for identifying significant contributors because it can only be a statutory parameter.

To evaluate utility of the network, we determine total trust function F. The value of F depends upon direct trust value ψ_1 and indirect trust value ψ_2. Our problem of trust-based TSS is represented as an optimization problem:

$$Maximize\ \ Total\ \ Trust, F = \sum\nolimits_{\delta t>1} \psi_1\left(x_i\right) + \psi_2\left(x_i\right)$$

where F can get a positive, zero or negative value. The direct trust values $\psi_1\left(a_i\right)$ are evaluated as opinion based function $\psi_1\left(x_i\right) = f\left(\theta_1\right)$. The opinion value θ_1 for user x_i is derived using the following equation:

Table 1. List of symbols or notations used in the algorithm

Symbol/Notation	Definition/Explanation
H	Set of N number of users; $H = \left\{x_1, x_2, \ldots, x_N\right\}$
F	Final trust function
$\psi_1\left(x_i\right)$	Direct trust value of user x_i at time t
ψ_2	Indirect trust value
θ_1	Opinion according to the graph
θ_2	Opinion according to the neighbors
TS	Final set of offloaders
τ_i	Trustworthiness of user x_i
α_i	Action status of user x_i .

$$\theta_1(x_j) = \sum\nolimits_{x_p, x_q \in H} \frac{\rho(x_p, x_q \mid x_j)}{\rho\left(x_p, x_q\right)}$$

where $\rho\left(x_p, x_q\right)$ represents the number of total edges between users x_p and x_q , whereas $\rho(x_p, x_q \mid x_j)$ identifies the number of edges through node x_j , but not x_p and x_q . This helps in identifying the homophilic behavior of these users x_p and x_q . This opinion value lets the BS identify the extent of help offered by a particular node at a particular instance. The state of a helper being selected as offloader at any instance is identified as action α_i . The indirect trust ψ_2 .is derived using lifetime l_i , association frequency nbr_{x_i} and ranking method (Zhang et al., 1999) but for maximum different set of neighbors according to the adjacency matrix. The cumulative sums of the diagonal rows and columns of the adjacency matrix enable us to determine homophily of associations. We evaluate trustworthiness τ on the basis of difference in the opinion values using the following equation:

$$\tau_i = \theta_i^{t+\delta t} - \theta_i^{t}, where \frac{\left|\tau_i\right|}{\tau_i} = \left\{+1, if\ \alpha_i = +1; and\ \ -1, if\ \alpha_i = -1\right\}$$

The action status of the helper in subsequent derivations is evaluated as $\alpha_i \subset \left\{+1, -1\right\}$. This actually determines whether the user x_i has been trustworthy or untrustworthy in the previous time period. In case if any two neighbors x_i and x_j are selected to cooperate for offloading i.e., $\alpha_i = \alpha_j = 1$ with equal trust values $\tau_i = \tau_j$, but their opinion values are different such that $\theta_i > \theta_j$

then the node with higher opinion value θ is considered for offloading. At the secondary level of neighborhood based optimization, we use indirect trust evaluation using the adjacency matrix of helper for its neighbors. The computational complexity of our algorithm is $O\left(N \times n\right)$, where N represents the total number of helpers and n represents the maximum degree of any helper, such that $n << N$. The above maximization problem is *NP*-hard and cannot be solved in polynomial time unless $P = NP$. This is attributed using *Theorem* 1 given as below:

Theorem 1: The problem of maximization of total trust function F is NP-hard.
Proof: To prove the NP-hardness of the problem, we consider the following special 0-1 knapsack problem:

Maximize: $f_1 x_1 + f_2 x_2 + f_3 x_3 + \ldots + f_n x_n$

subject to:

$$f_1 x_1 + f_2 x_2 + f_3 x_3 + \ldots + f_n x_n \leq S$$

and:

$$x_1, x_2, x_3, \ldots, x_n \in \left\{0,1\right\}$$

Here, f_1 is the size of the i^{th} user, S is the size of Knapsack and x_1 is the variable which indicates whether the i^{th} user is added into the knapsack. Such a special 0-1 knapsack problem is NP-hard (Martello et al., (1999). When we consider the special case of our Maximization problem for the evaluation of Total Trust, in which there is only one AP, i.e., $W = \left\{\left\langle \alpha_i, \tau_i, \theta_1, \theta_1 \right\rangle\right\}$ and $\alpha_i \subset \left\{+1 / 0 / -1\right\}$. Hence our data offloading problem of maximization of total trust function F can be expressed as:

