Hindawi
Wireless Communications and Mobile Computing
Volume 2018, Article ID 8612817, 16 pages
https://doi.org/10.1155/2018/8612817

Research Article

Effect of User Mobility upon Trust Building among Autonomous Content Routers in an Information-Centric Network

Jerzy Konorski and Jakub Grochowski

Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology, Poland

Correspondence should be addressed to Jerzy Konorski; jekon@eti.pg.gda.pl

Received 10 June 2018; Revised 25 October 2018; Accepted 28 October 2018; Published 19 November 2018

Academic Editor: Rüdiger C. Pryss

The capability of proactive in-network caching and sharing of content is one of the most important features of an information-centric network (ICN). We describe an ICN model featuring autonomous agents controlling the content routers. Such agents are unlikely to share cached content with other agents without an incentive to do so. To stimulate cooperation between agents, we adopt a reputation and trust building scheme that is able to explicitly account for both objective current content availability and subjective willingness to cooperate. The scheme is further complemented with a so-called one-time goodwill mechanism introduced to avoid penalizing agents failures to provide temporarily unavailable content. In a simulated ICN environment under a modified Random Waypoint user mobility model, we investigate the resiliency of the reputation and trust building scheme to subversion, that is, strategic (selfish or malicious) agents acquiring higher trust values than honest ones, for varying user mobility scenarios. The scheme proves resilient in low-mobility scenarios, while increased user mobility is shown to have a negative effect. The one-time goodwill mechanism partly remedies this for high-mobility scenarios. We validate the results by comparison with an existing reputation and trust building scheme and with an alternative user mobility model.

1. Introduction

Information-centric network (ICN) is a content delivery-oriented network architecture that aims to better suit the needs of contemporary network users, typically interested in obtaining specific information rather than establishing a connection with a specific network site hosting this information. The concept of ICN is especially useful now that the Internet has become a truly large-scale network accessible from almost every household. New network paradigms are being developed to facilitate content delivery which employ elaborate content caching schemes. Content caching allows for content to be saved locally, close to the interested end users, thus reducing the need for resource intensive on-demand routing and transfer of large files or streams. Content caching is effective if performed cooperatively, that is, when network nodes are coordinating and sharing cache contents with each other. However, while in a centrally controlled network such node behavior can be enforced, large-scale networks are likely to have parts of their functionality governed by fully or partially independent logical entities located at the nodes and controlling their behavior. These entities are able to make autonomous (in particular, selfish) decisions within the bounds of their assigned functionality and thus can be regarded as autonomous rational agents.

An autonomous agent has to be incentivized to provide content to users directly connected to the node it controls. A form of benefit (e.g., payment or compensation) for the agent should therefore be envisaged. Obviously, routing and transferring content through the network cause increased network resource usage and delays that diminish user satisfaction. Hence, an agent looks for content requested by a user above all in its local cache and, should this fail, interacts with nearby nodes to request access to their caches. However, since sharing cache content with other agents in itself does not generate any benefit, autonomous agents need additional incentives. Reputation-based trust building schemes [1–3] yield an effective solution provided that high reputation an agent earns by cooperating (sharing cached content) during interactions with a subset of agents is rewarded by

cooperation also on the part of those agents with whom the agent in question has not interacted. Such a presumption is called *indirect reciprocity* and underlies most existing reputation systems, as well as many biological, economic, and sociological models of autonomous agents [1, 4–6].

In this paper, we investigate the effects of a reputation and trust building scheme first introduced in [7], adapted to the goal of promoting cooperative behavior (i.e., sharing cache contents) in an ICN environment with autonomous agents. The scheme relies upon indirect reciprocity and features network-wide propagation of agents' trust values which reflect an agent's willingness to cooperate with others. Agents have an incentive to cooperate with other agents of high trust values, as it implies that they themselves will receive high trust values which will induce third-party agents to share content with them. To avoid penalization of agents failing to provide requested content due to its temporary unavailability rather than ill will, we complement the scheme with a *one-time goodwill* mechanism whereby an agent stores a list of content requested and provided in the past and occasionally disregards failure to provide content not yet requested. An implementation of the scheme in a simulated ICN environment is presented and its effectiveness is measured for scenarios with varying parameters of user mobility. Note that increased user mobility is likely to result in frequent requests for temporarily unavailable content (which a requested agent has not yet had the time to cache), which in turn may build an impression of ill will shown by well-behaved agents. Our main findings make for a better understanding of the effect user mobility has on the resiliency of the trust and reputation building scheme to *subversion*, an undesirable condition whereby well-behaved agents receive lower trust values than those exhibiting selfish behavior. The presented results are validated through a comparison with an existing reputation and trust building scheme and with an alternative user mobility model. We believe this contribution will help in designing future reputation schemes to promote interagent cooperation in ICN environments where user mobility may seriously affect the system operation.

The rest of the paper is organized as follows. In Section 2, we briefly discuss related work. Section 3 presents the details of the considered ICN model and outlines the basics of the employed reputation and trust building scheme. Using simulation applied to a public Dropbox Traces dataset, in Section 4, we evaluate the effects of user mobility, discuss the obtained results, and compare them with some alternative solutions. Section 5 concludes the paper.

2. Related Work

A number of ICN architectures have been proposed and evaluated so far, including DONA [8] and Content-Centric Networking (CCN) [9] and its later extensions: Named Data Networking (NDN) [10], PURSUIT [11], or SAIL [12]. Mobility in ICNs is a topic that attracted much attention, however, as yet no proposed solution has been widely accepted. Many research teams focus their studies on a model with user mobility and wired node-to-node communications [13, 14]. However, few studies on implementing ICN in a fully mobile and opportunistic network have been performed [15, 16].

Several existing studies focus on incentives for sharing cached content in ICNs populated by noncooperative agents. For example, in [17], a system was suggested and implemented, in which selfish nodes form a group that jointly determines contents of each individual node's cache and shares cache contents within the group for increased individual gain. Other studies formulate game models assuming that players receive compensation in return for caching specific content [18, 19]. An evolutionarily stable cooperation strategy in a peer-to-peer (P2P) environment using BitTorrent has been proposed under the name of iRep [20]; it consists in first enabling connections with neighbor agents of higher trust values, as derived from prior content transfers.

Reputation and trust building schemes are a thoroughly studied topic in the context of multiagent environments with autonomous noncooperative agents such as e-commerce and P2P systems or distributed wireless networks [2, 3]. The raison d'être of reputation building is indirect reciprocity, a well-known assumption [1, 4–6] whose validity is sometimes questioned on formal grounds but often demonstrated experimentally [4]. The scheme employed in our research was introduced in [7] in an abstract environment and aims to distinguish honest agents that abide by the set content sharing rules from strategic agents that attempt to reduce the cost of content sharing while retaining high trust values. An advantage of the scheme is that it explicitly models current content availability and thus more precisely accounts for ill will dictating refusal to share content even though it is available. To the best of our knowledge, no prior work exists on implementation of a reputation and trust building scheme with such a property in an ICN environment with autonomous agents and mobile users. Still, for the sake of comparing the presented scheme with existing work, in Section 4.4, we refer to a scheme proposed in [21] which, although not intended for ICN (instead, designed in the context of the Social Internet of Things), bears enough similarity to ours to enable a fair comparison.

3. Model

ICN is a network architecture paradigm meant to respond to the challenges of the contemporary and future Internet, which is increasingly used for accessing and exchanging information rather than for establishing end-to-end communication between hosts. In other words, users are more interested in obtaining a specific piece of information (further referred to as an *information object*) than in connecting to a specific host; the latter may be necessary but just as a means to an end. As such, the focus of ICN is on information itself, naming information at the network layer and disassociating information from the site (e.g., server) that is hosting it. From the network perspective, a specific information object is treated in the same way regardless of its hosting site's identity. This enables information mobility, caching information at locations close to interested users, vast improvement of information delivery, and reducing the

need for time- and resource-intensive information routing and transfer. The same approach was taken by the earlier Content Delivery Networks [22], an overlay on top of existing Internet architecture. The ICN approach is to instead create new network architectures, with an outlook for eventually replacing the Internet architecture of today.

3.1. Network Entities. The ICN architecture used in our work is based on Named Data Networking (NDN). It assumes existence of three types of network entities:

(i) *Publishers* are responsible for storing available information objects and sharing them with interested parties

(ii) *Subscribers* are the users who generate requests for access to specific information objects and have an option of introducing new information objects into the network by sending them to specific Publishers for storage; it is assumed that every information object available in the network first has been introduced by some Subscriber

(iii) *Content Routers* (CRs), also referred to as *nodes*, are responsible for maintaining the communication backbone of the network by connecting to Publishers and Subscribers, as well as to one another, and for hop-by-hop forwarding of relevant messages

3.2. Message Types. The model assumes that two types of messages are exchanged between the network entities:

(i) *Interest*: generated by a Subscriber as a request for a specific information object (identified in the message) to be delivered to the Subscriber. The message is forwarded hop-by-hop by CRs towards the Publisher in possession of the object, until either the Publisher is reached or one of the forwarding CRs finds the information object in its cache. The latter is preferable from a network designer's point of view, as it means the request is fulfilled in a shorter time and consumes less network resources (e.g., bandwidth) [23]

(ii) *Data*: contains a specific information object. Our model differentiates between two subtypes: a *regular Data* message is generated either by a Publisher or a CR as a response to an *Interest* message. It is then routed in the direction from which the *Interest* message arrived, traversing the same path in the opposite direction until reaching the originating Subscriber [22]. The second subtype is *Subscriber-generated Data* messages generated when a Subscriber decides to make new content available in the network by sending it to a specific Publisher. In addition to information objects, this type of message contains the identity of the Publisher to which it is being sent. This second subtype of *Data* messages does not exist in typical NDN implementations, which assume that Subscribers are only able to generate *Interest* messages

3.3. Content and Flows. Content available in the network consists of pieces of information (e.g., files), each of which is assumed to be divided into small equal-size segments represented by one uniquely named information object. The object naming scheme is not strictly specified here, with the understanding that the requirement of network-wide name uniqueness is met. Hence, when a Subscriber wishes to receive specific content, it needs to generate an *Interest* message for each individual information object that is part of that content. Likewise, in order to send content through the network, a *Data* message needs to be generated for every object that is part of the content. We define a *flow* as a sequence of messages of the same type (either *Data* or *Interest*) related to a specific Subscriber which either has requested or is the recipient of the corresponding information objects and a specific Publisher responsible for storing these information objects. A flow may encompass more than one piece of content (e.g., several files), as long as the identities of the Publisher and Subscriber remain the same and all information objects contained or requested in the flow's messages are unique. Therefore, requesting or sending specific content through the network is likely to generate a flow of multiple messages, unless the content is represented by only one information object.

