Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

BoDMaS: Bio-inspired Selfishness Detection and Mitigation in Data Management for Ad-hoc Social Networks

Ahmedin Mohammed Ahmed[a,b], Xiangjie Kong[a,*], Li Liu[c], Feng Xia[a], Saeid Abolfazli[d], Zohreh Sanaei[d], Amr Tolba[e,f]

[a] *School of Software, Dalian University of Technology, Dalian 116620, China*
[b] *Kombolcha Institute of Technology, Wollo University, Kombolcha 208, Ethiopia*
[c] *School of Information Science and Electrical Engineering, Shandong Jiaotong University, Jinan 250357, China*
[d] *YTL Communications, Xchanging Malaysia, Kuala Lumpur, Malaysia*
[e] *Riyadh Community College, King Saud University, Riyadh 11437, Saudi Arabia*
[f] *Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Kom 32511, Egypt*

ARTICLE INFO

Article history:
Received 29 February 2016
Revised 13 August 2016
Accepted 13 September 2016
Available online 14 September 2016

Keywords:
Ad-hoc Social Networks
Community
Data replication
Selfishness
Social willingness

ABSTRACT

Existing data management protocols for socially-aware networks assume that users are cooperative when participating in operations such as data forwarding. However, selfishness as a non-cooperative act of misbehavior can seriously degrade network performance and fairness, particularly in Ad-hoc Social Networks (ASNETs). Therefore, detecting and counteracting selfishness on performance of cooperative users are crucial to the success of ASNETs. In this paper, we propose BoDMaS, a biologically inspired method, to detect and mitigate the impact of node selfishness on data management performance and efficiency of ASNETs. In design of BoDMaS, we consider social willingness (which depends on depth of social relationship among users) as a social behavior and bacteria chemical products as a counter to achieve optimal ASNETs performance. Counter is a parameter attached to individual user counting successful data operations performed in relation with others. Using social willingness and counter, BoDMaS assesses and classifies users, and counteracts their selfishness. BoDMaS is evaluated from different aspects demonstrating its ability to accurately detect and counteract selfishness in replication operations for ASNET environments.

1. Introduction

Emerging socially-aware networks that leverage social behaviors of participating nodes to improve networking throughput is gradually dominating wireless communication towards replacing traditional wireless networks [1–3]. Among various socially-aware networks, Ad-hoc Social Networks (ASNETs) [3] are gaining momentous ground due to their unique characteristics, particularly low resource consumption cost, mobility support, and infrastructure-less settings. Such features are often observed in biological processes that inspire inventing and designing novel cooperative architectural concepts [5]. ASNETs are proliferating as the common communication platform in broadly important areas such as pervasive conference/meetings and health-care, remote environmental monitoring and public safety, and ubiquitous urban data acquisition and national defense.

In socially-aware networking environments, users generate large amounts of data by exploiting capability-rich mobile devices, and are often willing to share data with users who have social relationships, social ties or greater similar interests with themselves. However, successful adoption of ASNET services (e.g., data dissemination and replication [4,6]), is inhibited in the absence of motivation/incentive for participating users who collaborate and share their resources. Cooperation among users is crucial to the survival of the network, as it forms the basis for key network services. If users (selfish users) refuse to collaborate in delivering the network services, end-to-end connection may not be possible leading to network performance degradation. Existing solutions assume that users are willing to collaborate with others [7]. However, users in practice are selfish with varied degrees of selfishness (from non-selfish to fully-selfish) depending on the strength of their social-tie with the underlying network, especially when there is no cooperating motivation/incentive [8]. Selfish users are unwilling to spend their precious resources for operations that do not directly benefit them [9]. For example, they may be willing to collaborate with socially-tied users (e.g., friends, coworkers, room-mates), but not others. Fig. 1 shows an example of a selfish user who inhibits efficient data forwarding in an exemplary scenario. The sender user S has two route choices ($S \rightarrow A \rightarrow B \rightarrow R$ and $S \rightarrow A \rightarrow C \rightarrow D \rightarrow R$) to

[*] Corresponding author. Fax: +86 41162274455.
E-mail address: xjkong@ieee.org (X. Kong).

http://dx.doi.org/10.1016/j.adhoc.2016.09.013
1570-8705/© 2016 Elsevier B.V. All rights reserved.

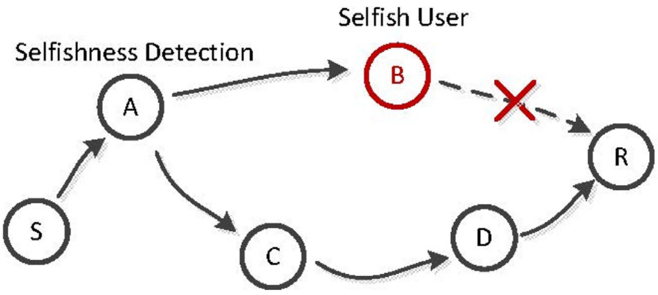


Fig. 1. An example demonstrating user selfishness in forwarding data from source to destination.

forward data to the user *R* at the receiver side; one is 3-hops and another is 4-hops far from receiver. Though efficient networking demands data transmission through lower hop route (3-hop in this example), the selfish user *B* located in middle of 3-hop route inhibiting data transmission via this route. Hence, transmission must be carried out via longer route over 4 hops leading to higher communication overhead [10]. Therefore, it is essential to detect selfish users and isolate them to limit their negative behavioral impact on the network performance.

Although a variety of solutions aim to address the problem of detecting and isolating misbehaving users in wireless networks [11], most existing works have focused on addressing selfishness by employing approaches such as reputation and incentive based [12], trust-based [13], ACK-based [14], game theory [15] or quorum-based [16] mechanisms to incentivize and motivate users to collaborate in services for others. In spite of significant findings in the detection and isolation of users' selfishness, there are still numerous issues that limit their applicability [17,18]. Firstly, social behaviors of participating nodes are neglected in the design and development of existing algorithms and hence makes them inefficient to be directly applied to ASNETs to deal with selfishness. Secondly, a huge overhead is induced from sharing reputation information amongst the users, additional ACK packets dissemination, and decision ambiguity that arises if the requested user refuses to return an acknowledgment. Thirdly, cooperative users might be indirectly punished due to their location in the network. Fourthly, network might be flooded by when a user sends the same data several times to the same receiver. Lastly, existing bio-inspired solutions (such as [16]) in this field consider only quorum systems but not social properties such as social ties.

ASNETs lack a centralized controlling and monitoring terminal, thus, making it a challenging task to effectively detect and isolate such misbehaving nodes from the network. Selfishness is a non-cooperative act of misbehavior, which is notably different from malicious behavior. It is noteworthy that our focus in this paper is only on selfishness and thus we ignore malicious behaviors (more detailed explanation in Section 3). To overcome the above limitations of existing algorithms, we design a bio-inspired algorithm named BoDMaS aiming to detect and counteract selfishness in ASNETs where high cooperation is highly desirable. We develop our solution taking inspiration from a biological mechanism resident in bacteria (quorum sensing) and social community systems. Our initial results are extremely encouraging, indicating that the choice of social behavior is critical and that novel techniques can be successfully imported from biologically inspired models.

In this paper, we are mainly focusing on user's behavior with respect to data replication operations (i.e., query/update) at the top of the data management model. Under this focus, each node can be classified as either cooperative (well-behaving) or selfish (misbehaving). This model may also apply to malicious nodes indirectly to some extent when it comes to timeout manipulations. However, malicious behavior is not to be under-estimated and shall undoubtedly be considered in our future work. Other classes of reliability model (trust and adversary) are also outside the scope of this paper.

The remainder of this paper is structured as follows. Section 2 shows a brief review on the related work. Section 3 presents an overview of the system model and assumptions. Section 4 provides the detailed design architecture and briefly describes the functions of each BoDMaS component. Section 5 demonstrates the effectiveness of our proposed system and discusses the results. The last section formalizes the conclusion from the work conducted.

2. Related work

ASNET's communication entirely depends on the cooperation of participating users for its successful operation. In the absence of fixed infrastructures in ad-hoc networks, users are necessarily relying on each other to maintain stability. There are two types of ad-hoc networks, namely single-hop and multi-hop [14]. In single-hop networks, receiver is located in sender's direct neighborhood and can be communicated directly since they are located in their radio range. However, in multi-hop networks, receiver is not in the sender's direct neighborhood, and successful communication between these two nodes requires packets to travel through more than one hop before reaching the receiver. Therefore, cooperation of intermediate users in multi-hop networks is essential for effective operation. To gain an insight into the problem and realize such a vital need, several studies have been undertaken, particularly on wireless users' behavioral characteristics that impact on their cooperation in communication networks. Misbehavior has been widely studied in wireless networks [11,19], mobile ad-hoc networks [20,21], peer-to-peer networks [22], vehicular networks [23], delay tolerant networks [24,25] and other forms of networks [26–29]. The existing solutions are built based on reputation, incentive, ACK and game theory with dominant idea to motivate users to cooperate with others in the network.