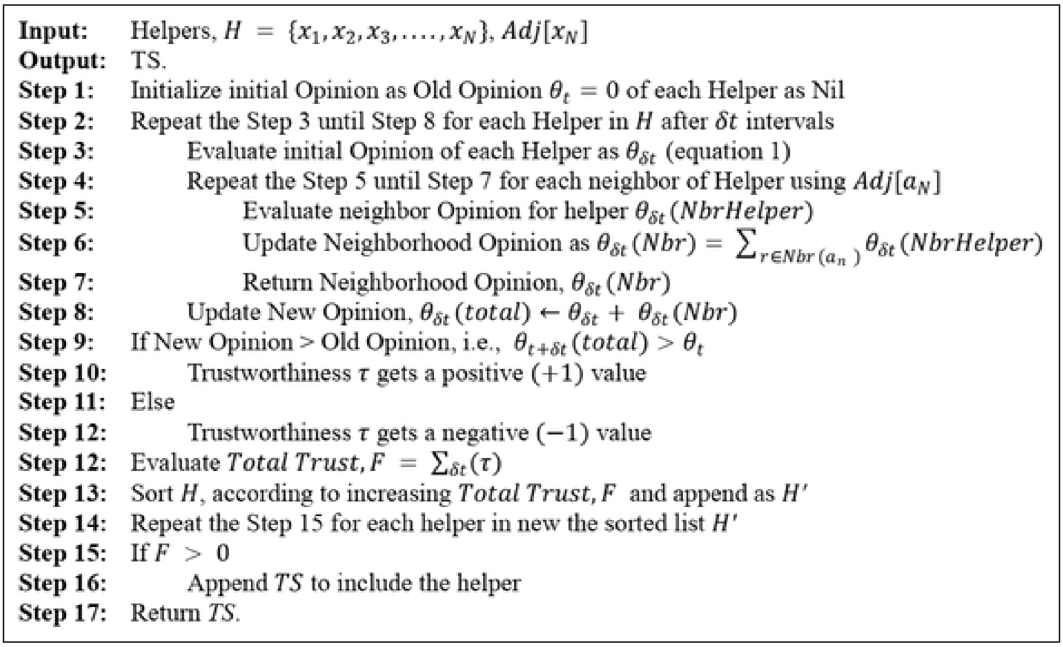
Maximize: $\sum_{x_i}^{i=m} \psi_1 + \psi_2$

subject to:

$$\sum_{x_i}^{i=m} \psi_1 + \psi_2 \leq \tau_i$$

Mapping S from the equation above to the equation, $F = \psi_1 + \psi_2$ we can state that the above two problems are equivalent. Thus we can prove that our problem is a special case of 0-1 knapsack problem, which is *NP*-hard. Hence, our trust problem is also *NP*-hard.

Table 2. Algorithm 1: Trust Model algorithm, TMA



```
Input:    Helpers, $H = \{x_1, x_2, x_3, ...., x_N\}$, $Adj[x_N]$
Output:   TS.
Step 1:   Initialize initial Opinion as Old Opinion $\theta_t = 0$ of each Helper as Nil
Step 2:   Repeat the Step 3 until Step 8 for each Helper in $H$ after $\delta t$ intervals
Step 3:       Evaluate initial Opinion of each Helper as $\theta_{\delta t}$ (equation 1)
Step 4:       Repeat the Step 5 until Step 7 for each neighbor of Helper using $Adj[a_N]$
Step 5:           Evaluate neighbor Opinion for helper $\theta_{\delta t}(NbrHelper)$
Step 6:           Update Neighborhood Opinion as $\theta_{\delta t}(Nbr) = \sum_{r \in Nbr(a_n)} \theta_{\delta t}(NbrHelper)$
Step 7:           Return Neighborhood Opinion, $\theta_{\delta t}(Nbr)$
Step 8:       Update New Opinion, $\theta_{\delta t}(total) \leftarrow \theta_{\delta t} + \theta_{\delta t}(Nbr)$
Step 9:   If New Opinion > Old Opinion, i.e., $\theta_{t+\delta t}(total) > \theta_t$
Step 10:      Trustworthiness $\tau$ gets a positive $(+1)$ value
Step 11:  Else
Step 12:      Trustworthiness $\tau$ gets a negative $(-1)$ value
Step 12:  Evaluate $Total\ Trust, F = \sum_{\delta t}(\tau)$
Step 13:  Sort $H$, according to increasing $Total\ Trust, F$ and append as $H'$
Step 14:  Repeat the Step 15 for each helper in new the sorted list $H'$
Step 15:  If $F > 0$
Step 16:      Append $TS$ to include the helper
Step 17:  Return $TS$.
```

Simulation Results

In this section, we present the results and their analysis after some data pre-processing steps according to model requirements for a mobile ad hoc network. We have considered the Crawdad WTD data-trace for our simulation purpose, which considers the opportunistic network of PDA users. We consider only the associated users and access points with respective time schedules and battery consumption status for 77 days. It is better suited for MANET realization. During our analysis, we needed to establish the graph analysis of the entire network with fixed delay tolerance at different time intervals.

We have compressed the datatrace to derive only the associations where a user was found to be connected to the access points. Although, we ignore the battery status for our initial analysis, we limit our work to determine the trust across the remaining dataset attributes, which consists of total 1,32,15,412 records. This battery status has been used in the later stages for energy consumption verification. We also restrict our network observation limited to only those users and access points on the basis of the ASSOCIATED attribute. This identifies the user to be linked or not linked with a respective access point. It shrinks our analysis further to 52,19,839 such records. For these input sets of graphs, we derive the opinion based trust using the triadic closures of number of cliques, clustering coefficients, and page rank significance. We compare the contribution of trustworthy or non-trustworthy users. Finally, we compare our data offloading scheme with the heuristics of network associations based on degree of users and access points. These results in a newer routing mechanism are observed based on trust as a function of time.