3.4. Data Structures at CRs. Each CR (node) maintains three data structures: *Content Store* (CS), *Forwarding Information Base* (FIB), and *Pending Interest Table* (PIT). Figure 1 illustrates their usage when routing *Data* and *Interest* messages, and Figure 2 details their usage when handling messages at CRs.

(i) CS is the node's cache: when a *Data* message is routed through the node, depending on the decision of the agent managing the cache, the data (information object) may be saved in the node's CS. Should the object's size exceed the currently free space in the CS, some objects saved in the CS may be removed at the managing agent's discretion. Since each piece of content is represented by one or more information objects, it is possible for specific content to be only partially present in CS

(ii) FIB contains the necessary routing directions: it maps available information objects to visible neighbors, to whom a pertinent *Interest* message must be sent so that it will eventually arrive at the Publisher in possession of that object. Moreover, identities of specific Publishers are mapped to visible neighbors as well, to ensure that *Subscriber-generated Data* messages arrive at their destination. Each CR's FIB needs to be updated whenever new information objects become available in the network

(iii) PIT tracks requests that have been routed through the CR and have not yet been fulfilled; when an *Interest* message arrives at the node, it tries to fulfill the request by checking the content in its CS and responding with a *Data* message containing an appropriate information object if found. Should the

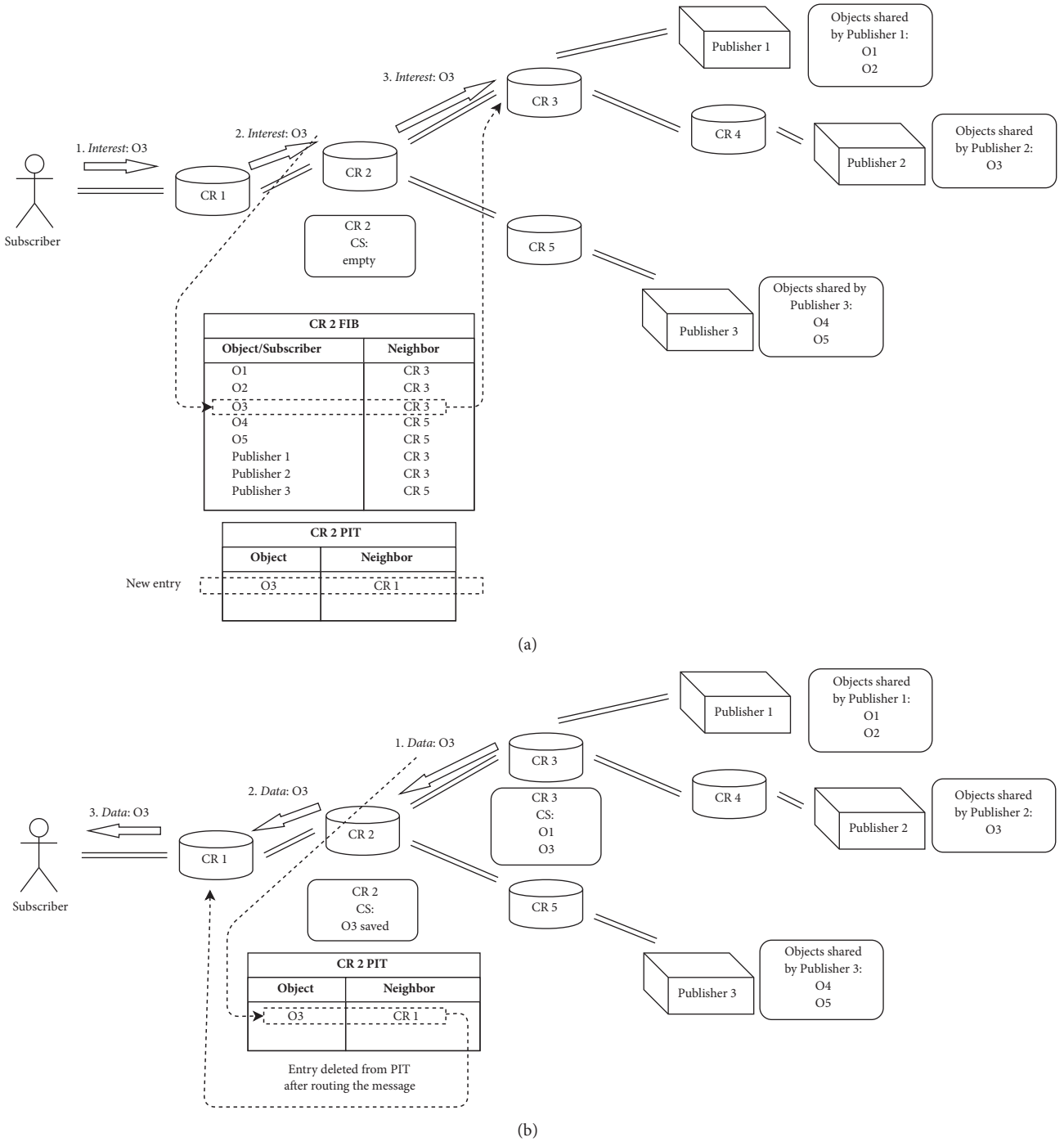

Figure 1: Examples of message routing: (a) *Interest,* (b) *Data* (O*x*: information objects, CR: Content Router, CS: Content Store, FIB: Forwarding Information Base, PIT: Pending Interest Table).

object not be found, the *Interest* message is routed in the direction indicated by FIB, and a new entry containing the direction from which this message arrived as well as the content it requested for is added to PIT. When a *Data* message moves through the node, it is routed in the directions indicated by the PIT entries related to the message's content. These entries are then removed from PIT with the understanding that the requested information object will have been sent towards the appropriate Subscribers [10, 24]. An exception to the above is when a *Subscriber-generated Data* message is sent towards a specific Publisher supposed to later share the pertinent content. In such a case, the message is not checked against the

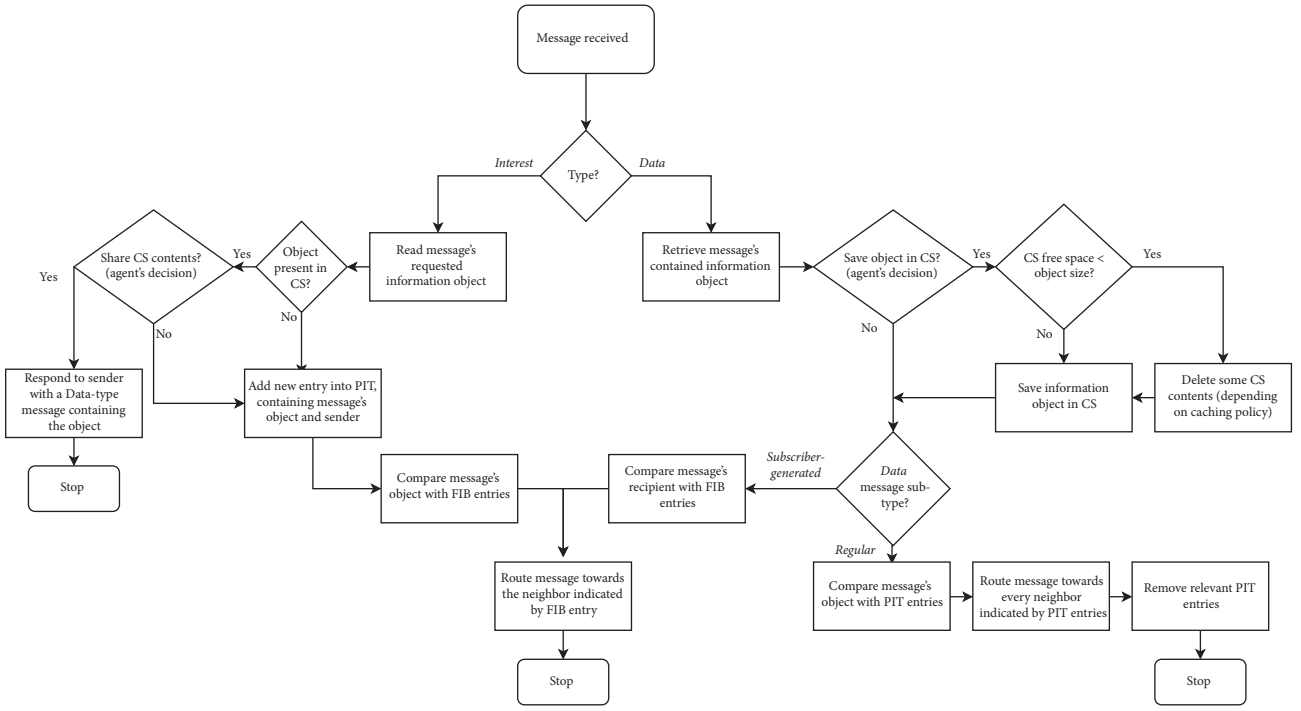

Figure 2: Message handling at a CR.

