A Statistical Learning Reputation System for Opportunistic Networks

Diogo Soares
Federal University of Amazonas
Institute of Computing
Email: diogo.soares@icomp.ufam.edu.br

Edjair Mota
Federal University of Amazonas
Institute of Computing
Email: edjair@icomp.ufam.edu.br

Camilo Souza
Federal University of Amazonas
Institute of Computing
Email: camilo.souza@icomp.ufam.edu.br

Pietro Manzoni
Polytechnic University of Valencia
Computer Engineering Department
Email: pmanzoni@disca.upv.es

Juan Carlo Cano
Polytechnic University of Valencia
Computer Engineering Department
Email: jucano@disca.upv.es

Carlos Calafate
Polytechnic University of Valencia
Computer Engineering Department
Email: calafate@disca.upv.es

***Abstract*—Contacts are essential to guarantee the performance of opportunistic networks, but due to resource constraints, some nodes may not cooperate. In reputation systems, the perception of an agent depends on past observations to classify its actual behavior. Few studies have investigated the effectiveness of robust learning models for classifying selfish nodes in opportunistic networks. In this paper, we propose a distributed reputation algorithm based on the game theory to achieve reliable dissemination of information in opportunistic networks. A contact is modeled as a game, and the nodes can cooperate or not. By means of statistical inference methods, we derive the reputation of a node based on learning from past observations. We applied the proposed algorithm to a set of traces to form a distributed forecasting base for future action when selfish nodes are involved in the communication. We evaluate the conditions in which the accuracy of data collection becomes reliable.**

I. Introduction

Mobile opportunistic networks are characterized by lack of persistent connectivity, long delays, and low frequent encounters between the nodes. Contacts between pair of users are the main alternative for the propagation of messages, each network node acting as an intermediary for carrying copies of messages in the end-to-end communication.

Due to the absence of a fixed infrastructure, the interconnection between nodes is subject to high data loss rate and long delays. The communication among the nodes occurs opportunistically when one node is within the transmission range of another one. The message is passed in bundles instead of packets, and the receiving node carries the message and forwards it opportunistically later. The communication occurs in a decentralized manner, based on individual decisions that contribute to the transfer the message across the network. Since there is no central arbitration with respect to the transfer, one can not assume that the cooperation of other users will always occur. Due to resource constraints, though, some nodes may avoid cooperating with the communication, acting selfishly during the forward of data.

From a social point of view, during a contact the user can either contribute to the common good and to cooperate with the transfer or can act selfishly and take advantage of the network users to transfer data. This behavior is defined in economic theory as the *free-rider* problem [1], i.e., the selfish node requests transfer of its data, but avoids passing on data from other nodes. The traffic only occurs through the collaborative users, decrementing the number of possible opportunistic routes, as well as the individual and overall system performance. Intuitively, a contact is associated with the cost in terms of resource utilization to forward incoming messages, and with the benefit associated with the obtaining the cooperation of other nodes. The benefits are not always greater than the costs, so there is no explicit incentive for cooperation.

Some studies have shown that the presence of the *free-rider* behavior on a portion of the network nodes degrades considerably the individual and overall system performance when compared to the scenario where everyone cooperates [2] [3], [4]. The degradation occurs as a consequence of the reduction of the possible routes, causing a constant traffic break, raising the maximum resource utilization of the cooperative nodes. As a result, the cost for cooperation during the communication increases. Based on this fact, the identification of selfish behavior and the selection of proper mechanisms to deal with are fundamental to the implementation of opportunistic mobile networks.

Some approaches to create mechanisms to encourage cooperation have been studied in the literature. In general, these approaches can be a stimulus or inhibition. Incentive schemes [5] [6] use credit methods to induce users to cooperate with the data transfer; therefore, the network services are only available for users who have good credit. However, in opportunistic networks the mobility generates different contact patterns among users, which makes the credit system biased, for example, to users with higher popularity. Thus, the credit may not always reflect the actual credibility of a node, making difficult the implementation of the system in real environments. On the other hand, the approaches based on the inhibition use mechanisms to detect selfish users and inhibit them to make use of the network resources, and can exclude them from the traffic until they change their behavior [7]. In this approach, it is common the existence of a reputation system that measures the reliability of a node collaboration from the point of view of their neighbors, reducing the reliability under evidence of non-cooperation, or increasing the reliability otherwise.