We have also checked for the impact of the change of degree of the users with the passage of time. The trust also changes as the time progresses with a change in the degree of users. The limitation of ns-2 evaluation is that the energy evaluation is not possible using this simulator for MANETs. Therefore, we have used Python's NETWORKX library to resolve this problem using the environment statistics as given in Malliaros et al. (2016). Based on the energy derivations of Zhou et al. (2011), we also implement the free space wireless radio model. We calculate the energy consumption per satisfied helpers when a node transmits a uniform 1 bit of information to its neighbors as:

$$E_{avg} = \frac{\varepsilon^{elec} + \varepsilon \times d^2}{Number\ of\ Satisfied\ users}$$

where ε^{elec} identifies the energy consumed per bit measured in J/bit, by transmission electronics when a node sends or receives 1 bit of information, taken as 50 nJ/bit. Here, we consider ε as the free space constant value 10 pJ/bit/m^2 simulated over transmission range d of 250 meters for MANETs as given in Movahedi et al. (2015). These energy derivations are limited to MANETs only.

Using the above simulation setup, we first observe the impact of positive or negative trusts for mobile data offloading. It is followed by the comparative analysis of our trust derivation based offloaders with the offloaders retrieved by HTMAC implementation (Janani et al., 2018). Next, we check for their impact over time delay tolerances and energy usages.

Contribution of Positive and Negative Trust Users

To illustrate the significance of trust, we have repeated the random trust-based simulations. Our results in Figure 2 illustrate the significance of ten simulations done over the WTD data-trace based on the random assignment of trustworthy and non-trustworthy users. Figure 2 shows that untrustworthy users contribute more than trustworthy contributors in realistic environments. The practical observation of the proportional contribution of trustworthy and untrustworthy nodes is also shown in Figure 3. It shows that more than 50% contribution is always from the unreliable nodes. This may lead to an unstable or biased incentive distribution to such helpers for offloading. However, very small contribution is from true helpers, which are always less than 50% in practical scenarios as given in Figure 3.

Performance of Our Proposed Trust Model Algorithm

As illustrated in Figure 4, we get optimized results with our final target set identified on the basis of trust values derived from our algorithm. To measure the effectiveness of our algorithm, we compare our results with algorithms for random trust assignments. Next, we compare our results with a literature based trust assignment model. The derivation of influential nodes on the basis of trust function enables us to derive more optimal results taking into account the mobile users. Our results

Figure 2. Impact of Trust over network connectivity

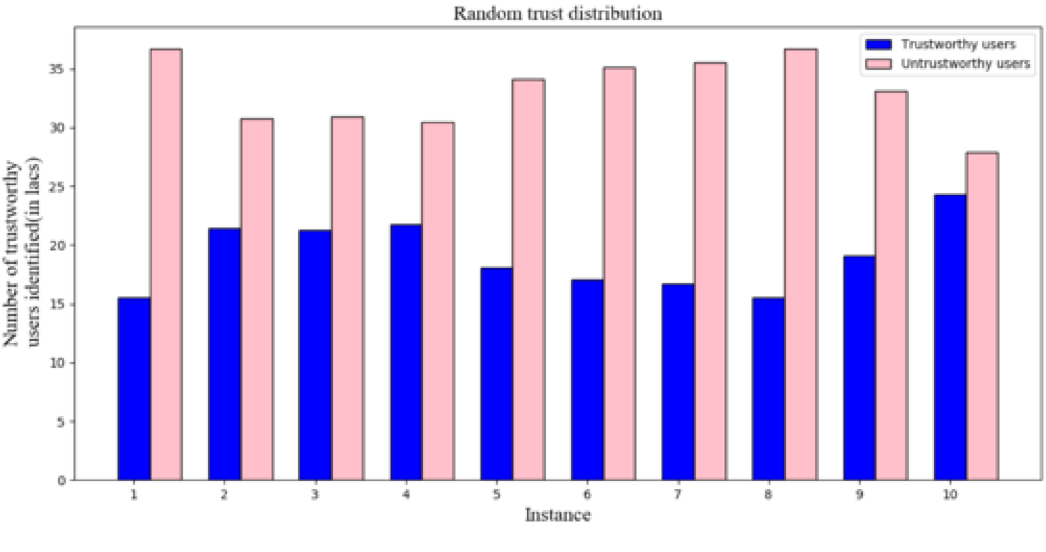
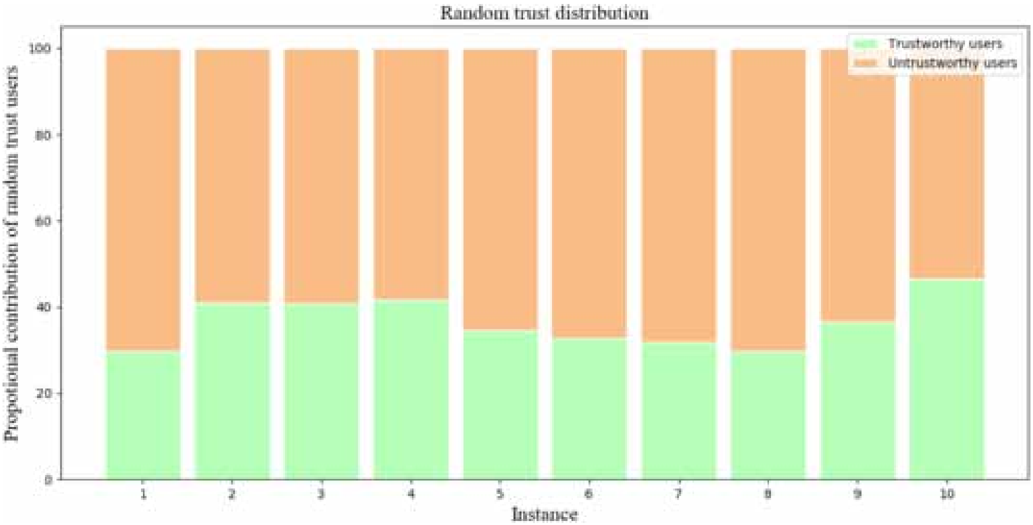