Gera et al. [20] proposed an opinion-based cooperative trust model in the presence of malicious nodes. With respect to the behavior observed, each node determines the trustworthiness of the other nodes. Their trust model exploits information sharing among nodes to accelerate the convergence of trust establishment procedures, and is further robust against the propagation of false trust information by malicious nodes. However, continuous information sharing overhead is degrading native resources of wireless nodes in the network. The authors in [22] focused on the problem of maintaining significant levels of cooperation in peer-to-peer networks. Their algorithm is adapted from novel "tag" models of cooperation that do not rely on explicit reciprocity, reputation or trust approaches. Another line of work by Li and Cao [25] uses contact records based on which the next contacted node can detect if the node has dropped any packet in order to develop a distributed scheme to detect selfishness in DTNs. The same authors of [25] have published a scheme named SSAR (Social Selfishness Aware Routing) [8], which considers both users' willingness to forward and their contact opportunity to select a forwarding node, resulting in a better forwarding strategy than those based solely on contact. However, in none of these works, focus is given to the selfish attitude of nodes and researchers are trying to motivate cooperation among nodes.

McCoy et al. [19] presented MIND, a reputation-based authentication protocol for identifying and handling misbehaving and malicious users in the neighborhood. In this protocol, each user conducts a continuous follow-up over its neighbor user's forwarding behavior by comparing the incoming and outgoing data of its neighbor. However, this can cause a higher detection rate for false positives. Furthermore, when a user queries its neighbors and if the reply is invalid or fails to reply, the user decides that a neighbor has failed without giving any reason for the failure. In addition to the reputation-based mechanisms, there are some proposals on enforcing collaboration for wireless ad-hoc networks (i.e., [21]), addressing the problem of resilience in the network with the presence of misbehaving users (i.e., [26]) and blacklisting misbehaving users while maintaining the privacy in the network (i.e., [27]).

LeBlanc et al. [26] showed that users' connection or neighborhood is no longer adequate for the assurance of resilient consensus when the users use their own inbuilt nature that only require each user to know its own neighborhood. However, the results in their proposal apply to directed graphs and consider undirected graphs as an exceptional case. In addition to that, they categorize misbehaving users as a restricted type of Byzantine user in which every user is required to send similar message to all of its neighbors which causes the users to consume high energy. On the other hand, Nymble [27] has been proposed with the aim of permitting anonymous blacklisting of misbehaving users. This proposal tries to reinvent the common practice of address banning, without actually telling a user's address. However, this protocol exposed to some sensitive security and trust issues reducing from the usage of trusted third parties that can simply work together to disrupt a user's secrecy.

From Komali et al.'s [28] and Pelechrinis et al.'s [29] perspective, it is difficult to justify the cooperative theory because nodes are either competing for network resources or conserving their own limited resources. Therefore, they proposed an algorithm called DIA (δ-improvement algorithm) in which each node makes some decrements in its power level if the change improves its operation. Their performance evaluation shows that there might be a fundamental conflict between an efficient and fair allocation. It has been shown that it is important to integrate load balancing and fairness preserving mechanisms into misbehavior detection [30], so as to e.g. predict how much resource the user is willing to offer to strangers. However, these algorithms are unable to fulfill unique requirements of ASNETs.

Data management, particularly data availability is one of the most crucial tasks in ASNET environments. Replication is one of the prominent techniques for ensuring the accessibility of data among partitioned communities. Data replication is a technique of creating and managing replica. Replica is a data item that is stored redundantly at multiple communities. Researchers in [6] proposed ComPAS which detailed the means of allocating replicas in different communities in order to increase data availability. However, one of the assumptions in designing the system model is that all the participating users are cooperative in every aspect, such as forwarding read queries and update operations which is not the reality in ASNETs. In order to address challenges emerging from misbehaving users in replication operations for MANETs, Mannes et al. [16] proposed QS^2 by incorporating bio-inspired mechanisms into quorum systems. Quorum systems are powerful mathematical tools to reason about distributed implementations of shared objects including read/write operations [31]. In particular, quorum systems have been used for reasoning in implementations that tolerate misbehavior and are optimally resilient to process failures. More sophisticated forms of quorum systems have been introduced to cope with different failures and these require larger intersections among quorums, eventually leading to an increased overhead.

Drawing from the analogy with existing quorum systems as communities, we believe that applying biologically inspired mechanisms [32,33] in this regard will help to reduce the limitations of existing algorithms. This has also been proved in our previous work [34] related to data forwarding for socially-aware networks. To the best of our knowledge, BoDMaS is the first work to consider social willingness in designing a bio-inspired algorithm to detect and neutralize the impacts of selfish users within dynamically changing network conditions of ASNETs.

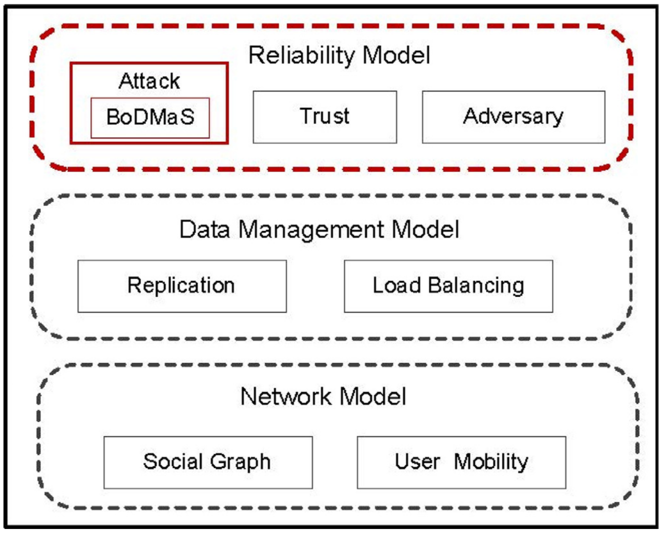


Fig. 2. Simplified ASNET system model.

3. ASNET system model

In this section, we first present the overall model of a simplified ASNET system illustrated in Fig. 2 and explain interlayer interactions and functionality of its major components. Subsequently, we discuss matching analogy between bacteria operation and ASNET functionality. Network model (including social graph and user mobility components), data management model (consisting of replication and load balancing components), and reliability model (comprising attack, trust, and adversary components) are described. The successful operation of ASNET entirely depends on the cooperation among sub-models and components.

3.1. Sub-system models

In this section, we briefly describe sub-system models of a simplified ASNET illustrated in Fig. 2, which can support the requirements for designing protocols/algorithms of ad-hoc social applications in upper layer.

(1) *Network model*: Network in ASNET is modeled using social graph and user mobility. Social networks exhibit the small world phenomenon that node encounters are sufficient to build a connected relationship graph [1,4]. Social graph is an abstract graph where vertices represent individual people and edges describe social ties between individuals. Through the use of a social graph, a variety of social metrics (e.g., social relationship, communality, centrality, and similarity) can be easily calculated. Therefore, it is crucial to obtain social graphs for social-based data management design approaches like ASNETs [6].

We model the social community network as a bidirectional, weighted communication that is symmetrical at every link between users. It means that if a user Y is able to receive a message from user X at time t, then user X can also receive a message from user Y at time t. As in other studies [8,9], this assumption is often valid using selected wireless MAC layer protocols (i.e., IEEE 802.11) that require bidirectional communication for reliable transmission. The network is composed of a vertex set G of all n users/nodes identified by $\{d_0, d_1 \ldots d_{n-1}, d_n\}$, and a set of edges, E, to be the social links between users. Every user $d_i \in G$ has a unique address or identification and the same processor and energy capacity. The weight of edge XY is X's willingness to forward query/update packets for Y . The weight of edge XY and that of YX may be different. In ASNETs, users have limited bandwidth and computational capability. Furthermore, users in multi-hop mode are assumed to rely

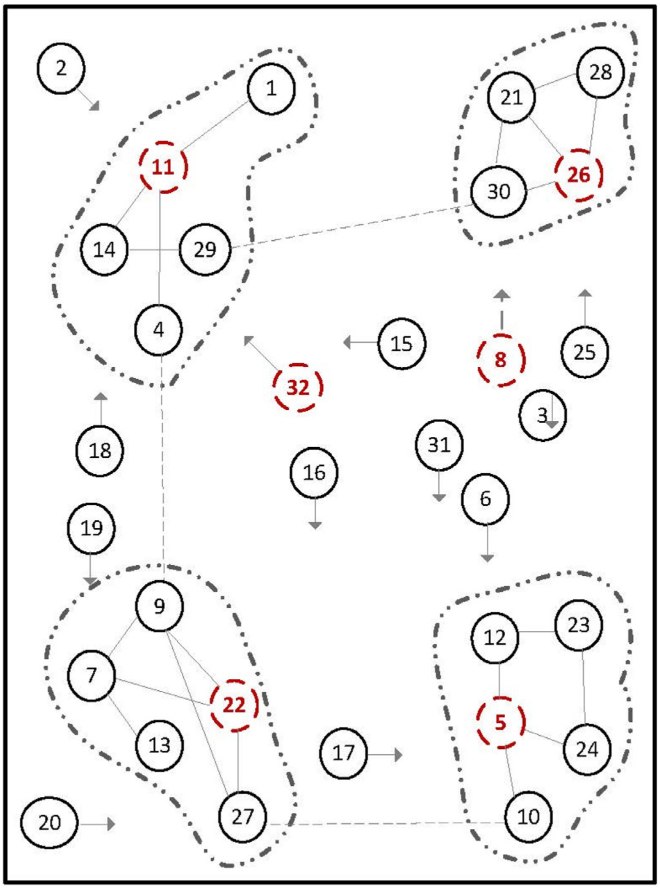


Fig. 3. Illustration of user mobility within an ASNET of 32 users. There are four communities (denoted using the gray dotted lines) and 32 mobile users (denoted using circles), where some users are selfish (represented by the red dashed circles) and some are roaming outside a community (moving directions are represented using arrows). (For interpretation of the references to color in this figure legend, the reader is referred to the web version of this article.)

on intermediate users to route packets since they may not reach directly due to their coverage area [35].