This paper presents a new reputation mechanism as a mean to build a model of trust among the network users. We introduce a clustering approach to classify the nodes into classes according to its respective reputation values. Unlike other studies in the literature, we use a new way of providing a reputation system that is consistent with the social patterns present in opportunistic networks based on the user contacts. The proposed mechanism reflects the degree of selfishness and cooperation in the social field. Just as two users have different degrees of social relationships, they may have different degrees of selfishness with the rest of the population, and our model aims to capture this possibility by using the clustering technique to separate them accurately.

For this purpose, we assume that the contact is an opportunity for decision-making, in which each node has to take actions (cooperate or not cooperate), and each action is performed with a probability of the node to be or not to be selfish. We evaluate this mechanism through a robust scheme to make the overall learning process by aggregating data from different users for further dissemination of informations about the selfish nodes in the network. This way, the information also comes from other users, decreasing the time for learning effectiveness. Subsequently, we apply our formulation to a simulation driven by contact traces taken from real environments to estimate the effectiveness of the learning process.

II. Related Works

Opportunistic networks operate independently of a central authority or basis. The nodes exchange messages with each other to provide connectivity. A node is said to be selfish when it refuses to forward data from other nodes due to individual actions such as saving energy or buffer space. The frequency of selfish actions, however, strongly degrades the overall network performance [3], [4], [2]. Thus, recognition of selfish behavior is crucial for modeling protocols that can ensure future cooperation between the network nodes by means of reaction methods to selfish behavior as punishment [4] or incentive incentivo [8]. Some papers in the literature address the classification of selfish nodes. In some cases, however, because of inherent features of opportunistic networks, to ensure a positive review for a selfish node becomes a difficult task.

Some mechanisms found in the literature propose to detect selfish behavior using detection system like watchdog [4] and the catch [9] protocol. Basically, in these systems the nodes have a module aiming to discover the misbehaving nodes. To address this problem, the nodes overhear the wireless channel in order to analyze the traffic to identify misbehaving trend. However, due to the noisy channel, the node mobility and the lack of connectivity, the detection accuracy is not always guaranteed, producing a rate of incorrect detections. The following terms are important for understanding the argumentation discussed here..

True positive (TP)
When a node is classified as selfish, and it is indeed selfish.

False positive (FP)
When a node is classified as not selfish, but it is selfish.

False negative (FN)
When a node is classified as selfish, but it is not selfish.

True negative (TN)
When a node is classified as not selfish, and it is indeed not selfish.

Reputation systems have emerged as an alternative to the measurement of the cooperation level of a node when there is a level of uncertainty involved in the detection. In a reputation system, each node observes the behavior of their neighbors and builds a table with the reputation values. A low-reputation value means that the neighbor node probably has a selfish behavior while a high-reputation value signalizes a cooperative behavior.

We consider that the correct classifications are either TP or TN, while FP and FN are inaccurate ratings. Reputation systems are an attempt to minimize the number of incorrect recognitions when there is a level of uncertainty about the observations made by the nodes. The assumption made by reputation systems are that it is most accurate to classify an agent about your behavior when the number of observations about it increases. Marti et al. [4] proposed a model of detection and reputation on which the detection system (watchdog) uses a threshold value θ to determine the misbehavior of a particular node. However, aspects such as transmission power, collision and high delays are bottlenecks for watchdogs.

To minimize the magnitude of false positives and false negatives on detection, they proposed a mechanism of reputation called *pathrater*, that maintains the reputation of each node, excluding from the routing the nodes that reach a very low threshold of reputation. The pathrater keeps the ratings for other nodes to perform the node selection for routing data. Therefore, the packets are carried by the nodes with the highest reputation in the path. The reputation of nodes increases periodically while a path is active and decrease after each connection between the nodes are broken detected by the watchdog system.

Bansal et al. [10] proposed a reputation system in which the penalty imposed to nodes detected as selfish is -2, while the benefit applied to not selfish nodes is +1. Every node starts with a reputation equals to zero and when this reputation values exceeds a certain threshold $\theta = -40$, this node is put on a faulty list. The goal is to impose a lenient punishment to nodes detected as selfish. To give a second chance, the nodes are removed from the faulty list after a certain timeout t. However, this removal is made without any criterion as a change at the behavior of the detected selfish nodes. Thus, this method fails on punishing or incentivizing the selfish nodes in an appropriate way.