Figure 3. The proportional contribution of Trust



from Figure 4 show an optimal behavior with merely 10% contribution done by positive trust-based offloaders enabling 73% of the entire network to stay connected. Our derivation of trust considers the evolving nature of opinion in comparison to the random trust assignment model, which considers only the attributes based on the degree of nodes, irrespective of their trustworthiness. We ignore the comparisons beyond 50% contribution of our trust-based offloaders in the network, owing to less practical feasibility of such contributions (Figure 3). From the Figure 5, we establish the performance of trust for mobile data offloading solution using our algorithm. It assures about 70% of the users to be satisfied successfully from our trust model with mere incorporation of just 10% of positive trust based users. After establishing the optimal contribution towards trust establishment from Figure 4, we compare our results with the literature-based trust derivations done by distrust users using Figure 5.

Data Offloading Performance of TMA

After the random assignment of trusts for users, we compare our result with trust-based derivations using HTMAC-based algorithm (Janani et al., 2018). We check our algorithm for the contribution of trustworthy as well as non trustworthy users. There is a significant improvement of data offloaded using TMA. Figure 6 shows that less trust-based offloaders are contributing better in the case of TMA than HTMAC. We have at least 3% less contribution from our less trust-based offloaders in this case. When we analyze the efficiency of high trust contributors, we observe the results as depicted in Figure 7. It shows that the contribution of high trust-based offloaders derived using TMA increases with increasing percentage of their incorporation. Corresponding to 25% high trust-based offloaders, we achieve a maximum of 13% better contribution in the comparison of HTMAC. Hence, we are now in a state to conclude that the offloaders selected using our TMA give more optimum results in terms of offloaded data. Later, we analyze the results for their time delay and energy usages also.

Time Delay Performance of TMA

Assuring better offloading contribution, we analyze the delay involved in transmission using TMA offloaders. We have observed that using our TMA, the time delay is also reduced significantly, which is up to 50% less than HTMAC as shown in Figure 8. The results show that TMA performs better than HTMAC in time delay performance also. Hence, we can also conclude that the offloaders using TMA are faster in data offloading.

Figure 4. Performance of TMA based helpers

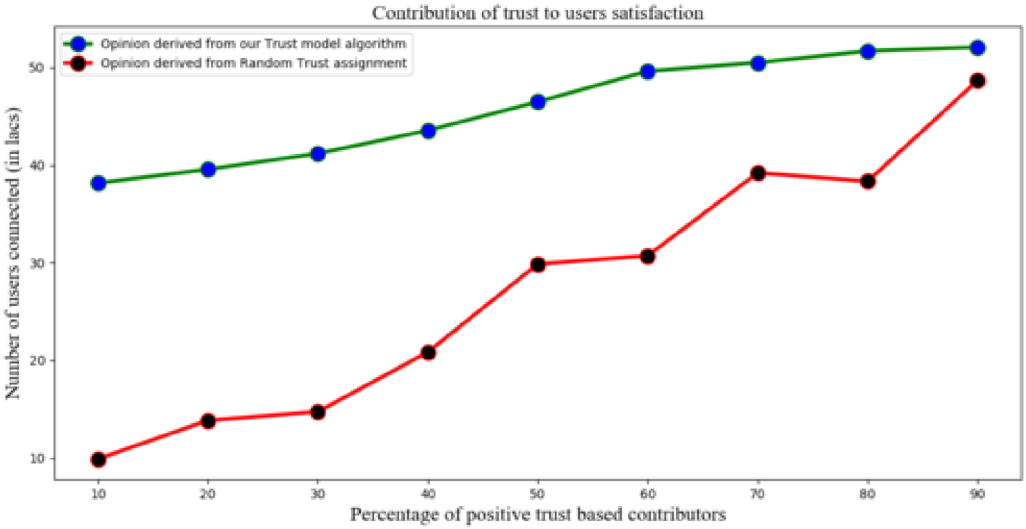
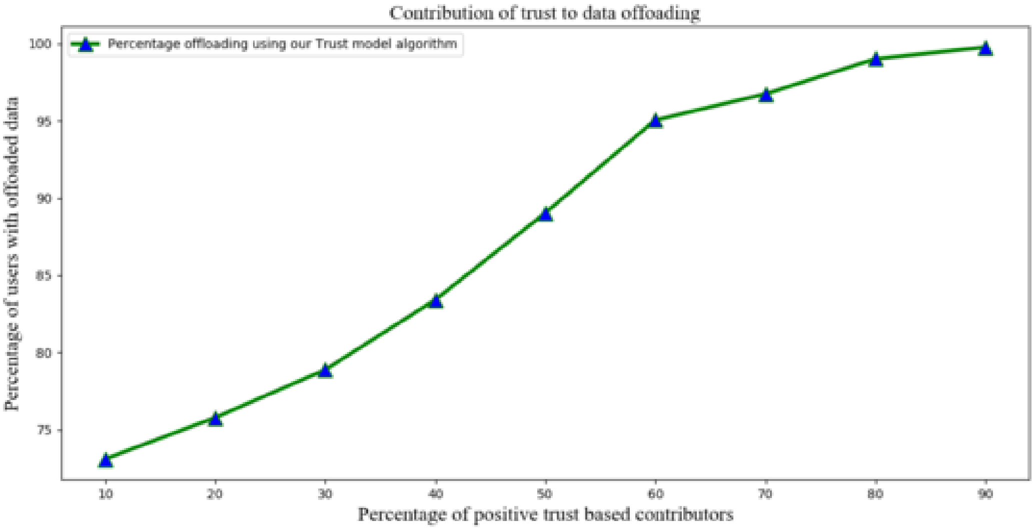