PIT entries but is simply routed in the appropriate direction. The pertinent information objects may be cached within CS

3.5. Topology. In our model, network entities are located on an infinite two-dimensional plane. The initial locations of the entities are confined to a predefined area, the locations of CRs and Publishers being decided randomly according to a uniform probability distribution. All connections are two-way and, for two entities to be considered neighbors (i.e., to have a connection between themselves), it is enough that at least one of them has established a connection to the other. A connection between CRs i and j can be established if the following condition holds:

$$\exists_{p \in P} dist\,(i,j) = \min\left\{dist\,(i,k) \mid k \in C \wedge dist\,(k,p) < dist\,(i,p)\right\}, \quad (1)$$

where P is the set of Publishers, C is the set of CRs, and $dist(a,b)$ is the Euclidean distance between entities a and b. Thus the connection can be established if there exists a Publisher p such that j is the closest to i among all CRs that are closer to p than is i. As a result, CR i's FIB is updated so that CR i will route messages destined for Publisher p through CR j.

A connection between CR i and Publisher p can be established if the following condition holds:

$$\forall_{k \in C} dist\,(i,p) = \min\left\{dist\,(i,k) \mid k \in C\right\}. \quad (2)$$

Thus a connection between i and p is established if no CR is closer to i than is p. This results in updating CR i's FIB so that messages destined for Publisher p will be routed directly to p rather than through other CRs.

Each Subscriber is connected with the currently closest CR, referred to as its *community node*. A Subscriber's initial location coincides with its initial community node's; during subsequent Subscriber movement, its community node may change.

3.6. Subscriber Mobility. In this paper, Subscriber mobility is accounted for using the *Random Waypoint Mobility* (RWP) model with elements of the *Time-Variant Community* (TVC) model [25].

At any given time $\tau = 1, 2, \ldots$ (measured in equal-duration slots), a Subscriber can be in one of two feasible states, *moving* or *stationary*. The current location of a Subscriber in slot τ is represented by the plane coordinates $X(\tau)$ and $Y(\tau)$, and its movement can be described by the following parameters: velocity $v(\tau)$ (in the stationary state, $v(\tau) = 0$), angle $\alpha(\tau)$, and remaining state duration $\mu(\tau)$. Assuming $\mu(\tau) > 0$, the location of a Subscriber at the start of the next slot can be calculated as follows:

$$X(\tau+1) = X(\tau) + v(\tau) \cdot \cos(\alpha(\tau)),$$
$$Y(\tau+1) = Y(\tau) + v(\tau) \cdot \sin(\alpha(\tau)), \quad (3)$$

with $\mu(\tau)$ decremented in each slot; when it reaches 0, the Subscriber's state changes from moving to stationary and vice versa, and a new $\mu(\tau+1)$ is randomly generated within a given value range. If the state change is from stationary to moving, new $v(\tau+1)$ and $\alpha(\tau+1)$ are also randomly generated. As mentioned before, each Subscriber has an established connection to its community node, the CR closest to it,

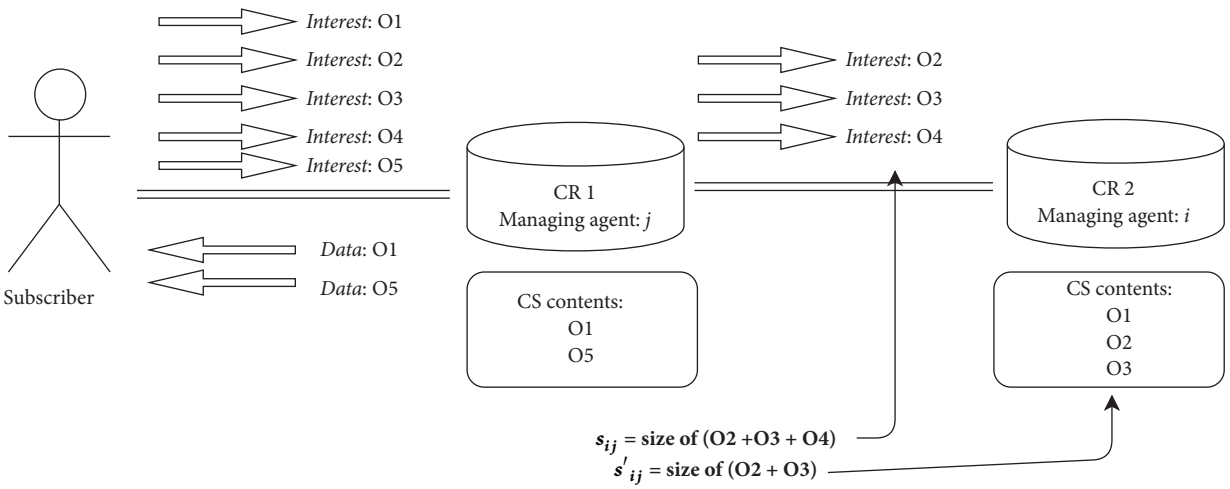

Figure 3: Example interaction between agents i and j: j receives *Interest* messages from a Subscriber requesting information objects O1,. . .,O5, but due to limited cache contents are able to respond with only two *Data* messages. To fulfill the Subscriber's request, j interacts with i and requests sharing objects O2, O3, and O4, of which O2 and O3 are available in i's CS.

which can be severed and give way to a new connection if Subscriber's movement causes another CR to become the closest [26].

The TVC model assumes human-like behavior on the part of the Subscribers and so their tendency to operate and periodically reappear in specific Subscriber dependent areas termed *communities*. The moving state is refined by differentiating *movement periods*: during a *Normal Movement Period* (NMP), the Subscriber moves as in the RWP model, and during a *Concentration Movement Period* (CMP), the Subscriber's mobility is restricted to its community [27]. In our work, CMP is modeled in a simplified way: whenever a Subscriber's state changes from stationary to moving, the state will be CMP with a predefined probability p_{CMP} and will be NMP otherwise. Upon entering CMP, the Subscriber returns to its initial community node location and continues to move in accordance with the RWP model until the state changes back to stationary.

3.7. Agents. The autonomous agents in our model, one per CR, are responsible for controlling CRs; they make autonomous decisions regarding the local CS and its content. The agent decides whether content moving through the CR should be saved in CS and which content, if any, should be removed when CS has no more free space. Moreover, when receiving an *Interest* message pertaining to an information object present in CS, the agent makes a decision whether to respond with a *Data* message containing the information object or route an appropriate *Interest* message instead. Hence, in addition to providing community node services to the directly connected Subscribers, agents may share the CS contents with one another.

3.8. Interactions. Interagent interactions in our model are pairwise (Figure 3). An interaction occurs when an agent is unable to fulfill, using its CS, all the requests in *Interest* messages belonging to a single flow from a directly connected Subscriber. This forces the agent to route one or more of the flow's *Interest* messages to one of its neighbor CRs with which a connection needs to be established. That neighbor then has an option to provide the service, that is, share the contents of its CS (rather than routing the messages further on), in which case it will be called the *service provider*, whereas the original agent will be called the *service recipient*. Let us assume a division of the time axis into *cycles* (not necessarily coinciding with the Subscriber mobility-related slots). An interaction between a service provider i and a service recipient j in cycle t can be characterized by the total size $s_{ij}(t)$ (e.g., in bytes) of content requested from i by j and the total size $s'_{ij}(t)$ of content requested that is currently available in i's CS. We define the amount of *available service* as $A_{ij}(t) = s'_{ij}(t)/s_{ij}(t)$, where $A_{ij}(t) \in [0, 1]$. In response, the service provider i may decide to send to the service recipient j the content of a total size $s''_{ij}(t)$, which is all, some, or none of its available content. We accordingly define the amount of *provided service* as $P_{ij}(t) = s''_{ij}(t)/s_{ij}(t)$, where $P_{ij}(t) \in [0, 1]$ and $P_{ij}(t) \leq A_{ij}(t)$. Note that, owing to there being multiple Publishers in the network, (1) implies that interactions can in principle occur between any pair of agents (i.e., connections can be established between any pair of CRs).

3.9. Reputation and Trust Building Scheme. Providing service to connected Subscribers in the form of content access can be reasonably assumed to generate benefit (e.g., payment or any other compensation) for the agent, thus giving it an incentive to do so. On the other hand, providing service to other agents in the form of CS content sharing in itself generates no such benefit, so a selfish agent striving to maximize its own benefit could well ignore any requests from other agents and refuse to provide service to them. To remedy that, a centralized reputation and trust building scheme is employed, whose aim is to calculate a *trust value* for each agent, describing that agent's willingness to provide

services to other agents. Following [7], one of the network entities is designated as the *Reputation Aggregation Engine* (RAE). After each interagent interaction, the service recipient generates *reputation data* reporting its satisfaction with the received service. The reported reputation data are collected by RAE and aggregated into the agents' trust values, to be next disseminated among the agents and influence their service provision decisions. In the spirit of indirect reciprocity, it is anticipated that these decisions should be more favorable towards recipients with high trust values but can also depend on the providers' trust values [1]. However, each agent is free to adopt its own policy. Regarding this, agents can be classified into a multitude of categories; for simplicity, only two categories will be considered:

(i) *honest* (h-)agents are willing to provide more service to and report more favorable reputation data regarding agents with high trust values and hence are striving to build high trust values of their own

(ii) *strategic* (s-)agents exhibit selfish or malicious behavior, aiming, respectively, to receive much service from other agents while providing little and possibly reporting unfair reputation data or to *subvert* the reputation and trust building scheme, that is, acquire higher trust values than honest agents

We assume that the agents operate under *virtual anonymity*, meaning that their permanent identities are only known to RAE and are never disclosed. On the other hand, RAE is unable to recognize the categories of the agents, even though it knows their trust values, since it is unable to decide whether the collected reputation data are fair or whether the reputation and trust building scheme has been subverted. Furthermore, we conservatively assume that s-agents can recognize each other as such and collude in pursuit of their goals by differentiating their service provision and reporting behavior depending on the recognized category of the interacting agent.