User mobility is another component in modeling ASNET networks. Users move according to the group movement pattern in a surrounded area. Community partitions in the network can occur when the network between the communities fail simultaneously due to movement of users or scarce resources. Group mobility refers to the scenario where several mobile users tend to move together. The system tries to solve the problem of selfishness in replication operations by exploring group mobility. The underlying group mobility model is assumed to be Reference Point Group Mobility Model (RPGM) as used in our previous work [6]. In our system, each mobile user first exchanges its motion behavior with its neighbor based on the social relationship in the community. Mobile users may collaborate and, hence, move as a group instead of independently. RPGM is a better choice to model this kind of team collaboration behavior. As shown in Fig. 3, all users are divided into several mobility groups and all mobile users within the same mobility group are of similar moving behavior [36].

(2) *Data management model*: In ASNETs, replication helps to avoid data losses in case of an unpredictable group mobility that causes community partition and also aids in reducing the number of hops when data is transmitted. By replicating, data availability can be improved, because there are multiple replicas in the network and the probability of finding one copy of the data is high [37]. We employ ComPAS [6] as the data management/replication technique. ComPAS is chosen due to its significant improvement in ASNETs performance since it exploits social relationships while replicating in the community to achieve optimal efficiency and consistency. Further, it can also reduce the query delay, since users can get the data replicas from some nearby communities. Users in this context are capable of performing two types of operations: *query* and *update*.

ComPAS is a system based on partitioning of social community combined with social relationship and a user-level replication so that data availability for all users is guaranteed. The system gives a fixed number of replicas required for each user that results in an efficient replication solution. ComPAS's features a primitive that the most desirable location to replicate a user i is the primary storage place of most of its neighbors, because most neighbors will benefit from this replica when they issue a read query. Furthermore, it aims to find an efficient and consistent way to store X replicas for each user's data in the storage space at Y communities ($X < Y$) and it chooses the value of X depending on the replication budget of the system and its desired availability. For detailed illustration of ComPAS's operation, interested readers can refer to [6].

Load balancing in this model is designed to offload excess load from one user to the others to enable fair and balanced load in the entire community. The significance of load balancing in BoDMaS is that it decreases computing latency caused by an overloaded node in the community. In the absence of load balancing, if a user receives significantly larger number of tasks compared to other nodes, its computing time imposes a noticeable delay on the overall cooperative task. The result of such delay promotes selfishness in the network since cooperative execution of tasks in such scenarios takes longer time.

(3) *Reliability model*: Reliability in ASNET can be verified from a different perspective. In our proposed model, we consider reliability from three perspectives of defining three components of attack, trust, and adversary. As mentioned in the previous sections, among the components our focus is only on the *attack component* (*selfishness*). Selfish users work in the network for their own benefit. They simply do not cooperate with other users in data transmission process to conserve their own energy, or give priority to their own interest. These selfish users disturb the performance of ASNET to a great extent. *Trust* is a critical determinant of sharing information and developing new relationships in a network [38]. Although trust is not our target and it is not essential to our proposed scheme, we assume the source of data is anonymous to intermediate users. Other technical aspects related to trust such as authentication is out of the scope of this paper. Malicious attacks (i.e., modifying or injecting malicious data in the replication system) and free-riding behaviors are grouped in *adversary component*, which are out of the scope of this work. We use different color and border for *attack box* in Fig. 2 to highlight the focus of presented BoDMaS in this article.

3.2. ASNET and bacteria analogy matching

In biological systems, two main entities can be observed [39], namely (1) the organism that collaborates in the biological process (e.g., virus, ants, bees, fish, and bacteria) and (2) the environment (i.e., communities in ASNET). Among these, bacteria have complex social properties resulted from their communication abilities that govern their colony. These social behaviors enable the bacteria to evolve through various fluctuating environmental situations by utilizing cooperative and non-cooperative behaviors [40]. They use quorum sensing to coordinate actions that cannot be carried out by a single bacterium. As individual and limited functionalities, their adjustment to the environment is very limited and therefore they rely on mobility. Quorum sensing can be defined as a decentralized coordination process which allows bacteria to estimate the density of their population and regulate their behavior accordingly by focusing on production and detection of chemical products called Acyl-Homoserine Lactone Autoinducers (AHL-A_i). Each bacterium is similar to a mobile node that extracts information from the environment, interprets the information, develops common knowledge and learns from past experiences [41]. Our proposed algorithm, considers social willingness as a social behavior and the characteristics observed in bacteria as a biological mechanism. AHL-A_i (hereafter A_i for the sake of simplicity and brevity) acts as a signaling chemical gradient to detect and determine the amount of bacteria in the environment, allowing them to develop a collaborative behavior for the whole group that depends on the amount of bacteria engaged. The social behavior existence in both the community and bacteria makes a dynamic and autonomous solution, inspiring the proposed algorithm.

4. BoDMaS: detailed architectural design

Throughput this section, we present the overall architecture of our BoDMaS proposal and describe how BoDMaS fits into the typical ASNET system. We also describe functional interaction among BoDMaS components and provide algorithm pseudo code. We also discuss our model verification approach.

4.1. BoDMaS architecture

BoDMaS aims to detect user's selfishness and counteract it to maintain the reliability of replicated data. Using three major components of behavior assessment, user classification, and user selection & reaction, our proposal detects selfish users and takes actions against the involvement of selfish users in replication operations (i.e., query and update). The behavior assessment is executed by comparing social willingness level and observation of A_i represented by the amount of replica updates, queries, and forwards issued by users. Fig. 4 presents an illustrative view of our proposal consisting three basic components, namely: *behavior assessment*, *user classification* and *user selection & reaction*.

Fig. 5 depicts interaction sequence among these major BoDMaS components. The behavior assessment component adopts and monitors social willingness level for intermediate users. Based on the A_i score from the assessment, the next component evaluates the users in the process. The user classification component uses the score to compare it with the threshold (*Thr*) and identifies users with selfish behavior. Finally, the user selection & reaction component selects cooperative users in order to perform data update and query operations, and takes action against selfishness by notifying other users. The remaining part of this section describes the details of each BoDMaS component.

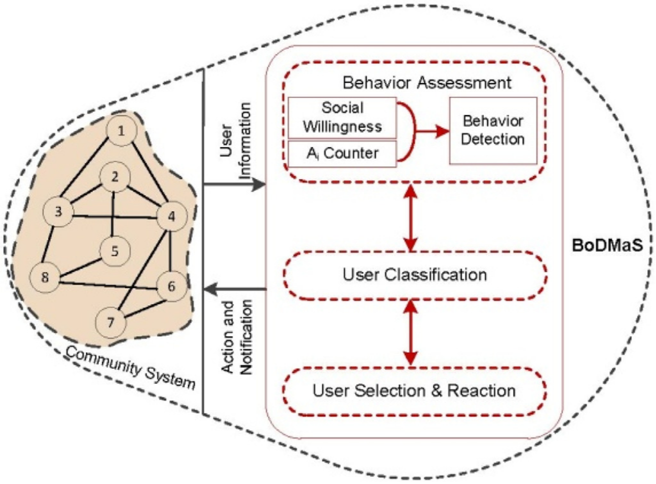


Fig. 4. BoDMaS architecture.

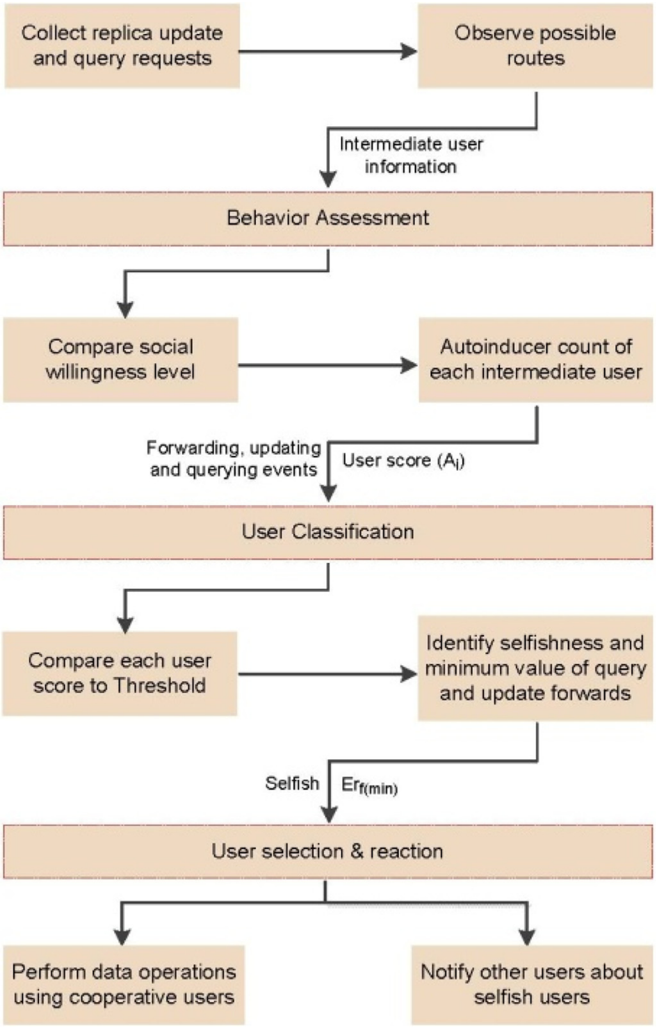

Collect replica update and query requests
Observe possible routes
Intermediate user information
Behavior Assessment
Compare social willingness level
Autoinducer count of each intermediate user
Forwarding, updating and querying events
User score (Aᵢ)
User Classification
Compare each user score to Threshold
Identify selfishness and minimum value of query and update forwards
Selfish
Er_f(min)
User selection & reaction
Perform data operations using cooperative users
Notify other users about selfish users

Fig. 5. Functional interactions among BoDMaS components.