Figure 5. Contribution of TMA helpers



Energy Consumption Performance of TMA

Here, we compare the average energy usage by buffer capacity for each satisfied helper in the network. The results are depicted in Figure 9. TMA is better than HTMAC-based procedure for energy usage also. There is at least 8 pJ/user less energy consumption with 5% contribution of TMA offloaders. There is a maximum of 15 pJ/user less energy consumption with 25% TMA offloaders. Since the results are depicted only for single helper contribution, we observe that there is a significant energy improvisation for larger realistic networks. As we go on to add more trust-based helpers according to TMA, we achieve energy optimized network with comparatively less energy consumption.

Figure 6. Performance of TMA based untrustworthy helpers

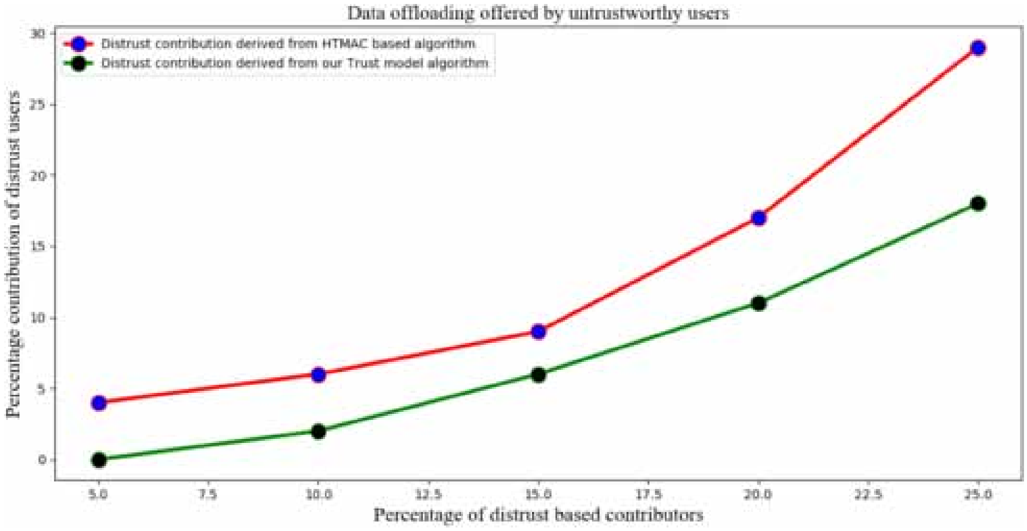
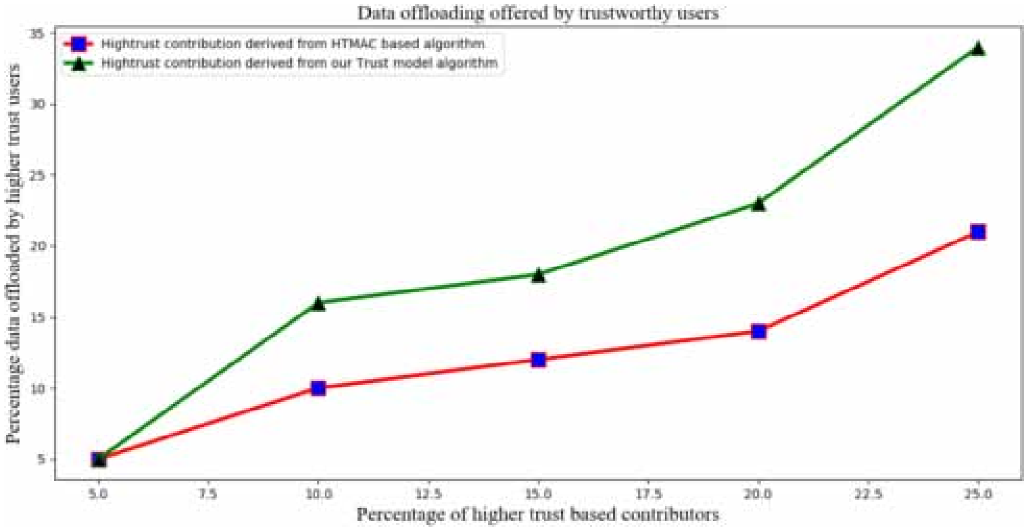


Figure 7. Performance of TMA based trustworthy helpers



CONCLUSION AND FUTURE SCOPE

Trust is a vital attribute to determine more efficient offloaders in any opportunistic network. This helps in more efficient mobile data offloading using such offloaders to enable smart agriculture-based information systems for farmers. Few farmers may withdraw their support from the network and act mischievously as the time progresses. Thus, it is not always more beneficial to rely on the degree of helpers, especially in realistic networks of farmers. Hence, we need to consider the evolutionary nature of opinion for such farmers who continue to be trustworthy or become faulty with time. We have successfully demonstrated that the throughput of a trust-based offloading model is better than non trust-based derivation as well as random trust based derivation. Our contribution towards *TSS*