In cycle t, an interaction between a service provider i and a service recipient j results in provided service $P_{ij}(t)$ granted by the former according to its service provision policy and reputation data $R_{ij}(t) \in [0,1]$ reported by the latter according to its reporting policy. Clearly, $R_{ij}(t) \leq P_{ij}(t) \leq A_{ij}(t)$. A service provision policy can be expressed as a nondecreasing function $f_{ij}(\cdot)$ of $A_{ij}(t)$, and a reporting policy can be expressed as a nondecreasing function $g_{ij}(\cdot)$ of $P_{ij}(t)$; both functions may depend on either agents' category and trust value. We take

$$P_{ij}(t) = \min\left\{A_{ij}(t), p_{ij}\right\}, \tag{4}$$

$$R_{ij}(t) = \min\left\{P_{ij}(t), r_{ij}\right\}, \tag{5}$$

where $p_{ij} \in [0,1]$ and $r_{ij} \in [0,1]$ are category and trust value dependent thresholds that, respectively, quantify agent i's honesty when providing service and agent j's honesty when reporting reputation data. Let H and S be the time-invariant sets of h- and s-agents in the network, respectively, and let $V_i(t)$ be agent i's trust value in cycle t. Then we take

$$p_{ij} = \begin{cases} 1, & \text{if } i \in S \text{ and } j \in S, \\ y, & \text{if } i \in S \text{ and } j \in H, , \\ \mathbf{1}\left(V_j(t) \geq 1 - x\right), & \text{if } i \in H, \end{cases} \tag{6}$$

$$r_{ij} = \begin{cases} 1, & \text{if } i \in S \text{ and } j \in S, \\ z, & \text{if } i \in H \text{ and } j \in S, \\ \mathbf{1}\left(V_i(t) \geq 1 - x\right), & \text{if } j \in H, \end{cases} \tag{7}$$

where $\mathbf{1}(\cdot)$ is the indicator function of the stated logical condition and $x, y, z \in [0,1]$ are parameters governing agents' service provision and reporting policies. In particular, an honest service provider grants $P_{ij}(t) = A_{ij}(t)$ if the service recipient's trust value is high enough and 0 otherwise, whereas a strategic service provider grants $P_{ij}(t) = A_{ij}(t)$ to a fellow strategic service recipient and at most y to an honest one, where y is chosen with a view of attaining high $V_i(t)$ for large enough t. Likewise, an honest service recipient reports $R_{ij}(t) = P_{ij}(t)$ if the service provider's trust value is high enough and 0 otherwise, whereas a strategic service recipient reports $R_{ij}(t) = P_{ij}(t)$ about a fellow strategic service provider and at most z about an honest one, where z is chosen with a view of attaining high $V_j(t)$ for large enough t.

Initially, each agent receives the maximum trust value, that is, $V_i(0) = 1$. To establish the agents' trust values in cycle t, RAE calculates a weighted sum of reputation data about each agent i collected from all its service recipients, with emphasis upon recent data from high-trust ones:

$$R_{i,\Sigma}(t) = \frac{\sum_{j \in N \setminus \{t\}} V_j(t) \cdot R_{ij}\left(t - \Delta_{ij}(t)\right)}{\sum_{j \in N \setminus \{t\}} V_j(t)}, \tag{8}$$

where $N = H \cup S$ is the set of all agents and $\Delta_{ij}(t)$ is the number of cycles that have elapsed since i last provided service to j (if agent i has not provided service to agent j up to cycle t, we take $\Delta_{ij}(t) = \infty$ and $R_{ij}(u) = 1$ for $u \leq 0$). To keep the model simple, we assume just two levels of trust values per cycle, obtained as follows. RAE partitions the set N into disjoint subsets $N_{\text{low}}(t)$ and $N_{\text{high}}(t)$ using any clustering algorithm so that, for any $i \in N_{\text{high}}(t)$ and $j \in N_{\text{low}}(t)$, $R_{i,\Sigma}(t) \geq R_{j,\Sigma}(t)$. Let $N_i(t)$ be the subset containing agent i. Agent i finally acquires a trust value equal to the arithmetic average $\sum_{j \in N_i(t)} R_{j,\Sigma}(t)/|N_i(t)|$, normalized to the analogous arithmetic average in the set $N_{\text{high}}(t)$. Thus

$$V_i(t+1) \begin{cases} = 1, & \text{if } i \in N_{\text{high}}(t), \\ \leq 1, & \text{if } i \in N_{\text{low}}(t). \end{cases} \tag{9}$$

From the computational complexity viewpoint, the scheme's operation can be viewed as a three-step process:

(i) Firstly, for each agent i, RAE calculates $R_{i,\Sigma}(t)$, a weighted sum of last reported reputation data about i obtained from every other agent. This step has a computational complexity of $O(n^2)$, where $n = |N|$

(ii) Secondly, RAE performs clustering of agents depending on their $R_{i,\Sigma}(t)$ values in order to obtain two clusters. The complexity depends on the clustering algorithm used. We adopt the k-means, an iterative algorithm that is computationally difficult in a general case; however, its complexity can be assessed for instances where dimensions of the value vector and the number of target clusters are both known and constant. In our case, the vector of $R_{i,\Sigma}(t)$ values is only one-dimensional and we seek to partition n agents into two clusters. This gives us a complexity of $O(n)$ for a single iteration, with no more than n iterations. The final complexity of the clustering algorithm is therefore $O(n^2)$

(iii) Finally, each agent i receives a new trust value $V_i(t)$ dependent on the cluster the agent belongs to and on the sum of $R_{i,\Sigma}(t)$ for agents in each cluster. This is a fast process with computational complexity of $O(n)$.

Overall, the computational complexity of our scheme is $O(n^2)$. With a realistic number of agents on the order of $n = 1000$, the computation time is insignificant compared to message delays between agents, measured at up to 10 milliseconds on medium-range processing equipment.

3.10. Caching Policy. Agents are responsible for the CS contents at nodes they control. By default, any information object that moves through a node is saved in CS unless its size exceeds the currently free space. Should that happen, the agent in control proceeds with cleaning up CS: all cached information objects are examined in the nondecreasing order of "hits" (the numbers of times an object has been requested by other agents or Subscribers). An object is removed from CS if the agent j that last requested it has $V_j(t) < 1–x$ in the case where the CS is controlled by an h-agent or is an h-agent in the case where the CS is controlled by an s-agent. This continues until enough space is freed in CS or all content has been evaluated.

3.11. One-Time Goodwill Mechanism. Using our reputation and trust building scheme with highly mobile Subscribers may be difficult, as frequent connection changes imply that the content contributed or requested by a Subscriber in the past is unlikely to be cached near the Subscriber's current location. Thus, in successive interactions, available service $A_{ij}(t)$ is likely to be low despite of the service providers' honesty. In order to reduce penalization of h-agents in such circumstances, an additional mechanism called *one-time goodwill* is introduced at h-agents. It prescribes that each h-agent should maintain a list of information objects it requested during past interactions with a given agent j. When agent i requests from agent j content that does not appear on the list, it generously assumes that j may not have had a chance to save this content in its CS but is willing to do so now; therefore, regardless of the provided service $P_{ij}(t)$, agent i reports $R_{ij}(t) = 1$. Agent j is then assumed to have saved this content in its CS, a suitable entry is added to agent i's list, and future interactions between i and j related to this content proceed as usual.

3.12. Security. The design of a comprehensive security communication system for information-centric networks is a complex issue and deserves a separate study. Here we assume that such a system is already in place and has no influence on the operation of the considered reputation and trust building scheme, as is often the case for publications pertaining to such schemes. Therefore we only briefly comment on selected security issues relevant to our study.

In Named Data Networking (NDN) [10], an implementation that underlies our considered ICN architecture, data (stored contents) security is based on public key cryptography. Each network entity possesses a private and public key pair which are used for content encryption and generates digital signatures for the purpose of content verification. The key pair is bound to an entity's identity through a certificate issued by a Certificate Authority. An entity may possess more than one identity, each with its own keys and a signature. All content available in the network must be signed and encrypted by its producer, in our case the Subscriber originally responsible for uploading the content to the network. NDN forces all *Data* messages to include a signature of the producer, ensuring content integrity. *Interest* messages do not carry content whose integrity may be compromised or information pertaining to the identity of the interested Subscriber. Therefore securing them with a signature is not necessary and in fact may reduce confidentiality as it might allow third parties to learn that a given Subscriber is interested in certain content. However, measures to thwart flooding and DoS attacks should be used. The NDN architecture allows for such techniques to be applied locally at node level or collaboratively between nodes, with potential attacks detected through checking Pending Interest Table contents for spurious requests or through the use of timestamps to track expired *Interest* messages. Countermeasures against potential attacks include limiting rates of accepted *Interest* messages and/or dropping traffic incoming from a specific interface or pertaining to given content, as described, for example, in [28].

In addition to *Data* and *Interest* messages as well as stored content, security of trust data exchanged between the nodes and RAE has to be ensured. As RAE is a trusted entity, it is possible to set up a security association between RAE and any given node to communicate using signed messages. Alternatively, as the node-to-RAE connections are not part of the information-centric network and do not have to follow NDN conventions regarding message specifications, we may assume that they are carried out over a secure channel. This is possible due to the assumed virtual anonymity: although agents are anonymous to one another, their true identities are known to RAE (and never disclosed). As for the key exchange and management, one can suggest using either standard techniques such as the Internet Key Exchange (IKEv2) protocol or techniques specifically developed for information-centric networking. Regarding the latter, a thing to note is that just as information-centric network technology

is still in development, then so are the corresponding security techniques and no standardized solutions have been agreed upon yet. An example is the NAC protocol, described in [29].

4. Results and Discussion

The proposed reputation and trust building scheme should stimulate cooperative behavior of the agents on the premise that more service should be provided to high-trust agents. In particular, proper distinction between h- and s-agents should be enabled. In the ideal case, in each cycle *t,* we expect $H = N_{\text{high}}(t)$ and $S = N_{\text{low}}(t)$, whereas in the worst case, $S = N_{\text{high}}(t)$ and $H = N_{\text{low}}(t)$. The latter case means the scheme has been subverted by the s-agents and is in fact counterproductive: despite behaving selfishly or maliciously, the s-agents have earned the higher trust values and so can pose as h-agents, leading to wrong service provision decisions of genuine h-agents. In reality, neither of the above cases is likely to occur, mainly because of the time variability of the available service $A_{ij}(t)$ (note that it is determined by the CS contents at the CRs and therefore heavily depends on prior movement of *Data* messages through each CR; these messages are generated by Subscribers or in response to *Interest* messages from nearby Subscribers, whose locations may change rapidly). Hence, we can expect a fraction of h-agents to acquire the high trust values of 1 and a fraction of s-agents to acquire the lower trust values, hopefully both fractions being large enough. In this context, we address the following question: *How sharp is the distinction between h- and s-agents (in particular, how resilient is the reputation and trust building scheme to subversion) relative to the parameters of Subscriber mobility*? This question cannot be answered analytically due to the operational complexity of the described ICN architecture and reputation and trust building scheme, even though the model is somewhat simplified; therefore we resort to simulations.