4.2. Behavior assessment

To select an appropriate user for the operation, BoDMaS considers both users' willingness and A_i counts. In our context, a social willingness means an interpersonal social tie between users that falls into the strong or weak range. A selfish user may demonstrate different behavior (cooperative) for users with strong social relationship. That is, the user is willing to provide better service to those with stronger ties than those with weaker ties, especially when there are resource constraints [8]. The work of Li et al. [42] presented three ways of assigning social willingness level: Uniform Distribution of Social Ties (UST), Clustered Distribution of Social Ties 1 (CST1) and Clustered Distribution of Social Ties 2 (CST2). Among these, we use UST that uniformly assigns random values between [0, 1] as willingness level (ρ_{id}) for the friendship between users.

The social willingness level between each pair of users *i* and *d* is characterized by a rational number $\rho_{id} \in [0, 1]$, where $\rho_{id}= 1$ is strongest and $\rho_{id}= 0$ means no willingness at all. Based on this value, the source user chooses the direct neighbor that has strong social tie as an input to the next step. High willingness level does not indicate that the user is not selfish, because there are cases in which the selected neighbor can hold or ignore the received data without doing the job (here is one of the importance of A_i counter). To count replica forward operations $A_{i(f)}$, each user i has A_i counter linked with each neighbor having a social relationship in the community. The counting is conducted based on the communication between users, and occurs when a user receives replica query or update requests. Requesters attach their ID to the packet such that the behavior assessment component can use it to increment $A_{i(f)}$ counter for every user in the line (from source to destination).

4.3. User classification

This component implements users' scores, assigned by the behavior assessment component (and possibly the sequence of operations that led to each score), to identify selfish users in the network. A common approach is to compare the user's score to the *Thr* expected from a cooperative user. In order to get the correct *Thr*, the expected rate of forwards Er_f according to the behavior of replication has to be estimated. This rate is calculated within a given period of time and used to set $A_{i(f)}$ threshold. A user that has A_i count lower than this limit is classified as selfish. Using poisson distribution [31], the minimum query and update forwards ($Er_{f(min)}$) expected for each user is formulated as follows:

$$\sum_{i=0}^{Er_f} \frac{\lambda^{Er_{f(\min)}} \times e^{-\lambda}}{Er_{f(\min)}!} \geq \lambda \qquad (1)$$

where λ represents the probability of users to forward less than $Er_{f(min)}$. Selfish users do not follow this formula.

4.4. User selection & reaction

Finally, this component selects the cooperative users based on the score to perform the data operations. It also informs other users to avoid approaching selfish users. For example, in the case of update operations on replica, suppose that $Er_{f(min)}$ threshold is 3 forwards per second, a user whose score is greater than or equal to 3 is considered cooperative. Users with lower scores are classified as selfish. Algorithm 1 presents detailed BoDMaS operations.

Algorithm 1 Pseudocode for BoDMaS.

```
$\rho_{id}$ ← Social willingness level ($\rho_{id} \in [0, 1]$);
$A_i$ ← Autoinducers count;
$A_i(f)$ ← Autoinducers count for replica forward;
$Thr$ ← Score expected from a cooperative user;
$Er_{f(min)}$ ← Minimum query and update forwards at time $t$;
Behavior assessment:
for all direct neighboring users do
    compares $\rho_{id}$; where 1 is strongest and 0 is none;
    increment $A_i(f)$ counter for every user in the line (from source to destination);
end for
User classification:
for all users' scores collected do
    compare a user's score to a $Thr$;
    if User $A_i$ count < $Thr$ limit then
        classify the user as selfish;
        $Er_{f(min)}$ value is identified;
    end if
end for
User selection & reaction:
take action against users according to their behavior;
if User score ≥ $Er_{f(min)}$ then
    user is considered cooperative;
    perform data operations using cooperative users and notify other users about
    selfish users;
end if
```

To correctly verify the entire model, it is essential to calculate some values such as True Detection Rate (*TDR*) and False Detection Rate (*FDR*). Thus, we employ a set $M(b, r)$, containing all interactions of selfish users and a set $C(b, r)$ representing interactions of cooperative users in both query and update operations where b represents the user class (either selfish or cooperative) after the detection result by BoDMaS and r is the real class of that user. *TDR* represents the amount of detected selfish users and it is calculated using Eq. (2).

$$TDR = \frac{\sum K_i}{|M|} \qquad \forall \quad i \in M \qquad (2)$$

where $K_i = 1$ if $b_i = r_i$ and $K_i = 0$ if $b_i \neq r_i$.

FDR is of two types: False Negative (*FN*) and False Positive (*FP*). *FN* detects the selfish users mistakenly classified as cooperative users. This is calculated using Eq. (3) with all the same *TDR* assumptions.

$$FN = \frac{\sum K_i}{|M|} \qquad \forall \quad i \in M \qquad (3)$$

where $K_i = 1$ if $b_i \neq r_i$ and $K_i = 0$ if $b_i = r_i$. *FP* measures the amount of cooperative nodes classified as selfish as shown in Eq. (4), where C denotes all the cooperative interactions. It is modeled as $C(b, r)$ where $r = 1$ represents a selfish user and $r = 0$ represents a cooperative node.

$$FP = \frac{\sum K_i}{|C|} \qquad \forall \quad i \in C \qquad (4)$$

where $K_i = 1$ if $b_i = r_i$ and $K_i = 0$ if $b_i \neq r_i$. The next section presents performance and efficiency evaluation results.

5. Evaluation

In this section, we present performance and efficiency evaluation of BoDMaS based on accessibility degree, detection rates, and network load balance. Results obtained by the evaluation of ComPAS integrating BoDMaS (represented by ComPAS $\uplus$BoDMaS) is compared to ComPAS without BoDMaS within the same scenarios. The scheme is analysed considering the presence of selfish users in ComPAS operations. The network is composed of 32 users within 4 communities, and users move according to RPGM into an area of 400 m^2. The maximum speed range is 2–20 m/s with a varying pause time of 10–100 s. The expected updating and querying rates are $\lambda = 80$ and $\lambda = 24$, respectively. The forwarding threshold $Er_{f(min)}$ is 0.2 forwards per second. This scenario intends to represent an academic conference environment of mobile users that consists of different participants such as authors, organizers, speakers moving towards some common locations in the conference hall. The information shared concern about the participants' interests, like topics of presentations or keynotes at multiple session rooms. Table 1 summarizes the detailed evaluation parameters we use for simulation to demonstrate the effectiveness of our scheme.

5.1. Accessibility degree

Accessibility degree is the ratio of the number of successful access (query) requests to the number of all access requests issued which is an important metric for replication and reliability protocols. A replication method aims to increase the accessibility of data items in the network. Different from conventional static networks, it is nearly impossible to achieve 100% accessibility degree in ASNETs due to mobility of nodes and changing network topology. To demonstrate effectiveness of integrated ComPAS and BoDMaS (ComPAS $\uplus$ BoDMaS), we run simulation in two modes for accessibility degree; firstly simulation in the presence of selfish users and secondly, simulation in the absence of selfish users. The results of our performance evaluation are depicted in Fig. 6.

Table 1.
Simulation parameters.

Parameter	Value
Number of users	32
Number of communities	4
Defined area	20 × 20 m
Users/community	≈ 8
Number of simulations	10 trials
Simulation time	10 min
User movement	Reference point group mobility model
Maximum speed	2–20 m/s (variable)
Pause time	10–100 s (variable)
Expected updating rate	$\lambda = 80$
Expected querying rate	$\lambda = 24$
Forward threshold	$Er_{f(min)} = 0.2$ forwards per second
Number of selfish users	$N_{selfish} = 2, 4, 8$ and 16 users
Confidence interval	95%

Results of accessibility degree in the absence of selfish users for both ComPAS and ComPAS⊎BoDMaS are illustrated in Fig. 6(a) when maximum speed increases from 2 to 10 m/s. In low speed from 2 to 15 m/s, ComPAS⊎BoDMaS does not show positive accessibility improvement. However, as the maximum speed grows to 20 m/s, the difference is higher (from 85% to 95% for ComPAS and ComPAS⊎BoDMaS, respectively). Evaluation results advocate that the proposed scheme shows a better performance than ComPAS in high speed mobilities, because, distant BoDMaS users (from other users) and those with smaller social willingness (connectivity) are not chosen to participate in the replica query and update operations. This also shows that the proposed scheme enforces a minimal trade-off between accessibility and security.