Figure 8. Time delay using TMA based trustworthy users

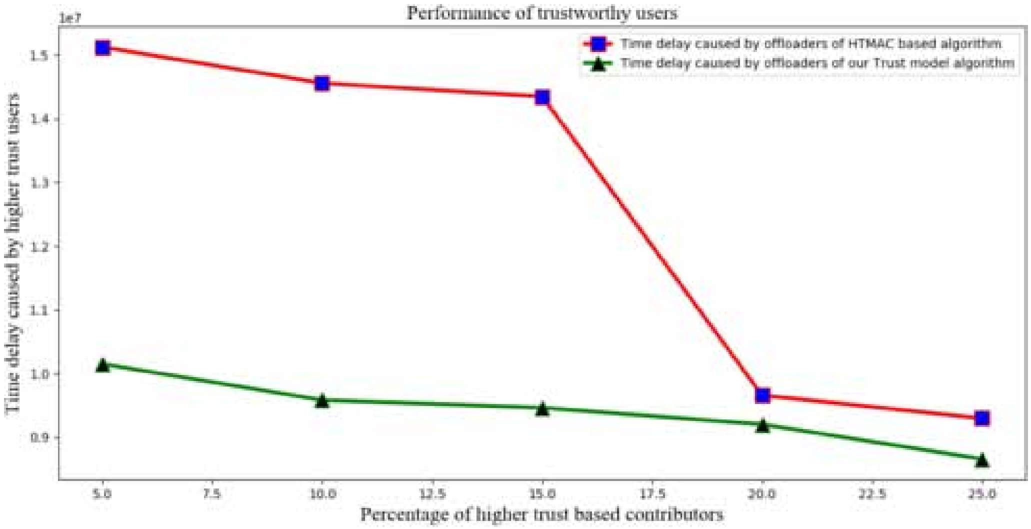
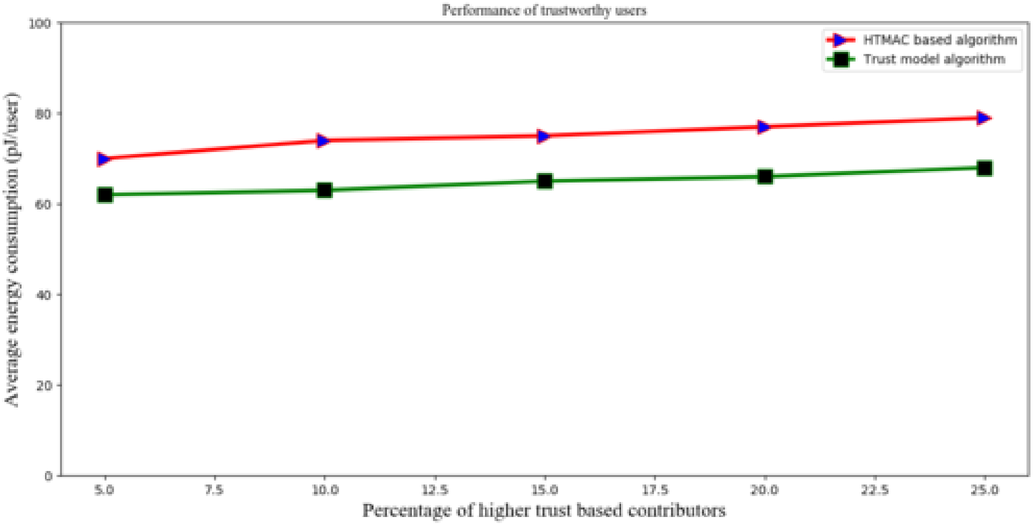


Figure 9. Energy usage of TMA based trustworthy users



identification can be explored more to derive the incentive distribution for offloading. This can be provided to the efficient farmers in terms of more data offerings. This model can also be used to derive classification rules for specific agriculture crops in future.

REFERENCES

Awada, A., Wegmann, B., Viering, I., & Klein, A. (2010, September). A game-theoretic approach to load balancing in cellular radio networks. In *21st Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications* (pp. 1184-1189). IEEE. doi:10.1109/PIMRC.2010.5672050

Balamurugan, C., & Satheesh, R. (2017). Development of Raspberry pi and IoT Based Monitoring and Controlling Devices for Agriculture. *Journal of Social, Technological and Environmental Science*, *6*(2), 207–215. doi:10.21664/2238-8869.2017v6i2.p207-215

Cai, R. J., Li, X. J., & Chong, P. H. J. (2018). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. *IEEE Transactions on Mobile Computing*, *18*(1), 42–55. doi:10.1109/TMC.2018.2828814

Chaterji, S., DeLay, N., Evans, J., Mosier, N., Engel, B., Buckmaster, D., & Chandra, R. (2020). *Artificial Intelligence for Digital Agriculture at Scale: Techniques, Policies, and Challenges*. arXiv preprint arXiv:2001.09786.

Cisco. (2020). *Cisco Annual Internet Report (2018–2023) White Paper*. Cisco.