Buchegger and Le Boudec [2] proposed CONFIDANT, a protocol that has an integrated mechanism that updates the reputation of a node when the evidences of selfish behavior exceed a particular threshold value. Additionally, they inserted a collaborative model for cooperation among the nodes. The rating is calculated by a function that assigns weights to own

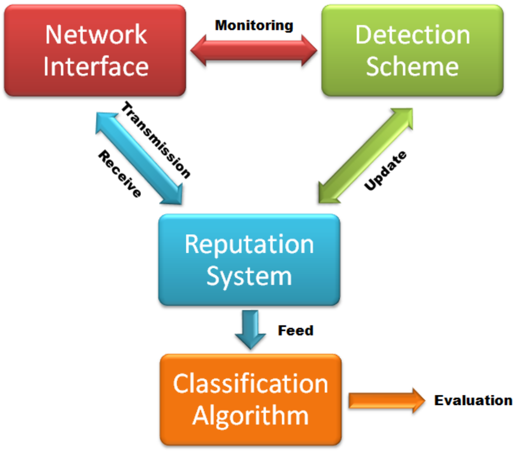

Fig. 1. Architecture of a network node

detections (higher weight) and information from neighbors (less weight).

In [11], the CONFIDANT mechanism of reputation uses a Bayesian filter to predict future behaviors after counting the positives and negatives related to the network nodes. The authors define a Beta distribution function to indicate the level of cooperation of a particular network node from its positives and negatives. Similarly, Li and Das [12] periodically decrement the reputation of the nodes not observed during a time interval. Due to the sparse nature of communication in opportunistic networks, this may not reflect the cooperation level of a node when a contact is established, and can generate inconsistencies under the influence of methods of punishment. Gini and Luca [13] assign weight for loss of reputation while there is no contact, and increase the reputation only for nodes that participate as intermediate nodes of messages transmitted successfully.

III. System Model

We define a network by a set of N mobile nodes and S selfish nodes Initially, the nodes have the same reputation, and no information about the network. Each node operates in a promiscuous mode and it may listen to every bundle transmitted by its neighbors. All the nodes have a common technique to detect selfish behavior by overhearing the bundles transmitted and received by its neighbors, in order to detect anomalies. Figure 1 shows the component structures of each network node. It has three main components acting with the network interface. The first one is the detection scheme, responsible by monitoring the data traffic searching for selfish nodes. The second one is the reputation system, which measures the cooperative level of its neighbors. And the third one is the classification algorithm used here to do fast classification of nodes based on its reputation. Thus, we first describe the network model which will be used in this discussion for further description of the reputation scheme and the classification technique presented in this work.

A. Network Model

We assume that the nodes are selfish, but they are not malicious, that is, they do not send false information over the network. Based on this premise, the network is modeled as an arbitrary graph $G = (N, E)$, with N nodes, E edges and S selfish nodes. We assume that every node has a detection mechanism like a watchdog. Since the detection system is not addressed in depth here, we assume that the detection method operates with a probability of detection P_e of detecting successfully the behavior of a node. Thus, we can vary the efficiency of the detection method with respect to detection errors on these systems We also assume that the network nodes operate in a broadcast mode in which the information about the knowledge of a network node can be disseminated between nodes when there is an edge connecting them.

B. Reputation Model

The reputation system executed by each node is an extension of the components presented in [2]. Each unselfish node carries a monitoring module to assess the behavior of neighbor nodes in the network. By each contact, some assessment is performed despite a node is selfish or not selfish. Thus, a node can get information from a neighbor B when one of the following situations occurs:

Selfish Contact
Node A, using its monitoring mechanism during a contact, detects that a neighbor node B is selfish. However, since monitoring errors can occur, we model this fact by using the probability of detection P_e

Not Selfish Contact
Both nodes A and B are not selfish. So they may share information about individual probes to feed the distributed reliable system. Similarly, the not selfish contact can be erroneously detected as selfish because the effectiveness of the detection system. Again this is modelled by the probability of detection P_e.