As displayed in Fig. 6(b), the use of BoDMaS shows an average improvement of 4.31% and 8.94% compared to the accessibility degree obtained by ComPAS without using BoDMaS in update operations for selfish users' participation with 4 and 8, respectively. The numbers of participating selfish users and the maximum speed have visible influence in ComPAS⊎BoDMaS for both operations (Fig. 6(b) and (c)), when compared to ComPAS. However, as depicted in Fig. 6(c), with low variation, the evaluation presents lower results than ComPAS for query operations. This is because effect of selfishness for accessibility degree is less on query operations as compared to update operations. In the remaining part of this section, we focus on demonstrating the effectiveness of the proposed scheme in terms of true and false detection rates for query and update operations as well as network load balance.

5.2. Detection rate

Detection rates obtained by BoDMaS for selfish user in query and update operations are illustrated in Fig. 7(a)–(c) and Fig. 8(a)–(c), respectively. TDR for query and update operations are presented in Figs. 7(a) and 8(a), while FDR (FN and FP) for query and update operations are presented in Fig. 7(b)–(c) and Fig. 8(b)–(c), respectively.

(1) *Query operation:* As depicted in Fig. 7(a), number of selfish users have visible impacts on detection rate results. For instance, with 2 selfish users ($N_{Selfish} = 2$) at a maximum speed of 2 m/s,

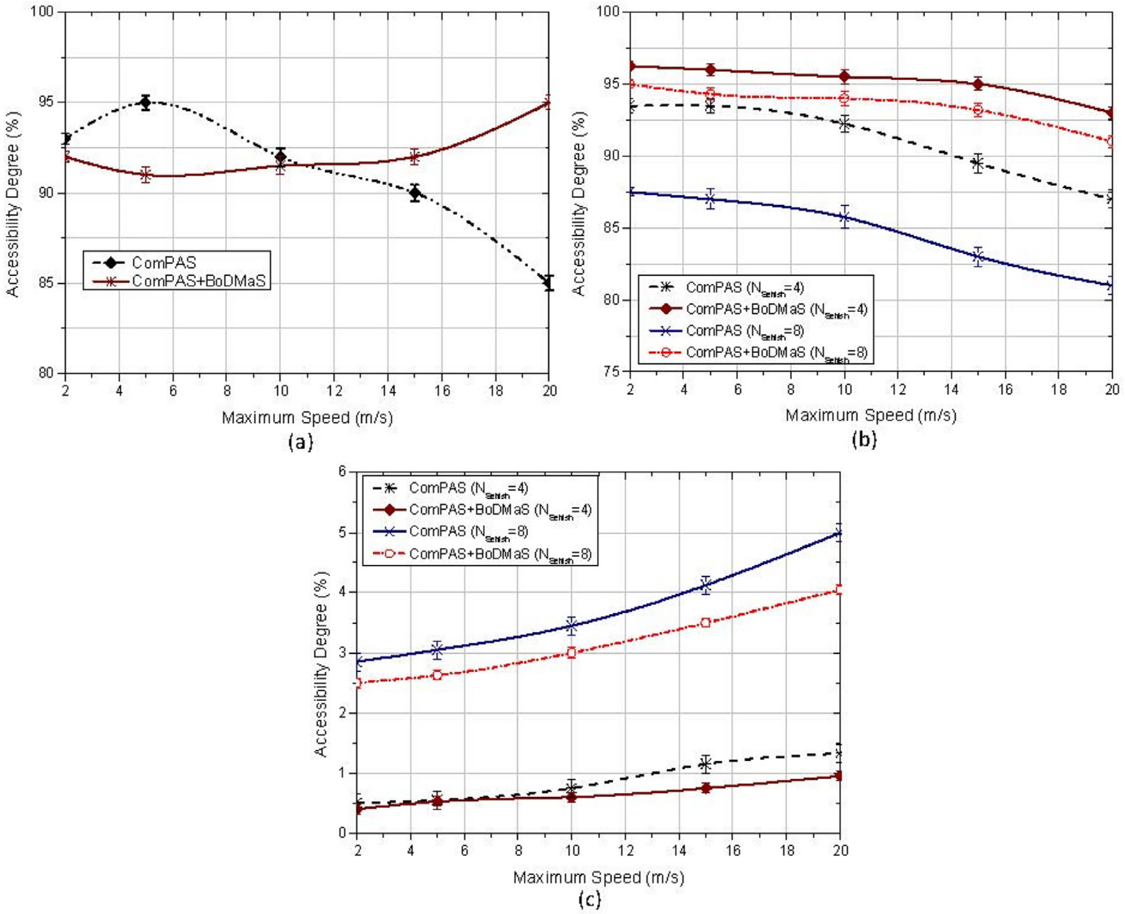


Fig. 6. Accessibility degree for ComPAS⊎BoDMaS and ComPAS; (a) without selfish users participation, and (b) with selfish users participation ($N_{Selfish}$= 4 and $N_{Selfish}$ = 8) in update operations, (c) with selfish users participation ($N_{Selfish}$ = 4 and $N_{Selfish}$ = 8) in query operations.

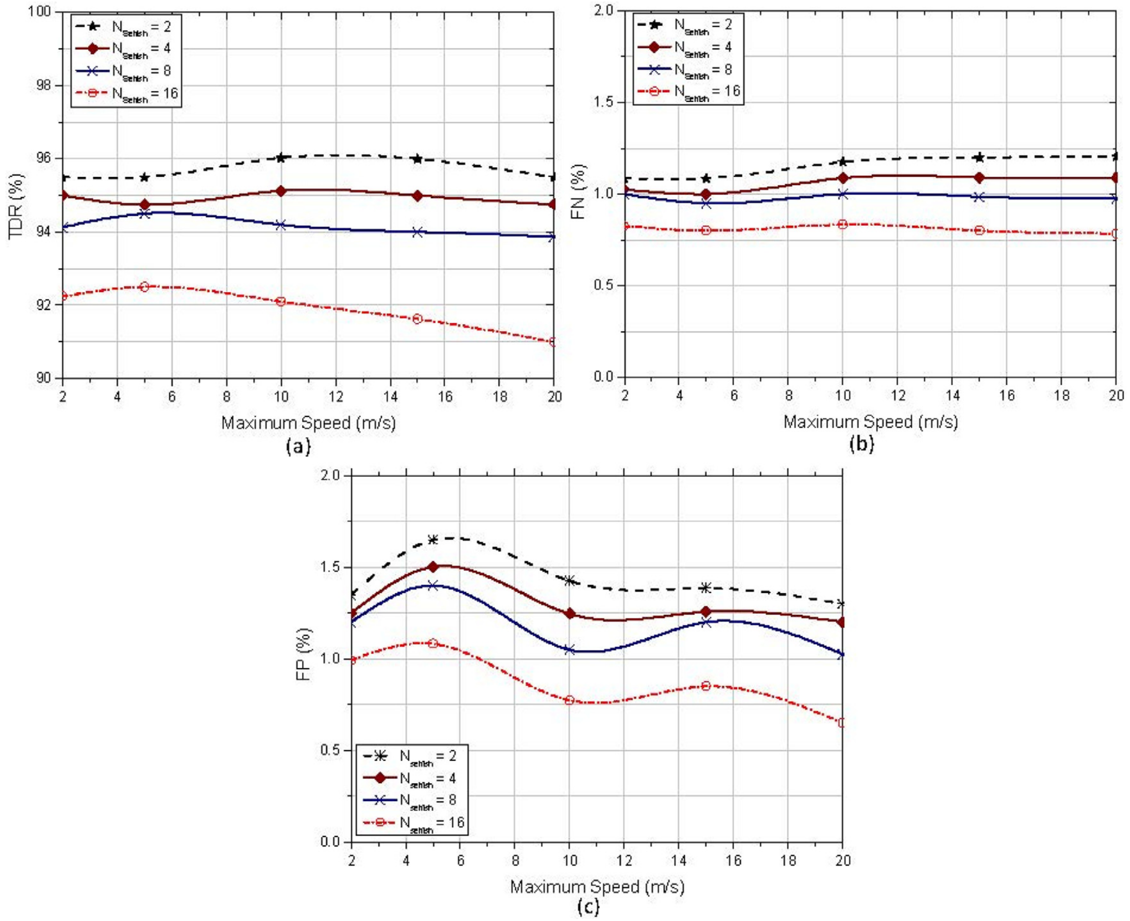


Fig. 7. BoDMaS detection rate of selfishness in query operations; (a) true detection rate (TDR), (b) false negative (FN), and (c) false positive (FP).