Elijah, O., Rahman, T. A., Orikumhi, I., Leow, C. Y., & Hindia, M. N. (2018). An overview of Internet of Things (IoT) and data analytics in agriculture: Benefits and challenges. *IEEE Internet of Things Journal*, *5*(5), 3758–3773. doi:10.1109/JIOT.2018.2844296

Gao, J., Buldyrev, S. V., Havlin, S., & Stanley, H. E. (2012). Robustness of a network formed by n interdependent networks with a one-to-one correspondence of dependent nodes. *Physical Review. E*, *85*(6), 066134. doi:10.1103/PhysRevE.85.066134 PMID:23005189

Gao, L., Iosifidis, G., Huang, J., & Tassiulas, L. (2013, April). Economics of mobile data offloading. In *2013 Proceedings IEEE INFOCOM* (pp. 3303-3308). IEEE. doi:10.1109/INFCOM.2013.6567155

Han, B., Hui, P., Kumar, V. A., Marathe, M. V., Shao, J., & Srinivasan, A. (2011). Mobile data offloading through opportunistic communications and social participation. *IEEE Transactions on Mobile Computing*, *11*(5), 821–834. doi:10.1109/TMC.2011.101

Haseeb, K., Ud Din, I., Almogren, A., & Islam, N. (2020). An Energy Efficient and Secure IoT-Based WSN Framework: An Application to Smart Agriculture. *Sensors (Basel)*, *20*(7), 2081. doi:10.3390/s20072081 PMID:32272801

Heble, S., Kumar, A., Prasad, K. V. D., Samirana, S., Rajalakshmi, P., & Desai, U. B. (2018, February). A low power IoT network for smart agriculture. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)* (pp. 609-614). IEEE. doi:10.1109/WF-IoT.2018.8355152

Huang, C., Hu, H. P., & Wang, Z. (2004, October). Modeling time-related Trust. In *International Conference on Grid and Cooperative Computing* (pp. 382-389). Springer. doi:10.1007/978-3-540-30207-0_48

Janani, V. S., & Manikandan, M. S. K. (2018). Mobility aware clustering scheme with bayesian-evidence trust management for public key infrastructure in ad hoc networks. *Wireless Personal Communications*, *99*(1), 371–401. doi:10.1007/s11277-017-5107-1

Jedari, B., Xia, F., Chen, H., Das, S. K., Tolba, A., & Zafer, A. M. (2019). A social-based watchdog system to detect selfish nodes in opportunistic mobile networks. *Future Generation Computer Systems*, *92*, 777–788. doi:10.1016/j.future.2017.10.049

Jung, B. H., Song, N. O., & Sung, D. K. (2013). A network-assisted user-centric WiFi-offloading model for maximizing per-user throughput in a heterogeneous network. *IEEE Transactions on Vehicular Technology*, *63*(4), 1940–1945. doi:10.1109/TVT.2013.2286622

Kang, X., & Sun, S. (2015, June). Incentive mechanism design for mobile data offloading in heterogeneous networks. In *2015 IEEE International Conference on Communications (ICC)* (pp. 7731-7736). IEEE. doi:10.1109/ICC.2015.7249563

Malliaros, F. D., Rossi, M. E. G., & Vazirgiannis, M. (2016). Locating influential nodes in complex networks. *Scientific Reports*, *6*(1), 19307. doi:10.1038/srep19307 PMID:26776455

Martello, S., Pisinger, D., & Toth, P. (1999). Dynamic programming and strong bounds for the 0-1 knapsack problem. *Management Science*, *45*(3), 414–424. doi:10.1287/mnsc.45.3.414

Movahedi, Z., Hosseini, Z., Bayan, F., & Pujolle, G. (2015). Trust-distortion resistant trust management frameworks on mobile ad hoc networks: A survey. *IEEE Communications Surveys and Tutorials*, *18*(2), 1287–1309. doi:10.1109/COMST.2015.2496147

Oubabas, S., Aoudjit, R., Rodrigues, J. J., & Talbi, S. (2018). Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. *Vehicular Communications*, *13*, 128–138. doi:10.1016/j.vehcom.2018.08.001

Pham, T. N. D., & Yeo, C. K. (2018). Adaptive Trust and privacy management framework for vehicular networks. *Vehicular Communications*, *13*, 1–12. doi:10.1016/j.vehcom.2018.04.006

Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS Detection Mechanism Using Trust-Based Evaluation System in VANET. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 183532–183544. doi:10.1109/ACCESS.2019.2960367

Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks*, *94*, 101933. doi:10.1016/j.adhoc.2019.101933

Ray, P. P. (2017). Internet of things for smart agriculture: Technologies, practices and future direction. *Journal of Ambient Intelligence and Smart Environments*, *9*(4), 395–420. doi:10.3233/AIS-170440

Rebecchi, F., De Amorim, M. D., Conan, V., Passarella, A., Bruno, R., & Conti, M. (2014). Data offloading techniques in cellular networks: A survey. *IEEE Communications Surveys and Tutorials*, *17*(2), 580–603. doi:10.1109/COMST.2014.2369742

Salam, T., ur Rehman, W., & Tao, X. (2017, December). Cooperative MTC data offloading with trust transitivity framework in 5G networks. In *GLOBECOM 2017-2017 IEEE Global Communications Conference* (pp. 1-7). IEEE. doi:10.1109/GLOCOM.2017.8255045

Salam, T., Rehman, W. U., & Tao, X. (2018). Cooperative data aggregation and dynamic resource allocation for massive machine type communication. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 4145–4158. doi:10.1109/ACCESS.2018.2791577