4.1. Simulator. We have developed a special-purpose simulator written in C#, capable of generating various Subscriber mobility scenarios and utilizing them in conjunction with various configurations of the modeled ICN. The simulator is driven by an appropriately formatted real-world dataset containing sequences of messages generated by each Subscriber.

The functionality offered by the simulator is twofold: in addition to performing simulations of the adopted information-centric network model, it generates mobility scenarios according to Section 3.6. We believe that since the adopted mobility models are widely regarded as realistic, then so can be our simulator, since it reflects these models directly. When generating a mobility scenario, the simulator determines positions of nodes and Publishers and connections between them as described in Section 3.5. A position of each Subscriber is calculated in every time slot of duration τ, depending on the mobility model and its configuration. This allows the simulator to establish Subscriber-to-node connections and to keep track of these connections' changes. Message flows within each connection are extracted from a dataset file and drive the simulator. We have decided to use a real-life dataset available at https://www.simpleweb.org/wiki/index.php/Dropbox_Traces instead of artificially generating one according to standard statistical properties such as Zipf's law. Numerical values contained in the dataset (such as message timing, identities of Subscribers and Publishers, or content size) are therefore a credible representation of information-centric network activity.

The simulator reads the dataset file message by message—either *Interest* or Subscriber-generated *Data*. These messages are forwarded towards their destination according to nodes' Forwarding Information Bases, moving through one or more nodes. Node caches and other data structures are modeled as lists of currently stored contents or messages along with their size and are handled as specified in Section 3. The is also true of the operation of RAE, RAE-to-agents communication, and the one-time goodwill mechanism.

Low-layer communication mechanisms of the simulated network, that is, Subscribed-to-node and node-to-node transmission details, are outside the scope of our work. We believe that faithful implementation of such mechanisms, featuring transmission impairments, switching, routing, MAC-layer queuing, Subscriber collisions in wireless access channels, and so forth, would not qualitatively influence the workings and effects of our reputation and trust building scheme. In fact, papers on trust and reputation building as well as on information-centric architectures typically disregard the physical communication aspects, cf., for example, [10, 21]. Therefore, our simulator simply models message transfer as negligibly small propagation and processing delays (under 1 ms), plus message transmission times relative to their sizes. In the Dropbox Traces dataset used in our study, the average interaction between agents involves exchange of less than 3 MB of content, though requests for content up to 420 MB in size are occasionally observed. For example, if the nodes are interconnected via an optical fiber Gigabit Ethernet, then a store-and-forward end-to-end *Data* message transfer may on average take around 0.1 s, whereas shorter *Interest* and RAE-to-node messages take much less. A study of existing information-centric environments shows that such delays are insignificant compared to the time differences between agent interactions in relevant datasets. For Dropbox Traces, even in the most pessimistic scenario (where every generated *Interest* message causes an agent-to-agent interaction), the average time between agent interactions exceeds 30 s.

Security aspects including content naming and accessing or message protection are likewise omitted.

4.2. Dataset and Simulation Scenarios. The model was evaluated using the Dropbox Traces dataset containing real-life data related to Dropbox, an online file-hosting service offering cloud storage for its users' content [30]. The content may also be shared with other selected users or made publicly available. The dataset was compiled between March 24th and May 5th 2012 and is presented in the tabular form, with each entry pertaining to a single flow between a user and a Dropbox server. A total of 1011 unique users and 650 unique servers have been identified within the dataset [31], the total size of all available content being roughly 460 GB.

Table 1: Parameter values for mobility scenarios.

Scenario	$\mu(\tau)$ when in stationary state	$\mu(\tau)$ when in moving state
0	0	0
1	0..392	0..2
2	0..392	0..6
3	0..196	0..6
4	0..96	0..6
5	0..48	0..10
6	0..24	0..10
7	0..12	0..10
8	0..2	0..20

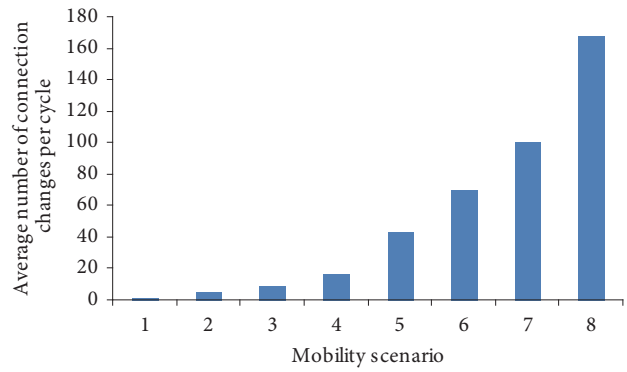

Figure 4: Average number of connection changes per cycle for mobility scenarios 1 to 8.

Rather than associating a user with only one server, each user's contents are distributed across multiple servers [30]. In our model, Dropbox users correspond to Subscribers, while Dropbox servers correspond to Publishers. CRs are introduced for caching data locally and therefore facilitating interactions between users and servers. The dataset was filtered to retain only user-server message flows related to data storage requests: user-to-server, represented by Subscriber-generated *Data* messages in our model, and server-to-user, represented by *Interest* messages generated by the Subscribers and followed by regular *Data* messages generated by either Publishers or CRs.

Nine mobility scenarios are compared, numbered 0 through 8, each utilizing the Dropbox Traces dataset and the same initial network topology, but with different parameters of Subscriber mobility. Scenario 0 assumes no Subscriber mobility, while scenarios 1 through 8 feature increasing Subscriber mobility, quantified as the average number of Subscriber-to-CR connection changes per slot τ. Common parameters across the scenarios include slot duration τ = 60 s, range of $v(\tau)$ = 0..30 m/s, range of α = 0..2 π, the initial Subscriber location within a 150x150 km square, and p_{CMP} = 0.5. The other parameter values used in each scenario are shown in Table 1. In order to ensure that the obtained results are mainly dependent on mobility rather than the caching policy or any shortcomings thereof, the CSs at the CRs are somewhat lavishly dimensioned at 128 GB each. Figure 4 shows the average number of connection changes per τ for each mobility scenario.

4.3. Results. The compared mobility scenarios assume the following common parameters that control the service provision and reporting policies of the agents: x = 0.8, y = 0.1, and z = 0.0. A total of 1000 agents were assumed, with 800 h-agents and 200 colluding s-agents ($|N|$ = 1000, $|H|$ = 800, and $|S|$ = 200). The clustering algorithm used for differentiating between agents' trust values was one-dimensional k-means over $R_{i,\Sigma}(t)$ [32, 33]. The values of available service $A_{ij}(t)$, relevant to the trust building, are related to the variable contents of each CR's CS and thus can be only statistically characterized depending on the Subscriber mobility scenario: random movement of Subscribers mobility influences message routes in the network and thus the opportunity of saving specific content in each CS. We have distilled from the Dropbox Traces dataset the experimental probability distributions of $A_{ij}(t)$ based on frequencies of occurring of specific values $A_{ij}(t)$. These are depicted in Figure 5 for the considered mobility scenarios. Figure 6 presents the corresponding average values of $A_{ij}(t)$ per interaction.

One sees a tendency for available service to decrease as Subscriber mobility increases. In a mobility-less scenario 0, the probability of $A_{ij}(t) = 1$ is quite high. This is because all content is first moved through CRs that may at a later time receive *Interest* messages regarding the corresponding information objects. The content remains available in the CRs' CS, unless it is removed according to the agents' caching policy. Under increased Subscriber mobility, the probability distribution of $A_{ij}(t)$ is increasingly tilted towards smaller values. This is because a Subscriber is more likely to send specific content into the network and then change its location before requesting that content. The route towards a Publisher sharing the corresponding information objects may change, with different CRs on the way which have not received these information objects yet. Moreover, information objects saved in CS are more frequently removed in a high-mobility scenario. It is also harder for an agent to assess whether a given information object is likely to be requested in near future and so should be saved in CS.

With a view of our main question, we have evaluated the proposed reputation and trust building scheme for the considered mobility scenarios by observing the fractions of h-agents and s-agents that obtained high trust values $V_i(t)$ = 1, as well as the average trust values of h-agents and s-agents. Each scenario was simulated in the absence and in the presence of the one-time goodwill mechanism employed at the h-agents. The respective results are shown in Figures 7 and 8.