5 m/s, 10 m/s, 15 m/s and 20 m/s, the true detection rate for query operation is around 95.5%, 95.6%, 96%, 95.8% and 95.35%, respectively. With 16 selfish users' participation ($N_{selfish} = 16$) at a maximum speed of 2 m/s, 5 m/s, 10 m/s, 15 m/s and 20 m/s, the true detection rate for query operation is around 92.25%, 92.5%, 92.1%, 91.625% and 91%, respectively. However, the TDR of selfish users in query operation for all the cases is higher than 90.95%, because the proposed algorithm continuously assesses the selfish behavior of users and changes its status from selfish to cooperative when user resumes collaboration in forwarding query operations. Fig. 7(b) displays 1.2% lower FN detection rate which shows very small error rate in mistakenly classifying selfish users as cooperative. This is due to the BoDMaS feature that counts A_i, individually. Furthermore, we evaluate FP detection rate as shown in Fig. 7(c) which is also a relatively small rate in mistakenly detecting cooperative users as selfish.

(2) *Update operation:* In order to evaluate the efficiency of BoDMaS during update operation, we simulated operation in varied scenarios with different numbers of selfish users ($N_{Selfish} = 2$, 4, 8 and 16) and analyzed detection rates (i.e., TDR and FDR). Results of our simulation are presented in two ways as shown in Fig. 8(a)–(c). The detection rates with 2 m/s, 5 m/s, 10 m/s, 15 m/s and 20 m/s on update operations are very similar to query operation. We depict them as small charts inside each chart in Fig. 8. Therefore, we suspected how the result shows similarity for these two different operations while there are some users which might be malicious to be considered as selfish due to the timeout manipulation on the data.

Timeout manipulation is considered in our scheme and it is experienced in update operations only. In order to verify this, we run the scheme with participation of 2, 4, 8 and 16 selfish users for continuous maximum speeds in a range of 2–20 m/s. For all the detection rates, this behavior (existence of timeout manipulation on update operation) proved to be true, as seen in Fig. 8(a)–(c). While TDR is higher than 90% for almost all cases, there is a point where this rate goes down below 90% with a speed of around 18 m/s as shown in Fig. 8(a). This is because some users are not considered as selfish, but have the behavior of malicious users happen partly as a timeout manipulation. The same is repeated for false negative and false positive detection rates as depicted in Fig. 8(b) and (c), respectively. This is an evidence to consider and improve the consistency of our scheme in terms of detection rates for update operations. Moreover, BoDMaS obtained good detection rates for update operations with the specified maximum mobility of users in the scenario.

5.3. Network load balance

Network load balance is the ability of our algorithm to balance traffic across users (including the operations) of network scenario without applying load balancing and fairness mechanisms. The evaluations of network load balance are presented in four ways as shown in Fig. 9(a)–(d). The effect of number of selfish users on the network load balance is depicted in Fig. 9(a). The network load balance decreases from 95% to 10% with the increase in the numbers of selfish users participation (from $N_{Selfish} = 2$ to $N_{Selfish} = 16$) due to

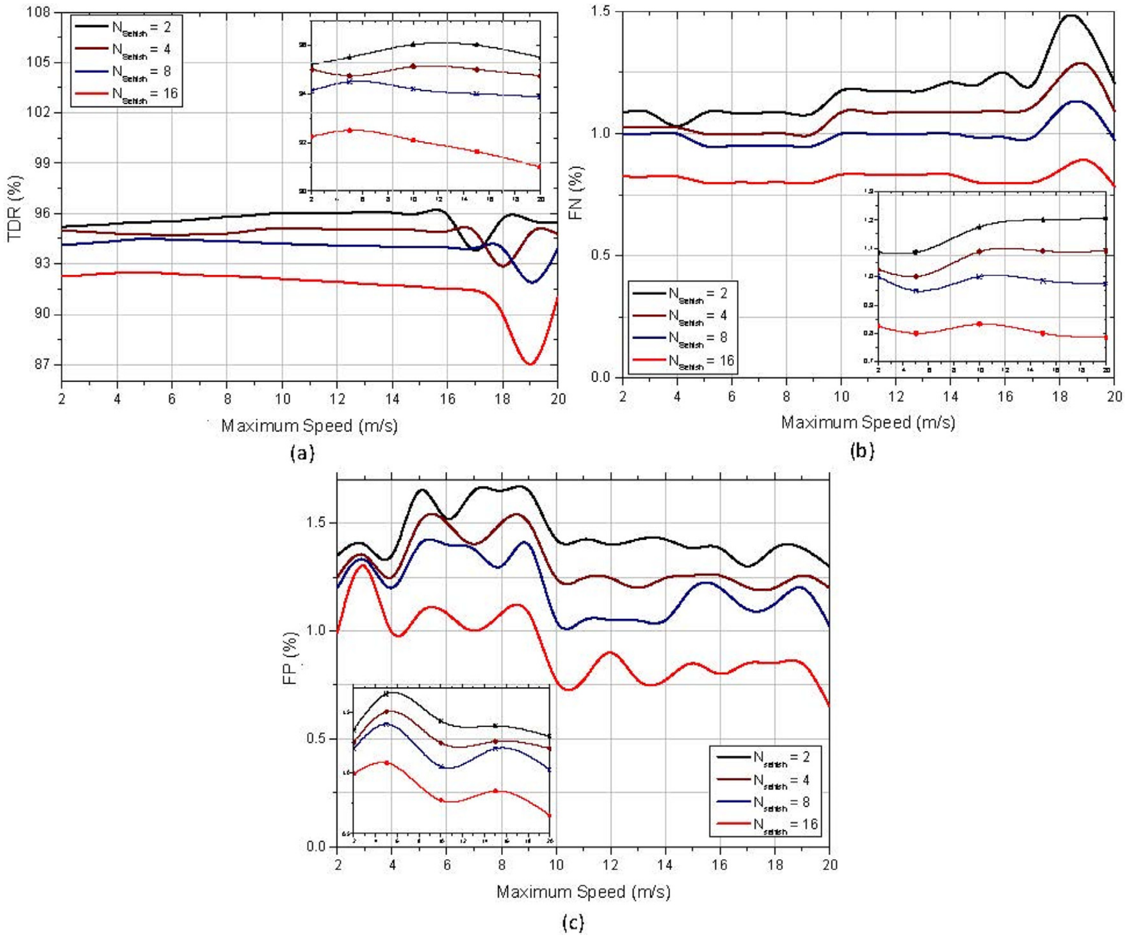


Fig. 8. BoDMaS detection rate of selfishness in update operations; (a) true detection rate (TDR), (b) false negative (FN), and (c) false positive (FP).

resource wastage of selfish users. At speed of 2 m/s, network load balance with 2, 4, 8 and 16 number of selfish users participation is 95.085, 48, 25.0125 and 10.025, respectively. On the other hand, for the maximum speed (20 m/s), it is 95.05, 46.5, 23.5 and 9.35 (messages × hope)/second. However, network load balance does not change when speed changes from 2 m/s to 20 m/s, which means that network load balance in BoDMaS is not much influenced by differences in low and high user mobility. The main reason for this anomaly is that the participation of selfish users has a dominating effect in most cases than the speed of these users.

As described at the very beginning of this section, we set threshold values for forwarding, query, and update rates. Using Fig. 9(b)–(d), we demonstrate the probability of how our choices of the values are comparably successful based on the network load balance even if we only compare with very few values. For instance, as displayed in Fig. 9(b), the network load balance with 0.2 forwarding rate is 61.0085, 66.85, 70.33, 77.895 and 89.933 at speed of 2 m/s, 5 m/s, 10 m/s, 15 m/s and 20 m/s, respectively. It's observed from Fig. 9(c) that network load balance is more efficient at 24 query rate for all mobility cases. Fig. 9(d) also shows the same case where network load balance is achieved effectively for update rate of 80 in all mobility cases. Based on these observations, the ability of our algorithm to balance traffic across users is successful using the threshold values; forward threshold of 0.2, query rate of 24 and update rate of 80 as shown in Fig. 9(b)–(d), respectively. Moreover, unlike Fig. 9(a), the network load balance shows an increasing behavior when the mobility of users (speed) is higher.

Overall, according to the simulation results shown in Figs. 6–9, we have demonstrated the effectiveness of our algorithm in terms of accessibility degree, detection rates (true detection rate and false detection rate) and network load balance.

6. Conclusion

In this paper, we have demonstrated the feasibility and significance of integrating social willingness with quorum sensing (a well-known bio-inspired mechanisms) to detect and counteract selfishness in ASNETs. We introduced BoDMaS, an algorithm that assesses user's social tie with quorum sensing to classify users as either selfish or cooperative. BoDMaS exploits user classification results to inhibit selfish users from performing operation in network and also alert cooperative users to stop forwarding requests to selfish users. For effective evaluation of BoDMaS, we integrate it with ComPAS (a socially-aware replication system that ensures high data availability in ASNETs) and run series of simulations in an academic conference and analyzed three metrics, namely accessibility degree, detection rates, and network load balance. The evaluation results yield high TDR, low FN and FP with fast detection speed leading to enhanced data replication in ASNETs which are evidences of BoDMaS effectiveness. Moreover, BoDMaS is efficient in terms of the ability to balance traffic in varied network scenarios.