Seufert, M., Burger, V., & Hoßfeld, T. (2013, October). HORST-Home router sharing based on Trust. In *Proceedings of the 9th International Conference on Network and Service Management* (CNSM 2013) (pp. 402-405). IEEE. doi:10.1109/CNSM.2013.6727865

Sharma, A., & Kumar, R. (2019). A Framework for Risk-Energy Aware Service-Level Agreement Provisioning (RESP) for Computing the Quickest Path. *Journal of Computer Networks and Communications*, *2019*, 1–8. Advance online publication. doi:10.1155/2019/4109453

Thilakarathna, K., Viana, A. C., Seneviratne, A., & Petander, H. (2013, July). Mobile social networking through friend-to-friend opportunistic content dissemination. In *Proceedings of the fourteenth ACM international symposium on Mobile ad hoc networking and computing* (pp. 263-266). doi:10.1145/2491288.2491319

Thilakarathna, K., Viana, A. C., Seneviratne, A., & Petander, H. (2016). Design and analysis of an efficient friend-to-friend content dissemination system. *IEEE Transactions on Mobile Computing*, *16*(3), 702–715. doi:10.1109/TMC.2016.2570747

Wang, Z., & Wong, V. W. (2015, June). A novel D2D data offloading scheme for LTE networks. In *2015 IEEE International Conference on Communications (ICC)* (pp. 3107-3112). IEEE. doi:10.1109/ICC.2015.7248801

Weifeng, L., Mingqi, Z., Jia, X., Siguang, C., Lijun, Y., & Jian, X. (2020). Cooperative caching game based on social Trust for D2D communication networks. *International Journal of Communication Systems*, *33*(9), e4380. doi:10.1002/dac.4380

Yu, G., Chen, Z. G., Wu, J., & Wu, J. (2019). Quantitative social relations based on trust routing algorithm in opportunistic social network. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), 83. doi:10.1186/s13638-019-1397-1

Zhang, J. X., Chen, D. B., Dong, Q., & Zhao, Z. D. (2016). Identifying a set of influential spreaders in complex networks. *Scientific Reports*, *6*(1), 27823. doi:10.1038/srep27823 PMID:27296252

Zhang, J. Z., & Xu, C. X. (1999). Trust region dogleg path algorithms for unconstrained minimization. *Annals of Operations Research*, *87*, 407–418. doi:10.1023/A:1018957708498

Zhang, Q., Gui, L., Tian, F., & Sun, F. (2017, May). A caching-based incentive mechanism for cooperative data offloading. In *2017 IEEE International Conference on Communications Workshops (ICC Workshops)* (pp. 1376-1381). IEEE. doi:10.1109/ICCW.2017.7962851

Zhou, H., Wang, H., Li, X., & Leung, V. C. (2018). A survey on mobile data offloading technologies. *IEEE Access: Practical Innovations, Open Solutions*, *6*, 5101–5111. doi:10.1109/ACCESS.2018.2799546

Zhou, P., Jiang, S., Irissappane, A., Zhang, J., Zhou, J., & Teo, J. C. M. (2015). Toward energy-efficient trust system through watchdog optimization for WSNs. *IEEE Transactions on Information Forensics and Security*, *10*(3), 613–625. doi:10.1109/TIFS.2015.2389145

Zhuo, X., Gao, W., Cao, G., & Dai, Y. (2011, October). Win-Coupon: An incentive framework for 3G traffic offloading. In *2011 19th IEEE international conference on network protocols* (pp. 206-215). IEEE. doi:10.1109/ICNP.2011.6089054

Prince Sharma is pursuing his Ph.D. from Jaypee University of Information Technology. He has completed his M.Tech. and B.Tech. from Himachal Pradesh University. He has a teaching experience of five years. His research interests include Computer Algorithms and its applications, Opportunistic networks, Smart Agriculture.

Shailendra Shukla is an Assistant Professor at the Computer Science and Engineering Department of the Motilal Nehru National Institute of Technology Allahabad. He received the MS-(Information Security) from the "Indian Institute of Information Technology Allahabad and then completed a Ph.D. from the Indian Institute of Technology Patna in computer science. His doctorial work is based on "On Boundary Detection and Localization in Wireless Sensor Networks". In this work, he proposed a collection of networking algorithms that address the security problems like routing in the Internet of Things, localization, boundary node detection (surveillance), virtual coordinate assignment (Geography routing/localizations), cyber-physical systems, monitoring, and surveillance. He has published articles in various publication houses like Elsevier, Springer, IEEE. Previously, he was associated with Jaypee University for 5 years.

Amol Vasudeva was born in New Delhi, India in 1973. He received his degree in Master in Computer Applications from Indira Gandhi National Open University, Delhi, India in 2001. He completed his M. Tech. degree in Computer Science and Engineering from Jaypee University of Information Technology, Waknaghat, Solan, Himachal Pradesh, India in 2009. In 2018, he completed his Ph.D. degree in Computer Science from Himachal Pradesh University, Summer Hill, Shimla, Himachal Pradesh, India. He has worked as a faculty in University Institute of Information Technology, Himachal Pradesh University, Shimla, Himachal Pradesh, India from 2001 to 2005. In 2005, he joined Jaypee University of Information Technology, Waknaghat, India, where he is currently an Assistant Professor (Senior Grade) in the Department of Computer Science. He is an IEEE and ACM Member. His research area includes security in wireless networks.