We model the contact between the nodes of the network as an infinitely repeated game. Each contact is a game $J = (N, A)$ with N players (nodes), and A = {cooperate, do not cooperate}, a set of possible actions of a player during an interaction. During a contact, the node u has interest that node v forward its message over the network, but v may or may not have interest to cooperate based on the trade-off between benefit and cost ratio related to the transfer. Thus, we define a round involving a pair of nodes in the contact $(u, v) \in E$ as the pair (A_u, A_v) employed by the pair (u, v) during the contact.

Every not selfish node is able to detect, with a certain probability of efficiency if a neighbor node is selfish. Each node can maintain a table of type (ID, R) which serves to maintain the individual history on its neighbors collect by its own, and assign a reputation value R for each node ID in accordance with the observations. We call R the degree of collaboration associated with the contact between (u, v).

Even for the collaborative nodes the reputation can be discriminating because of the social process associated with opportunistic networks. Collaborative nodes with stronger social bond will have higher reputation than collaborative nodes with weaker social ties. To address this variation of the problem, we use a variant of the sigmoid function[14], a mathematical strategy commonly applied in the literature on learning systems, neural networks, among others. The sigmoidal functions are able to assess the probability of occurring an event based on the experience observed in the system. When the network is started, the cooperation probability is equal for all nodes, but as the observations related to cooperation are collected from the network, these values are adjusted until cooperation probability reaches a value with little variability.

The observations of the behavior of the neighbor nodes is sufficient at some point in time to accurately understand a particular state of the system. The understanding of the systems becomes reliable even under small variations in the observations. These variations can raise from communication errors and errors in the detection system. We apply this function to the reputation model from new observations collected from the network, until the moment, the ranking can be considered reliable, with little risk of false negatives or false positives.

Since in opportunistic networks the total number of nodes is unknown, the scalability has to be considered, as well as the variation of the cooperation level due to reaction methods as methods of punishment/incentive. Thus, we discuss methods of further reaction with no major disruption in the reputation data. Another remarkable feature of these functions is the display of learning curves that can be used to predict the future behavior. This is a valuable function as we can predict selfish nodes with more accuracy and less information. This way, we analyze the probability of a node u to be more cooperative than v as a decision process defined by Eq. (1):

$$P_{cooperation}(u,v) = \frac{1}{1 + 10^{\frac{R_v - R_u}{F_d}}} \tag{1}$$

where $P_{cooperation}(u,v)$ describes the probability of u be more cooperative than v, R_k is the reputation of node $k \in N$ and F_d a significance factor to stress the difference between the reputations of the pair (u,v). Assuming $F_d = 5$, and the reputation of the pair $(R_u, R_v) = (10, 4)$, as well as $|R_v - R_u| > F_d$, the variation is significant to evaluate that node u is much more cooperative than v, $P_{after_{c}ooperation}(u,v) \simeq 0.94$. However, if $(R_u, R_v) = (8, 7)$, then $P_{cooperation}(u,v) \simeq 0.61$, which means that the difference between reputations may not be significant for an accurate assessment of the cooperation level between them, whereas in the first case the difference may mean that v can be selfish.

Thus, we define the update process as a two-step process for each pair of contact (u,v): update of the node v reputation and the reputation of the neighbor nodes of u, except v. In this case, we chose to create the second step as a way of encouraging the not selfish nodes by increasing its personal reputation through positive for selfish nodes. This update, however, only occurs when there is a positive selfishness on node v, not penalizing other nodes (selfish and not selfish) when in contact with v, not selfish node. The process of updating reputation goes like this:

Average reputation

By every contact, the node calculates its average reputation by Eq. 3, the arithmetic mean of the reputation of the neighbors at the moment of contact with node v.

$$AR(u) = \frac{\sum_{\forall k \in neighborhood_u - \{v\}} R_k}{|neighborhood_u| - 1} \tag{2}$$

Node update

The individual update of a node, when there is a positive for selfish node, is computed through Eq. 2, where $D(v) \in \ 0, 1$ assumes 0 when v is selfish and 1 otherwise. δ is he weight assigned to each new observation.

$$R_v{}' = R_v + RF(D(v) - P_{cooperation}(u,v)) \tag{3}$$

Neighbor update

The update of the other neighbor nodes is given by Eq. 2, with $D(k) = 1$, $P_{cooperation}(k,v) \forall k \in neighborhood_u$.