In our future work, we aim to enhance consistency of the algorithm for different parameters such as maximum speed and percentage of selfish users. We will also consider malicious users that

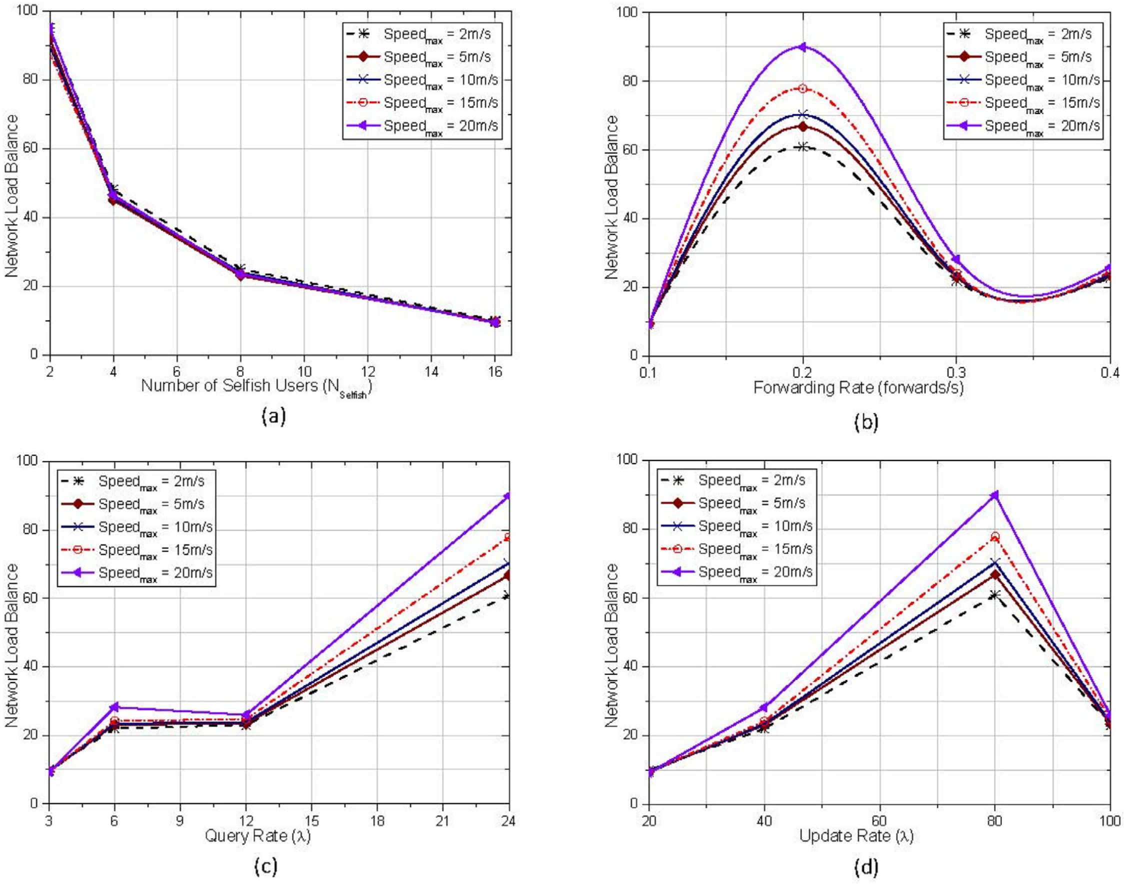


Fig. 9. BoDMaS network load balance efficiency in terms of; (a) number of selfish users ($N_{Selfish}$), (b) forwarding rate, (c) query rate, and (d) update rate.

inject malicious data to the process and evaluate the effectiveness of our system under expanded network environments. We further plan to consider the load of users in the model so that they will have fair distribution of operation requests.

Acknowledgments

This work was partially supported by the Natural Science Foundation of China under Grants no. 61203165 and 61572106, the Natural Science Foundation of Liaoning Province, China under Grants no. 201602154, the Dalian Science and Technology Planning Project under Grant no. 2015A11GX015, and the Fundamental Research Funds for Central Universities under Grants no. DUT15YQ112 and DUT15QY06.

References

[1] F. Xia, L. Liu, J. Li, J. Ma, A.V. Vasilakos, Socially-aware networking: A survey, IEEE Syst. J. 9 (3) (2015) 904–921.

[2] T. Qiu, D. Luo, F. Xia, N. Deonauth, W. Si, A. Tolba, A greedy model with small world for improving the robustness of heterogeneous internet of things, Comput. Netw. 101 (6) (2016) 127–143.

[3] X. Hu, T. Chu, V. Leung, E. Ngai, P. Kruchten, H. Chan, A survey on mobile social networks: Applications, platforms, system architectures, and future research directions, IEEE Commun. Surv. Tutor. 17 (3) (2015) 1557–1581.

[4] A.M. Ahmed, F. Xia, N.Y. Asabere, H.B. Liaqat, J. Li, Social community-partition aware replica allocation in ad-hoc social networks, in: Proceedings of the 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing (GREENCOM-ITHINGS-CPSCOM '13), 2013, pp. 834–841.

[5] S. Balasubramaniam, K. Leibnitz, P. Lio, D. Botvich, M. Murata, Biological principles for future internet architecture design, IEEE Commun. Mag. 49 (7) (2011) 44–52.

[6] F. Xia, A.M. Ahmed, L.T. Yang, J. Ma, J. Rodrigues, Exploiting social relationship to enable efficient replica allocation in ad-hoc social networks, IEEE Trans. Parallel Distrib. Syst. 25 (12) (2014) 3167–3176.

[7] M. Eirinaki, M.D. Louta, I Varlamis, A trust-aware system for personalized user recommendations in social networks, IEEE Trans. Syst. Man Cybern. Syst. 44 (4) (2014) 409–421, doi:10.1109/TSMC.2013.2263128.

[8] Q. Li, S. Zhu, G. Cao, Routing in socially selfish delay tolerant networks, in: Proceedings of the Twenty-ninth Conference on Information Communications, 2010, pp. 1–9.

[9] K. Gopalakrishnan, V.R. Uthariaraj, Scenario based evaluation of the impact of misbehaving nodes in mobile ad hoc networks, in: Proceedings of the First International Conference on Advanced Computing, 2009, pp. 45–50.

[10] S. Abolfazli, Z. Sanaei, M. Alizadeh, A. Gani, F. Xia, An experimental analysis on cloud-based mobile augmentation in mobile cloud computing, IEEE Trans. Consum. Electr. 60 (1) (2014) 146–154.

[11] J. Choi, A.W. Min, K.G. Shin, A lightweight passive online detection method for pinpointing misbehavior in WLANs, IEEE Trans. Mob. Comput. 10 (12) (2011) 1681–1693.

[12] M.T. Refaei, L.A. DaSilva, M. Eltoweissy, T. Nadeem, Adaptation of reputation management systems to dynamic network conditions in ad hoc networks, IEEE Trans/ Comput. 59 (5) (2010) 707–719.

[13] U. Venkanna, R.L. Velusamy, Mitigating the attacks on recommendation trust model for mobile ad hoc networks, in Proc. ERCICA (2013) 123–130.

[14] N. Kang, E.M. Shakshuki, T.R. Sheltami, Detecting Misbehaving Nodes in MANETs, in: Proceedings of the 2010 International Conference on Information Integration and Web-based Applications and Services (IIWAS' 10), 2010, pp. 216–222.

[15] K. Akkarajitsakul, E. Hossain, D. Niyato, Coalition-based cooperative packet delivery under uncertainty: A dynamic Bayesian coalitional game, IEEE Trans. Mob. Comput. 12 (2) (2013) 371–385.

[16] E. Mannes, M. Nogueira, A.D. Santos, A bio-inspired scheme on quorum systems for reliable services data management in MANETS, in: Proceedings of the 2012 IEEE Network Operations and Management Symposium (NOMS), 2012, pp. 278–285.

[17] S. Djahel, F. Nait-Abdesselam, Z. Zhang, Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges, IEEE Commun. Surv. Tutor. 13 (4) (2011) 658–672.

[18] A.M. Ahmed, F. Xia, Q. Yang, H.B. Liaqat, Z. Chen, T. Qiu, Poster: Bacteria inspired mitigation of selfish users in ad-hoc social networks, in: Proceedings of the Fifteenth ACM international symposium on Mobile ad hoc Networking and Computing (MobiHoc), 2014, pp. 421–422.

[19] D. McCoy, D. Sicker, D. Grunwald, A mechanism for detecting and responding to misbehaving nodes in wireless networks, in: Proceedings of the Second IEEE Workshop on Networking Technologies for Software Define Radio Networks, 2007, pp. 678–684.

[20] P. Gera, K. Garg, M. Misra, Eliminating misbehaving nodes by opinion based trust evaluation model in MANETs, in: Proceedings of the 2011 International Conference on Communication, Computing and Security (CCS), 2011, pp. 50–55.

[21] N. Jiang, K.A. Hua, D. Liu, A scalable and robust approach to collaboration enforcement in mobile ad-hoc networks, J. Commun. Netw. 9 (1) (2007) 56–66.

[22] D. Hales, B. Edmonds, Applying a socially inspired technique (tags) to improve cooperation in P2P networks, IEEE Trans. Syst. Man Cybern. Part A Syst. Hum. 35 (3) (2005) 385–395.

[23] M. Raya, P. Papadimitratos, I. Aad, D. Jungels, J.P. Hubaux, Eviction of misbehaving and faulty nodes in vehicular networks, IEEE J. Sel. Areas Commun. 25 (8) (2007) 1557–1568.