Note that Figure 7(a) shows the proportions of each type of agents (h- and s-) that, by the end of the simulation, managed to obtain high trust values (i.e., $V_{high}(t) = 1$). Let us call these proportions $\xi_{h,high}(t)$ for h-agents and $\xi_{s,high}(t)$ for s-agents. The remaining agents obtained a certain low trust value ($V_{low}(t) \leq 1$). The fractions of agents with low trust

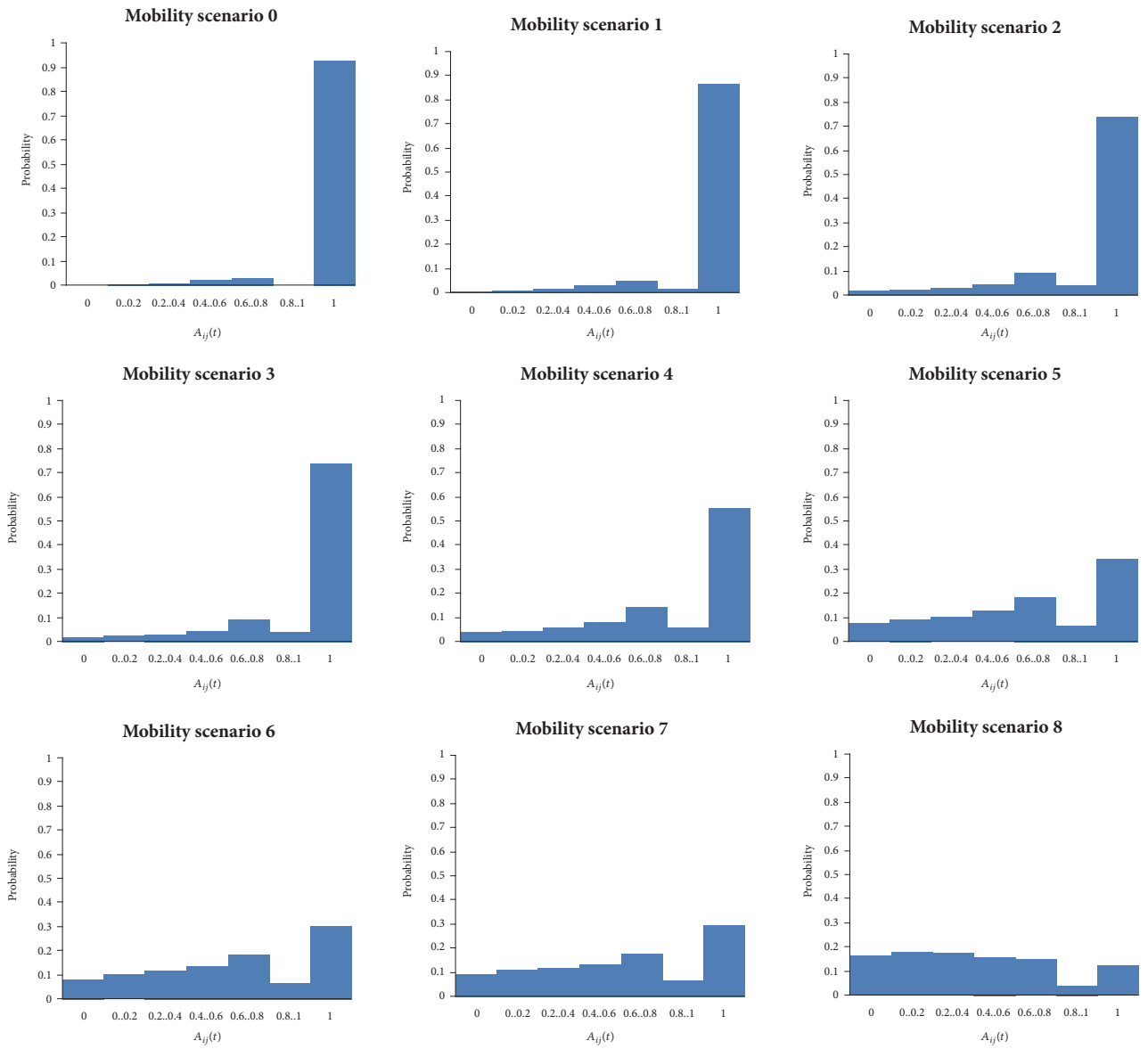

FIGURE 5: Probability distributions of $A_{ij}(t)$ for mobility scenarios 0 through 8.

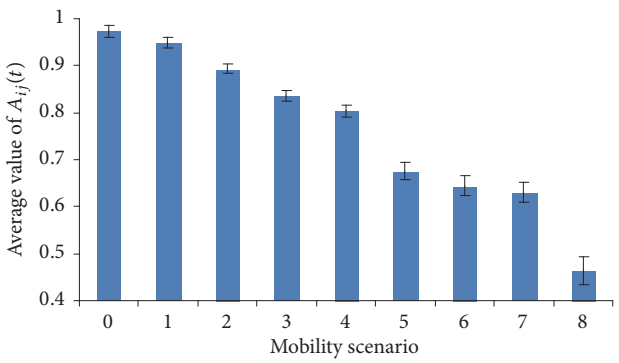

FIGURE 6: Average values of $A_{ij}(t)$ for mobility scenarios 0 through 8 (indicated are 95% confidence intervals based on 20 independent simulation runs).

values are $1 - \xi_{h,high}(t)$ for h-agents, and $1 - \xi_{s,high}(t)$ for s-agents. Figure 7(b) shows average trust values obtained by agents of each type; let us call them $V_{h,avg}(t)$ for h-agents and $V_{s,avg}(t)$ for s-agents. Based on (8) and (9) and assuming that statistical characteristics of agents within each type are identical, these trust values can be approximately calculated as follows:

$$V_{h,avg}(t) = \xi_{h,high}(t) + \left(1 - \xi_{h,high}(t)\right) \cdot V_{low}(t)$$
$$V_{s,avg}(t) = \xi_{s,high}(t) + \left(1 - \xi_{s,high}(t)\right) \cdot V_{low}(t) \quad (10)$$

A very low value of $V_{low}(t)$ explains the similarity of values between $\xi_{h,high}(t)$ and $V_{h,avg}(t)$, as well as between $\xi_{s,high}(t)$ and $V_{s,avg}(t)$ in Figure 7. With $V_{low}(t)$ typically below 0.03, the differences between Figures 7(a) and 7(b) are minimal. In contrast, panels in Figures 8(a) and 8(b) show visibly different

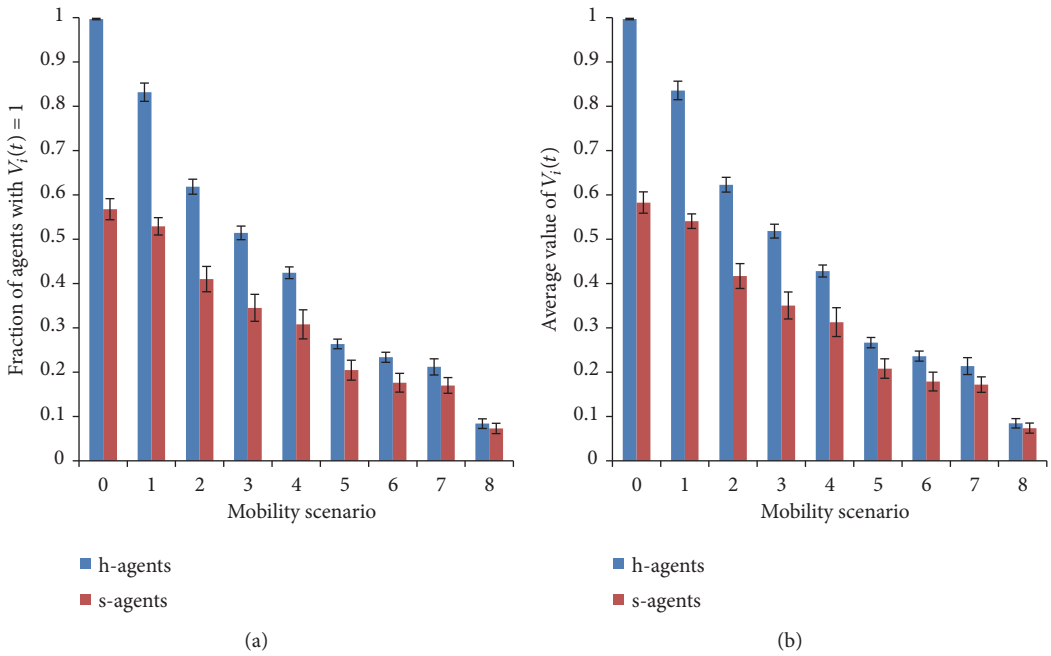

FIGURE 7: Reputation and trust building scheme in the absence of one-time goodwill mechanism; (a) fraction of agents with high ($V_i(t) = 1$) trust values; (b) average agent trust values (indicated are 95% confidence intervals based on 20 independent simulation runs).

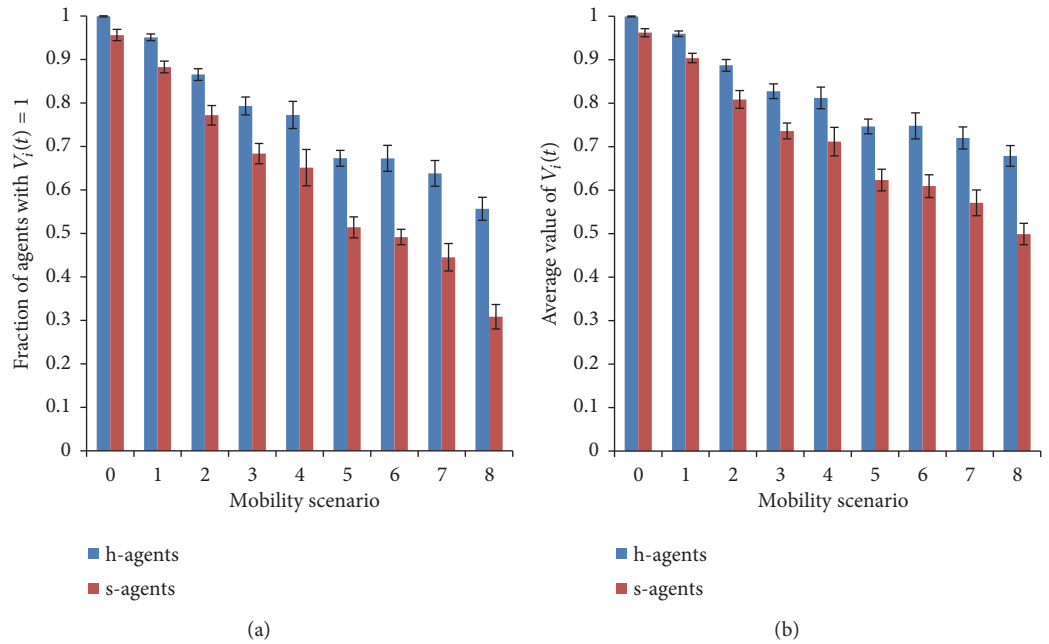

FIGURE 8: Reputation and trust building scheme in the presence of one-time goodwill mechanism; (a) fraction of agents with high ($V_i(t) = 1$) trust values; (b) average agent trust values (indicated are 95% confidence intervals based on 20 independent simulation runs).

values, which result from relatively large $V_{low}(t)$ values under the one-time goodwill mechanism, typically upwards of 0.15.