By means of the reputation model, each node can infer the behavior of a neighbor node based on its reputation value. Therefore, we introduced a verification algorithm which allows the classification of the behavior of a neighbor node after by collecting a number of observations. For this purpose, we use a clustering algorithm to choose from which moment on the available samples are enough to distinguish the reputations of selfish nodes and not selfish nodes.

C. Classification Model

Reputation systems perform sampling of the behavior of the network nodes based on the collected observations. Although the use of threshold is a widely adopted alternative in the literature, it may not accurately reflect the actual state of the network behavior. The first difficulty is the choice of the threshold value. High values may indicate low reliability though the convergence rate to this value is high. On the other hand, low values can indicate low reliability but with shorter convergence rate. In the latter case, however, the detection system may be vulnerable to sample errors, yielding low values of reputation. Since in opportunistic networks the contact distribution function does not follow is not uniform [15], the reputation values may converge at different rates for each network node. Because the contact of a selfish node can be more frequent inside a group of nodes than others, nodes with more contacts with selfish nodes will be updated a greater more frequently.

Our proposal includes a classification model-based clustering technique, which aims at separating the information already collected from the network into groups of users suspected of selfish behavior and not suspected of selfish behavior. The main advantage of this method is the ability to learn from the collected information besides fulfilling when necessary. Reputation systems can be used as a more accurate model to predict the behavior of a neighbor given its reputation. Basically, a node can classify its neighbor behavior as selfish or not selfish based on reputation values generated by the reputation scheme. However, reputation is a relative measure from the point of view of the nodes, and can not be classified *a priori* since the initial state of the network knowledge about the misbehavior of any node is unknown. Thus, the ability of learning is an essential component that makes the reputation model intelligent.

Some works in the literature utilize a threshold to assess a suspicious node as selfish. However, in opportunistic mobile networks this value may be subject to the distribution function of human contacts in these networks. To avoid this and be able to perform a classification without relying on network parameters, we used the technique of unsupervised learning, where the initial state of agents is unknow. This is an attempt to find a way to structuralizing nodes into clusters based on their reputation. Thus. each node can classify a suspect node whose characteristics vary greatly from one group of users with higher reputation.

Clustering techniques have been previously applied to build models of network behavior based on the nodes [16]. Grouping or clustering is the method of grouping objects into meaningful subclasses so that the members from the same cluster are quite similar. and the members from different clusters are quite different from each other [17]. Thus, clustering schemes are useful for classifying misbehavior based on reputation values.

We choose a partitioning algorithm for clustering data. This type of algorithm constructs a partition of the objects in a set of K clusters. Particularly, we used the k-means algorithm for construct these clusters. K-means takes into account which instances (the reputations of nodes) are represented on a euclidean space. Initially, each instance is assigned as a cluster of size equals to one. The iterative approach of this method puts each instance in one of the K clusters whose mean yields the least within cluster sum of squares. Since the sum of squares is the squared euclidean distance, so, each instance is assigned as the nearest cluster, i.e., the most similar class based on its attributes, in this case these attributes are the reputation values for neighbor nodes. At the end of iterations, the centroid values are returned by this algorithm. In this work, we used $K = 2$, whose first class covers the selfish nodes and the second class covers the cooperative nodes.

To evaluate the performance of the k-means algorithm applied to our model, we used the *Silhouette* coefficient to interpret and validate the clustered data [18]. In this method, the clustering efficiency is measured by the ratio of cohesion to dispersion of data within a class compared to other classes. Optimal values of this ratio are close to 1. We also evaluate the accuracy of clustering, analyzing the true positive rate (selfish nodes classified as selfish nodes) and the true negative rate (not selfish nodes classified as not selfish) given by Eq. (4) and Eq. (5), respectively. In this case, we consider that true positive rate is the accuracy for classification of the selfish nodes in a cluster containing nodes with selfish features and a true negative rate for the second cluster.

$$True\_Positive\_Rate\ (TPR) = \frac{TP}{TP + FP} \tag{4}$$

$$True\_Negative\_Rate\ (TNR) = \frac{TN}{TN + FN} \tag{5}$$

IV. Experimental Evaluation

We designed and implemented a trace-driven discrete event simulator written in C++. A trace file was obtained from measurements taken on real-world occurrences of pairs of contacts between devices carried by humans occurring in a given time interval. The trace is a set of a 4-tuple $< t_i, N_a, N_b, d_i >$, $1 \leq i \leq |T|$, with $|T|$ represents the number of instances of trace T and d_i a contact duration in the i-th instance. A contact is a chance for transmission between a pair of nodes (N_a, N_b).