[24] Y. Li, G. Su, D.O. Wu, D. Jin, L. Su, L. Zeng, The impact of node selfishness on multicasting in delay tolerant networks, IEEE Trans. Veh. Technol. 60 (5) (2011) 2224–2238.

[25] Q. Li, G. Cao, Mitigating routing misbehavior in disruption tolerant networks, IEEE Trans. Inf. Forensics Secur. 7 (2) (2012) 664–675.

[26] H.J. LeBlanc, H. Zhang, X. Koutsoukos, S. Sundaram, Resilient asymptotic consensus in robust networks, IEEE J. Sel. Areas Commun. 31 (4) (2013) 766–781.

[27] P.P. Tsang, A. Kapadia, C. Cornelius, S.W. Smith, Nymble: Blocking misbehaving users in anonymizing networks, IEEE Trans. Dependable Secur. Comput. 8 (2) (2011) 256–269.

[28] R.S. Komali, A.B. MacKenzie, R.P. Gilles, Effect of selfish node behavior on efficient topology design, IEEE Trans. Mob. Comput. 7 (9) (2008) 1057–1070.

[29] K. Pelechrinis, G. Yan, S. Eidenbenz, S.V. Krishnamurthy, Detection of selfish manipulation of carrier sensing in 802.11 networks, IEEE Trans. Mob. Comput. 11 (7) (2012) 1086–1101.

[30] F. Xia, A.M. Ahmed, L.T. Yang, Z. Luo, Community-based event dissemination with optimal load balancing, IEEE Trans. Comput. 64 (7) (2015) 1857–1869.

[31] J. Luo, J.P. Hubaux, P.T. Eugster, PAN: Providing reliable storage in mobile ad hoc networks with probabilistic quorum systems, in: Proceedings of the Fourth ACM international symposium on Mobile ad hoc Networking and Computing (MobiHoc), 2003, pp. 1–12.

[32] S. Khan, J. Lloret, E. Macias-López, Bio-inspired mechanisms in wireless sensor networks, Int. J. Distrib. Sens. Netw. 2015 (173419) (2015).

[33] S. Sendra, L. Parra, J. Lloret, S. Khan, Systems and algorithms for wireless sensor networks based on animal and natural behavior, Int. J. Distrib. Sens. Netw. 2015 (625972) (2015).

[34] F. Xia, L. Liu, J. Li, A.M. Ahmed, L.T. Yang, J. Ma, BEEINFO: An interest-based forwarding scheme using artificial bee colony for socially-aware networking, IEEE Trans. Veh. Technol. (2014) In Press, doi:10.1109/TVT.2014.2305192.

[35] H.B. Liaqat, F. Xia, J. Ma, L.T. Yang, A.M. Ahmed, N.Y. Asabere, Social similarity-aware TCP with collision avoidance in ad hoc social networks, IEEE Syst. J. 9 (4) (2015) 1273–1284.

[36] A.M. Ahmed, T. Qiu, F. Xia, B. Jedari, S. Abolfazli, Event-based mobile social networks: Services, technologies and applications, IEEE Access 2 (2014) 500–513.

[37] A. Derhab, N. Badache, Data replication protocols for mobile ad-hoc networks: A Survey and taxonomy, IEEE Commun. Surv. Tutor. (2009) 33–51.

[38] Y. Najaflou, B. Jedari, F. Xia, L.T. Yang, M.S. Obaidat, Safety challenges and solutions in mobile social networks, IEEE Syst. J. 9 (3) (2015) 834–854.

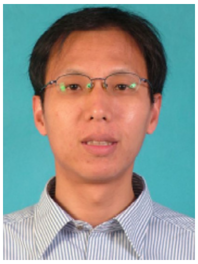
[39] J.L. Fernandez-Marquez, G.D.M. Serugendo, S. Montagna, M. Viroli, J.L. Arcos, Description and composition of bio-inspired design patterns: A complete overview, Nat. Comput. 12 (1) (2013) 43–67.

[40] M. Hassan, E. Hossain, S. Balasubramaniam, Y. Koucheryavy, Social behavior of bacterial nano-networks: Challenges and opportunities, IEEE Netw. Mag. 29 (1) (2015) 26–34.

[41] A. Einolghozati, M. Sardari, A. Beirami, F. Fekri, Data gathering in networks of bacteria colonies: Collective sensing and relaying using molecular communication, in: Proceedings of the 2012 IEEE Workshops on INFOCOM, 2012, pp. 256–261.

[42] H. Li, C. Wu, Z. Li, W. Huang, F.C. Lau, Stochastic optimal multirate multicast in socially selfish wireless networks, in: Proceedings of the 2012 IEEE INFOCOM, 2012, pp. 172–180.

Ahmedin Mohammed Ahmed received his B.S. degree in Computer Science in 2006 from Bahirdar University, Ethiopia, his Master degree in Software Engineering from Chongqing University, China in 2011 and Ph.D. degree from Mobile and Social Computing Laboratory of School of Software, Dalian University of Technology, China in 2015. He has been working as Assistance Professor of Computing in Kombolcha Institute of Technology, Wollo University, Ethiopia. He is also serving as Scientific Director of Kombolcha Institute of Technology, Wollo University, Ethiopia. He is a member of IEEE Society. His research interests include mobile and social computing, ad-hoc social networks, data management, middleware design, and smart community.



Xiangjie Kong received the Ph.D. degree from Zhejiang University, Hangzhou, China in 2009. Currently, he is an Associate Professor in School of software, Dalian University of technology, China. He has served as Editor Board Member of SpringerPlus, Guest Editor of several international journals, Workshop Chair or PC Member of a number of conferences. He has published over 30 scientific papers in international journals and conferences (with 20+ indexed by ISI SCIE). His research interests include big traffic data, social computing, and cyber-physical systems. He is a Member of IEEE and ACM.

Li Liu received the B.S. and M.S. degree in Computer Science and Technology from Shandong University of Science and Technology, Qingdao, China, in 2001 and 2004, respectively, and Ph.D. degree from Dalian University of Technology, China in 2015. She has been working at Shandong Jiaotong University, Jinan, China since 2004. Her research interests include opportunistic networks, socially-aware networking and mobile social networks.

Feng Xia received the B.Sc. and Ph.D. degrees from Zhejiang University, Hangzhou, China. He was a Research Fellow at Queensland University of Technology, Australia. He is currently a Full Professor in School of Software, Dalian University of Technology, China. He is the (Guest) Editor of several international journals. He serves as General Chair, PC Chair, Workshop Chair, or Publicity Chair of a number of conferences. He has published 2 books and over 200 scientific papers in international journals and conferences. His research interests include computational social science, big data, and mobile social networks. He is a Senior Member of IEEE (Computer Society, SMC Society) and ACM (SIGWEB), and a Member of AAAS.

Saeid Abolfazli is currently a research lead and data scientist at YTL Communications and Xchanging Malaysia where he is responsible for research and development efforts around business intelligence. He is also serving as associate editor of IEEE Transactions on Cloud Computing. He has completed Ph.D. from University of Malaya in 2014 where he was a part time lecturer and research assistant in High Impact Research Project (Mobile Cloud Computing: Device and Connectivity) fully funded by Malaysian Ministry of Higher Education. He received his M.Sc. (Information Systems) in 2008 from India and BE (Software Engineering) in 2001 from Iran. He has authored more than 40 research articles in prestigious international venues. His works are cited more than 450 times and his h-index reached 10 in less than 3 years. He continuously serves as organizing committee member and technical reviewer for top tier international conferences, including IEEE ISSRE and IEEE STC. He serves as reviewer in top CS journals, including IEEE TPDS, IEEE TMC, IEEE TCC, and IEEE/ACM TOMM. Dr. He is a member of IEEE society and IEEE CS Cloud Computing STC. His main research interests including big data and business intelligence, artificial intelligence, Enterprise IT, mobile cloud computing, resource scheduling, and service oriented computing.

Zohreh Sanaei is currently data scientist and computer science researcher working in business intelligence team at YTL Communications and Xchanging Malaysia. She has completed Ph.D. with distinction award from University of Malaya in 2014 where she was a research assistant in High Impact Research Project (Mobile Cloud Computing: Device and Connectivity) fully funded by Malaysian Ministry of Higher Education. She is also serving as an external reviewer of proposals submitted for Scientific and Technological Development's National Fund, technical reviewer for top journals and conferences (IEEE/ACM), and guest editor of Mobile Information systems on special issue of Mobile Cloud Computing. She has authored over 30 publications and one book chapter. She is one of the highly cited authors in mobile cloud computing area with more than 540 times and h-index 10 in 3 years of research. She is a member of IEEE society and IEEE CS Cloud Computing STC. Her main research interests including data analysis and statistics, big data and business intelligence, artificial intelligence, Enterprise IT, mobile cloud computing, resource scheduling, and service oriented computing.

Amr Tolba received the M.Sc. and Ph.D. degrees from Mathematics and Computer Science Department, faculty of science, Menoufia University, Egypt, in 2002 and 2006 respectively. He is currently onleave from Menoufia Univesity to Computer Science Department, Riyadh Community College, King Saud University (KSU), Saudi Arabia as Assistant Professor. His main research interests include Social Network Analysis, internet of things, ad hoc networks, intelligent systems, recommender systems, e-learning, and cloud computing.