The results show agents' trust values to decrease as Subscriber mobility increases. Since available service $A_{ij}(t)$ tends to drop under increased Subscriber mobility, even cooperative agents are less able to provide requested service provoking harsh reports from service recipients. The outcome is a low number of agents with high trust values. While the effect of Subscriber mobility on agent trust values is visible for both h- and s-agents, it is more pronounced for the former and, as Subscriber mobility increases, the fractions of agents with high trust values are drawn closer to each other. For Subscriber mobility scenario 8, cases were observed where a subversion occurred; that is, s-agents received higher trust

values than h-agents. With typically small $A_{ij}(t)$, both h- and s-agents provide little service to h-agents, who are in the majority; consequently, their reports, which dominate the weighted sum in (8), are less distinctive and it becomes more difficult to differentiate both agent categories. The s-agents are less sensitive to the diminished service availability as they can always count on favorable reporting by colluding fellow s-agents.

The proposed one-time goodwill mechanism assures that an agent is not punished for failing to provide content it has not been requested for before. As discussed above, such situations are common in increased-mobility scenarios. The mechanism then allows for a considerable fraction of agents to retain high trust values. Unfortunately, the same mechanism allows for unfairly high assessment of s-agents, which as service providers will only receive unfavorable reports after failing for a second time to share specific content with a given h-agent. This results in higher trust values for s-agents, especially in low- or no-mobility scenarios where interactions between agents are relatively infrequent. In higher-mobility scenarios, which see more interactions (due to a reduced possibility of requested content being available in a service provider's CS), an s-agent's behavior will sooner exhaust the one-time goodwill. Therefore, the difference between the average h- and s-agent trust values becomes more pronounced. Hence, the one-time goodwill proves useful in high-mobility scenarios.

4.4. Discussion. To validate the presented results, we first compare our reputation and trust building scheme with an existing one, functionally similar though intended for the Social Internet of Things (SIoT), and next introduce an alternative mobility model to compare its impact with that of the adopted RWP model with elements of TVC.

4.4.1. Comparison with Alternative Reputation and Trust Building Scheme. In [21], Nitti, Girau, and Atzori proposed a trustworthiness management scheme for the SIoT, hereafter referred to as NGA, featuring both subjective and objective trust formation models. We focus on the latter to enable a fair comparison. In this model, information about each node is collected and managed by special entities known as Pre-Trusted Objects (PTOs), which distribute among the nodes values of trustworthiness, T_j of each node p_j. A PTO can be roughly viewed as an analogue of our Reputation Aggregation Engine (RAE). NGA moreover assumes that malicious nodes may act benevolently when interacting with their close friends while showing malicious behavior otherwise, which corresponds to our notion of collusion among s-agents. Similarly, as in our scheme, the T_j values are aggregated based on reported feedback after a node interaction (roughly analogous to our $R_{ij}(t)$ values), however making extensive use of a number of defined attributes: interaction recency, transaction weights, type of internode relationship, nodes' computing power, and centrality, as well as the history of interactions between a given node pair.

We examine the transaction success rate as defined by NGA, which is close in spirit to the average amount $\mathsf{E}P_{ij}(t)$

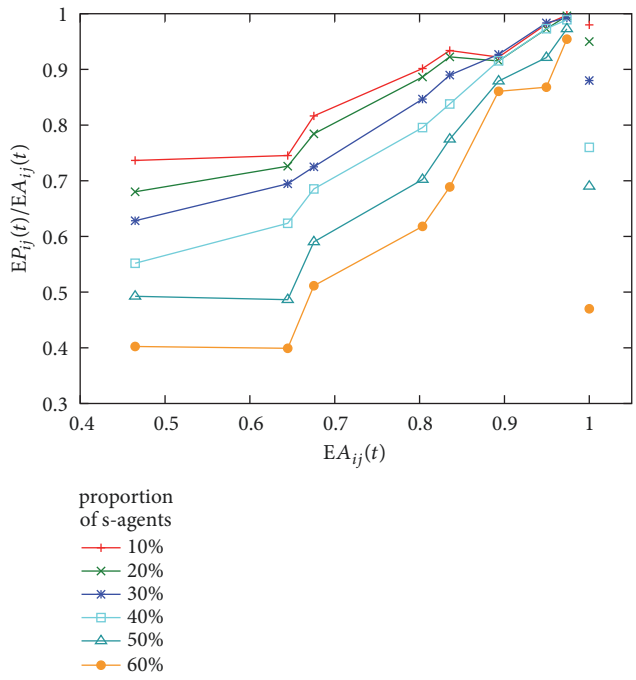

FIGURE 9: Honesty of service provider, expressed as $\mathsf{E}P_{ij}(t)/\mathsf{E}A_{ij}(t)$, against $\mathsf{E}A_{ij}(t)$, for various percentages of s-agents; $A_{ij}(t) < 1$: our scheme, $A_{ij}(t) = 1$: NGA.

of service provided in our scheme; increasing values of percentage of malicious nodes (corresponding to our s-agents) parameterize the comparison. It should be noted that our study differs from that of [21] in two aspects:

(1) While NGA assumes that a service provider is always able to perform good service, that is, the amount of service available $A_{ij}(t) \equiv 1$, in our study the values of $A_{ij}(t)$ vary between 0 and 1, and, for reasons explained in our original submission, decrease with the degree of Subscriber mobility. We enable a fair comparison by (a) taking the ratio $\mathsf{E}P_{ij}(t)$ / $\mathsf{E}A_{ij}(t)$ which measures the honesty of the service provider that the presence of the reputation and trust building scheme solicits, expressed as the proportion of the available service it is ready to provide, and (b) using only $A_{ij}(t)$ close to 1 to demonstrate the advantage of our scheme relative to NGA, whereas $A_{ij}(t) < 1$ illustrate the influence of mobility, our prime research goal

(2) While NGA assumes that a service recipient is able to choose a provider with the highest T_j, in our model it has no such capability; the provider is chosen from the currently available ones, as determined by the FIB contents. Since occasional (presumably poor) service provision by low-trust agents is therefore unavoidable, our fair comparison includes all interactions in NGA but only interactions between a high-trust service provider and an h-agent service recipient in our scheme.

Figure 9 summarizes the comparison. The results for $A_{ij}(t) = 1$ are read from [21, Figure 6(b)] while for $A_{ij}(t) < 1$

Table 2: Parameters and results for the CitySec mobility model.

Scenario	Normal road velocity v_{max}	High-speed road velocity $2v_{max}$	Average connection changes per τ	$EA_{ij}(t)$
1	0.5 m/s	1 m/s	2.3	0.89
2	1 m/s	2 m/s	5.5	0.79
3	2 m/s	4 m/s	12.6	0.69
4	4 m/s	8 m/s	24.2	0.61
5	10 m/s	20 m/s	46.6	0.57

they pertain to our scheme. One sees the superiority of our scheme at $A_{ij}(t)$ close to 1, that is, for low Subscriber mobility, especially if the proportion of s-agents becomes significant. This suggests that the lack in our scheme of the many defined attributes that NGA uses to control the credibility of the collected reputation data, that is, node centrality, type of mutual relationship, nodes' computation power, transaction weights, and so forth, is more than compensated by the much simpler, cluster-based derivation of the trust values and the conditioning of the provided service on both the service provider's and service recipient's trust values that our scheme prescribes. As a consequence, our scheme is more effective in reducing the influence of low-trust agents upon trust value formation and the amount of service provided to h-agents. At the same time, it is able to solicit more honesty on the part of h-agents whenever they interact with high-trust agents. For $A_{ij}(t)$ values below 0.8, the honesty sharply diminishes, reflecting the adverse impact of Subscriber mobility: due to more frequent poor service provided by high-trust agents, the h-agent service recipients become more distrustful.

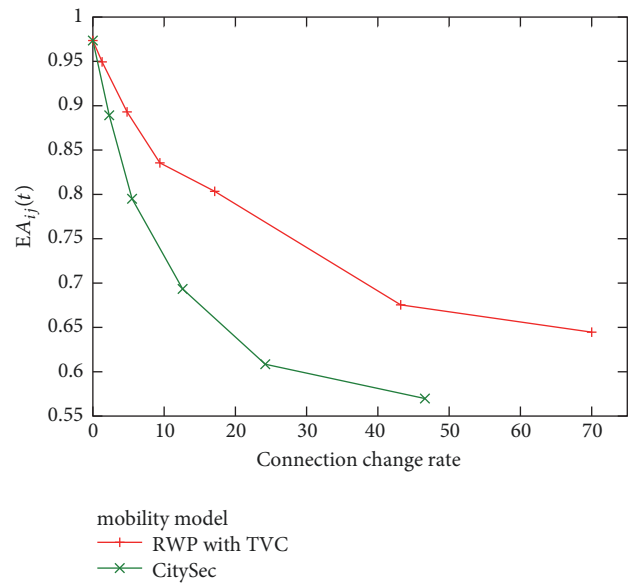

Figure 10: $EA_{ij}(t)$ against average connection change rate for RWP with TVC and CitySec mobility models.

4.4.2. Comparison with Alternative Mobility Model. Our intuition is that, for a given degree of mobility, the more predictable Subscriber movement (i.e., the more tendency to frequently appear in specific neighborhoods), the higher the average $EA_{ij}(t)$ of service available, yet the influence of the increasing degree of mobility upon $A_{ij}(t)$ is adverse regardless of the mobility model. We have attempted to verify this intuition by considering, besides the already described Random Waypoint Mobility model with elements of the Time Variant Community model (RWP with TVC), an alternative mobility model and a comparison of simulations results using both models.