The simulator takes as input the number of nodes N, the number of selfish nodes S, the efficiency rate of the detection system P_e and the simulation timeout. The contact trace used was the Reality Mining [19], experimentally conducted at MIT in a period of 246 days, with 97 samples. Was performed three different network observation, using the first 24, 48 and 72 hours of contact trace chosen empirically.

Since contacts are not uniformly distributed, we had to choose the selfish nodes randomly by using only the portion of nodes with the strongest social ties in the network. We did this in order to avoid large variation in the resulting samples since we found that selfish nodes with weaker social ties are more difficult to be observed. To accomplish this, we calculated the popularity based on the concept of freeman centrality [20], that is, how popular is a network node based on the number of contacts made with it.

Finally, we evaluate the performance of our model with different values of probability of detection P_e to study the behavior of the reputation system and the clustering algorithm for correctly classify the nodes.

V. Results

We evaluated the performance of our model by using different values for the detection probability efficiency P_e. We analyzed the silhouette coefficient to assess cohesion and dispersion of data in each class separated by k-means method (selfish and not selfish class). In the sequence, we analyzed the true positive and true negative rates for each class for different simulation run lengths, as described in Table I. When P_e increased from 75 % to 95 %, the silhouette coefficient improved about 9 % for 24 hours of observation, and about 11 % for 72 hours of observation. However, the detection rate of true positive (selfish nodes correctly detected as selfish nodes) was very accurate (around 89 %) when $P_e = 75\%$, with a gain of approximately 6 %.

Although there is no great improvement in the coefficient silhouette as the detection system becomes more effective, it achieves high reliability in terms of TPR and TNR, due the communication pattern in opportunistic networks. Although the silhouette coefficient is able to cover a good cohesion in the data classification represented by clusters, it is not able to represent well the dispersion of the reputation samples for the network nodes due to the communication pattern between nodes. When the simulation run length is long, the possibility of sporadic contacts between the network nodes grows accordingly. These contacts, however, are counted if the detection method is able to evaluate the neighbor node. When this occurs, the reputation of neighbor is changed, but it can take a while to be updated again due to sporadic contact with that neighbor, making samples slightly more dispersed, without affecting the silhouette coefficient, however, affect the accuracy of the TPR and TNR rates.

Another important evaluation carried out was the rate of true negatives. This metric is critical because during the launching of the reactive methods for misbehavior in the network since there is a more negative impact over the classification of a not selfish node as a selfish node (false negative) than the opposite case (false positive). An accuracy above 95% was obtained for $P_e \geq 80\%$, while for $P_e = 0.75$ yielded a minimum of 92% of accuracy, for a 48-hours run length.

$P_e = 0.75$			
Simulation run length	24	48	72
Silhouette	0.7001	0.70926	0.7488
TPR	0.8960	0.9373	0.9554
TNR	0.9427	0.9280	0.9733
$P_e = 0.80$			
Simulation run length	24	48	72
Silhouette	0.7295	0.7337	0.7819
TPR	0.9470	0.9619	0.9795
TNR	0.9575	0.9621	0.9838
$P_e = 0.85$			
Simulation run length	24	48	72
Silhouette	0.7499	0.7559	0.8031
TPR	0.9401	0.9604	0.9807
TNR	0.9725	0.9614	0.9875
$P_e = 0.90$			
Simulation run length	24	48	72
Silhouette	0.7462	0.7703	0.8231
TPR	0.9460	0.9858	0.9873
TNR	0.9753	0.9740	0.9921
$P_e = 0.95$			
Simulation run length	24	48	72
Silhouette	0.7673	0.7765	0.8259
TPR	0.9852	0.9895	0.9957
TNR	0.9891	0.9833	0.9972

TABLE I. RESULTS

VI. CONCLUSION

In this paper, we proposed a mechanism to detect selfish behavior based on a reputation system together with a clustering algorithm to find when the collected observations are sufficiently accurate to classify the nodes either selfish or not selfish. We used the probability of detection for the detection system, and we assessed the classification accuracy for true positives, true negatives, and we evaluated the performance of clustering using the silhouette coefficient. The numerical results show that this method has a high degree of accuracy even when there is variation in the reputation values of a node. This is due to the learning property of the sigmoid function used to model the reputation system.

This model can be used as a component for designing routing and congestion control algorithms for opportunistic networks with selfish nodes. By not using threshold values, also allows this system to classify without being dependent on the structure of communication among users. Moreover, the proposed model presented a rapid degree of convergence. As a future work, we intend to evaluate the proposed model for different levels of social egoism, that is, in scenarios when the nodes tend to behave selfishly to other nodes with weak social bond.

REFERENCES

[1] R. Hardin, "The free rider problem," in *The Stanford Encyclopedia of Philosophy*, spring 2013 ed., E. N. Zalta, Ed., 2013.

[2] S. Buchegger and J.-Y. Le Boudec, "Performance analysis of the confidant protocol," in *Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing*. ACM, 2002, pp. 226–236.

[3] Y. Li, G. Su, D. O. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 5, pp. 2224–2238, 2011.

[4] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*. ACM, 2000, pp. 255–265.

[5] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies*, vol. 3. IEEE, 2003, pp. 1987–1997.

[6] L. Buttyán and J.-P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks," *Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003.

[7] P. Michiardi and R. Molva, "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks," in *Advanced Communications and Multimedia Security*. Springer, 2002, pp. 107–121.

[8] Q. He, D. Wu, and P. Khosla, "Sori: a secure and objective reputation-based incentive scheme for ad-hoc networks," in *Wireless Communications and Networking Conference, 2004. WCNC. 2004 IEEE*, vol. 2. IEEE, 2004, pp. 825–830.

[9] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Sustaining cooperation in multi-hop wireless networks," in *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*. USENIX Association, 2005, pp. 231–244.

[10] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," *arXiv preprint cs/0307012*, 2003.

[11] S. Buchegger and J.-Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," *Communications Magazine, IEEE*, vol. 43, no. 7, pp. 101–107, 2005.

[12] N. Li and S. K. Das, "Radon: reputation-assisted data forwarding in opportunistic networks," in *Proceedings of the Second International Workshop on Mobile Opportunistic Networking*. ACM, 2010, pp. 8–14.

[13] G. Dini and A. L. Duca, "A reputation-based approach to tolerate misbehaving carriers in delay tolerant networks," in *Computers and Communications (ISCC), 2010 IEEE Symposium on*. IEEE, 2010, pp. 772–777.

[14] V. Rodriguez, "An analytical foundation for resource management in wireless communication," in *Global Telecommunications Conference, 2003. GLOBECOM'03. IEEE*, vol. 2. IEEE, 2003, pp. 898–902.

[15] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket switched networks and human mobility in conference environments," in *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*. ACM, 2005, pp. 244–251.

[16] L. Bo and J. Dong-Dong, "The research of intrusion detection model based on clustering analysis," in *2009 International Conference on Computer and Communications Security*. IEEE, 2009, pp. 24–27.

[17] M. Jianliang, S. Haikun, and B. Ling, "The application on intrusion detection based on k-means cluster algorithm," in *Information Technology and Applications, 2009. IFITA'09. International Forum on*, vol. 1. IEEE, 2009, pp. 150–152.

[18] P. J. Rousseeuw, "Silhouettes: a graphical aid to the interpretation and validation of cluster analysis," *Journal of computational and applied mathematics*, vol. 20, pp. 53–65, 1987.

[19] N. Eagle and A. (Sandy) Pentland, "Reality mining: Sensing complex social systems," *Personal Ubiquitous Comput.*, vol. 10, no. 4, pp. 255–268, Mar. 2006. [Online]. Available: http://dx.doi.org/10.1007/s00779-005-0046-3

[20] L. C. Freeman, "A set of measures of centrality based on betweenness," *Sociometry*, pp. 35–41, 1977.