The adopted alternative mobility model is known as City Section (CitySec) [34]. In this model, Subscriber mobility is constrained by the urban environment: the simulation area is a grid representing streets, each characterized by a speed limit. Thus Subscribers tend to prioritize movement over streets allowing for higher velocity as they seek to reach their destination. This means a degree of predictability is present in the model, as the probability of any given Subscriber being connected to a node near a high-speed street is higher than to a node distant from such a street. However, our original RWP with TVC model features more predictability, as a Subscriber returns to the location of its initial community node with probability $p_{CMP} = 0.5$ whenever its state changes from stationary to moving.

The following configuration of the CitySec model was assumed: a total of 250 streets (horizontal roads) and avenues (vertical roads) in a 60 x 60 km area and slot duration τ = 60 s, with starting and destination intersections decided randomly for each Subscriber. Upon reaching its destination intersection, the Subscriber remains stationary for 0..12 time slots and then a new destination is randomly generated. Streets and avenues numbered 50, 100, 150, and 200 are high-speed roads that Subscribers prioritize. On normal roads, Subscriber speed $v(\tau) = v_{max}$, which is the speed limit there, whereas on high-speed roads, $v(\tau) = 2v_{max}$. The simulations were performed using five mobility scenarios, differentiated by their v_{max} values. The parameters for each scenario and resulting average number of connection changes per slot, as well as average amounts of service available, are presented in Table 2.

Figure 10 presents a sample comparison of the two considered mobility models in terms of the average amount $EA_{ij}(t)$ of service available against various connection change rates. The comparison corroborates our intuition: the effect of increasing Subscriber mobility upon $EA_{ij}(t)$ is in general negative and much more pronounced with less predictable Subscriber movement under the CitySec model.

5. Conclusions

The reputation and trust building scheme proposed for the considered ICN environment has been shown to be resilient to subversion for a mobility-less scenario; however, its resiliency to strategic agents weakens as Subscriber mobility increases. There is a negative correlation between increased Subscriber mobility and the amount of available service; this weakens the resiliency of the scheme, as it becomes progressively unclear whether a given agent is providing little service due to low service availability or to being strategic.

To combat the negative influence of Subscriber mobility, a simple one-time goodwill mechanism has been introduced. Though its effect on the reputation and trust building scheme's resiliency turns out to be detrimental in low- or no-mobility scenarios, it nonetheless proves useful in high-mobility scenarios.

Overall, a negative impact of Subscriber mobility on the performance of our system was demonstrated and remedied in part by the one-time goodwill mechanism. However, more work is needed in order to develop a robust reputation and trust building schemes in ICN environments featuring autonomous entities and user mobility.

Data Availability

The simulator code and data used to support the findings of this study are available upon request from Jakub Grochowski at jakgroch@gmail.com. The Dropbox Traces dataset [30] is available at https://www.simpleweb.org/wiki/index.php/Dropbox_Traces.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is funded by the National Science Center, Poland, under Grant UMO-2016/21/B/ST6/03146.

References

[1] H. Ohtsuki and Y. Iwasa, "How should we define goodness?—reputation dynamics in indirect reciprocity," *Journal of Theoretical Biology*, vol. 231, no. 1, pp. 107–120, 2004.

[2] I. Pinyol and J. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: A review," *Artificial Intelligence Review*, vol. 40, no. 1, pp. 1–25, 2013.

[3] F. Hendrikx, K. Bubendorfer, and R. Chard, "Reputation systems: a survey and taxonomy," *Journal of Parallel & Distributed Computing*, vol. 75, pp. 184–197, 2015.

[4] M. A. Nowak and K. Sigmund, "Evolution of indirect reciprocity," *Nature*, vol. 437, no. 7063, pp. 1291–1298, 2005.

[5] R. L. Trivers, "The evolution of reciprocal altruism," *The Quarterly Review of Biology*, vol. 46, no. 1, pp. 35–57, 1971.

[6] Z. Wang, L. Wang, Z. Yin, C. Xia, and A. Sánchez, "Inferring Reputation Promotes the Evolution of Cooperation in Spatial Social Dilemma Games," *PLoS ONE*, vol. 7, no. 7, p. e40218, 2012.

[7] J. Konorski, "Trust dynamics analysis of CTR scheme subversion under virtual anonymity and trust-unaware partner selection," in *Proceedings of the 18th International Workshop on Trust in Agent Societies, TRUST 2016*, pp. 43–53, Singapore.

[8] T. Koponen, M. Chawla, B.-G. Chun et al., "A data-oriented (and beyond) network architecture," *Computer Communication Review*, vol. 37, no. 4, pp. 181–192, 2007.

[9] F. Oehlmann, "Content-Centric Networking," in *Proceedings of the FI and IITM Seminars*, pp. 43–49, 2013.

[10] L. Zhang, A. Afanasyev, and J. Burke, "Named data networking," *Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[11] N. Fotiou, P. Nikander, D. Trossen, and G. C. Polyzos, "Developing information networking further: From PSIRP to PURSUIT," in *Proceedings of the International Conference on Broadband Communications, Networks and Systems*, pp. 1–13, Springer, Berlin, Germany, 2010.

[12] http://www.sail-project.eu/.

[13] X. Jiang, J. Bi, and Y. Wang, "What benefits does NDN have in supporting mobility," in *Proceedings of the 2014 IEEE Symposium on Computers and Communication (ISCC)*, pp. 1–6, 2014.

[14] Z. Yan, S. Zeadally, S. Zhang, R. Guo, and Y.-J. Park, "Distributed mobility management in named data networking," *Wireless Communications and Mobile Computing*, vol. 16, no. 13, pp. 1773–1783, 2016.

[15] C. Anastasiades and T. Braun, *Information-centric communication in mobile and wireless networks [Ph.D thesis]*, Universitaet Bern, 2016.

[16] C. Anastasiades, T. Braun, and V. A. Siris, "Information-Centric Networking in Mobile and Opportunistic Networks," in *Wireless Networking for Moving Objects*, vol. 8611 of *Lecture Notes in Computer Science*, pp. 14–30, Springer International Publishing, 2014.

[17] X. Hu, C. Papadopoulos, J. Gong, and D. Massey, "Not so cooperative caching in named data networking," in *Proceedings of the 2013 IEEE Global Communications Conference, GLOBECOM 2013*, pp. 2263–2268, USA, December 2013.

[18] Y. Xu, Y. Li, S. Ci, T. Lin, and F. Chen, "Distributed Caching via Rewarding: An Incentive Caching Model for ICN," in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM 2017)*, pp. 1–6, Singapore, December 2017.

[19] F. Kocak, G. Kesidis, T.-M. Pham, and S. Fdida, "The effect of caching on a model of content and access provider revenues in information-centric networks," in *Proceedings of the Internetional Conference on Social Computing (SocialCom '13)*, pp. 45–50, 2013.

[20] X. Wei, M. Chen, C. Tang, H. Bai, G. Zhang, and Z. Wang, "IRep: Indirect reciprocity reputation based efficient content delivery in BT-like systems," *Telecommunication Systems*, vol. 54, no. 1, pp. 47–60, 2013.

[21] M. Nitti, R. Girau, and L. Atzori, "Trustworthiness management in the social internet of things," *IEEE Transactions on Knowledge and Data Engineering*, vol. 26, no. 5, pp. 1253–1266, 2014.

[22] G. Xylomenos, C. N. Ververidis, V. A. Siris et al., "A survey of information-centric networking research," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 2, pp. 1024–1049, 2014.

[23] G. Zhang, Y. Li, and T. Lin, "Caching in information centric networking: a survey," *Computer Networks*, vol. 57, no. 16, pp. 3128–3141, 2013.

[24] D. Saxena, V. Raychoudhury, N. Suri, C. Becker, and J. Cao, "Named data networking: a survey," *Computer Science Review*, vol. 19, pp. 15–55, 2016.

[25] A. K. Shukla, "Mobility models in wireless Ad-hoc network: a simulative study," *International Journal of Modern Trends in Engineering and Research*, vol. 4, no. 7, pp. 244–250, 2017.

[26] X. Lin, R. K. Ganti, P. J. Fleming, and J. G. Andrews, "Towards understanding the fundamentals of mobility in cellular networks," *IEEE Transactions on Wireless Communications*, vol. 12, no. 4, pp. 1686–1698, 2013.

[27] W.-J. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, "Modeling spatial and temporal dependencies of user mobility in wireless mobile networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 5, pp. 1564–1577, 2009.

[28] S. Signorello, S. Marchal, J. Francois, O. Festor, and R. State, "Advanced interest flooding attacks in named-data networking," in *Proceedings of the 2017 IEEE 16th International Symposium on Network Computing and Applications (NCA)*, pp. 1–10, Cambridge, MA, October 2017.

[29] Z. Zhang, Y. Yu, A. Afanasyev, J. Burke, and L. Zhang, "NAC: Name-based access control in named data networking," in *Proceedings of the 4th ACM Conference on Information-Centric Networking, ICN 2017*, pp. 186-187, Germany, September 2017.

[30] I. Drago, M. Mellia, M. M. Munafò, A. Sperotto, R. Sadre, and A. Pras, "Inside dropbox: understanding personal cloud storage services," in *Proceedings of the ACM Internet Measurement Conference (IMC '12)*, pp. 481–494, November 2012.

[31] https://www.simpleweb.org/wiki/index.php/Dropbox_Traces#Format.

[32] A. K. Jain, M. N. Murty, and P. J. Flynn, "Data clustering: a review," *ACM Computing Surveys*, vol. 31, no. 3, pp. 264–323, 1999.

[33] J. A. Hartigan and M. A. Wong, "Algorithm AS 136: a k-means clustering algorithm," *Journal of Applied Statistics*, vol. 28, no. 1, pp. 100–108, 1979.

[34] M. S. Hossain and M. Atiquzzaman, "Stochastic Properties and Application of City Section Mobility Model," in *Proceedings of the GLOBECOM 2009 - 2009 IEEE Global Telecommunications Conference*, pp. 1–6, Honolulu, Hawaii, November 2009.