Novel Routing Protocol for Mobile Ad hoc Networks with Selfish and Altruistic Nodes

Dimitra G. Kampitaki and Anastasios A. Economides
Interdepartmental Programme of Postgraduate Studies in Information Systems
University of Macedonia
Thessaloniki, 54006 Greece
{kampitaki, economid}@uom.gr

Abstract— **Selfish behavior may be observed in a Mobile Ad hoc Network (MANET) due to restricted resources. Unlike the past research which aimed to suppress that kind of behavior and isolate selfish nodes, we propose a scheme which exploits selfish behavior to improve the routing protocol's performance. We introduce an altruism coefficient which represents each node's overall satisfaction from the network services and while increased, it decreases selfish behavior. We then apply our scheme to an existing routing protocol and evaluate its performance. We show by simulation, that when selfish nodes exist in the network, our scheme improves the performance of the routing protocol.**

Keywords— altruism, Mobile Ad hoc Networks, routing protocols, selfishness

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) [1], [2] are mobile wireless networks without predefined infrastructure or central authority. They are characterized as open or closed depending on whether new nodes can or cannot be accepted into the network or whether there is connectivity with nodes not in the network. In a closed MANET the nodes that compose the network are in most cases all of the same type and probably are deployed from the same authority, in order to serve a common goal. On the contrary, in an open MANET, nodes can be of different types and therefore malicious or selfish behavior might occur. While malicious nodes are addressed as security threats, selfish nodes should not, as their behavior can be predicted and addressed, without excluding them from the network.

Routing protocols that were designed for early MANETs took for granted that all the nodes composing the network were willing to cooperate in order to serve a common goal, which in most cases was to sustain connectivity between nodes and transmit critical data. When mobile devices with advanced connectivity features became widely used, open MANETs came to reality. And while in a closed MANET existing routing protocols were sufficient and well performing, in an open MANET the same routing protocols have proven to perform poorly, due to the selfishness problem that emerged. Several approaches to that problem have been proposed so as to minimize the effects of that heterogeneity which emerged in an open MANET. In this paper, we present and evaluate a scheme that uses selfishness and altruism in MANETs in such a manner that can boost the performance of reactive routing protocols.

As a first step towards that, we have to define the terms selfishness and altruism. When the first MANETs emerged, the routing protocols took for granted that all of the nodes composing the network would be fully and utterly cooperative. There was no case of misbehavior, as the nodes of the network belonged to the same authority and there were no security threats. Thus, when a node was asked to forward a packet for a neighboring node, it was obliged to do so, even if that meant that no energy would be left for its own communication needs. We can define this kind of behavior as altruistic and consider it as the default behavior for the nodes when their resources are not restricted.

Nowadays, MANETs have evolved to open systems and at any time new nodes can join the network, nodes that operate under different authorities or with different energy, or processing capabilities can co-exist in the same MANET and share resources. Under this new paradigm, nodes can no longer be considered de facto cooperative or non-malicious. Selfishness occurs when energy or other resources of the node become low, so that the node will be only able to satisfy its own communication needs. In this work, we take into account only the energy level of the nodes and we assume that no nodes leave or enter the area where the MANET is located and there are no other networks in this area.

In the present work, we do not focus on security issues, so we do not include malicious behavior into our study. A node can be characterized as selfish when it deliberately drops or delays Route Request Packets (RREQ) during the Route Discovery Phase of the routing protocol, in order to save resources for its own communication needs. Other research might define selfish behavior differently, but for the purposes of our research we define as selfish a node that due to low energy resources deliberately drops RREQ packets. By dropping RREQ packets selfish nodes manage not to be selected as relay nodes for data transmission from a source to a destination node.

The rest of the paper is structured as follows: In Section II there is a concise review of related research. The proposed protocol is presented in Section III and its performance is analyzed in Section IV. Finally, Section V concludes the paper.

II. RELATED WORK

In this section a brief review of previous related research is presented. Various protocols have been designed and implemented for use in MANETs. They are categorized as

978-1-4673-8409-4/16/$31.00 ©2016 IEEE

proactive, reactive and hybrid, depending on the maintenance (proactive) or not (reactive) of a routing table at each node or partial of these behaviors (hybrid). There have been several performance evaluation and comparative studies that examine MANET routing protocols under different aspects and problems [3]-[11].

Selfishness is a problem that has yet to be addressed adequately, although it has been studied a lot. One of the first to identify and define misbehavior in MANETs was Marti in [12]. In his work the objective was to mitigate misbehavior. Following that, several works have been proposed [13-22]. In most cases the objective was to detect and isolate selfish nodes, while in others various schemes to encourage cooperation were proposed, either by credit-based [15], [18] or by reputation-based schemes [13], [14], [17]. A rather comprehensive review of selfishness in MANETs can be found in [23].

Research has also been made towards modelling selfishness and apply general solutions to the selfishness problem. In [24] an attempt is made to formally describe selfishness. Other studies employed game theoretic modeling [25] or semi Markov processes [26].

In [27] the operation of Dynamic Source Routing (DSR) protocol is investigated as selfishness emerges in a MANET due to energy depletion. Different types of selfishness are defined and the protocol performance, when nodes of different selfishness types coexist in the network, is examined. Three thresholds are defined and the probability between two thresholds is constant. This approach is used as a starting point for the present work. The main advantage of this approach is that when the node disseminates selfishness information, only two bits are required to represent the selfishness level, hence keeping routing overhead as low as possible.

III. PROPOSED PROTOCOL

In this section we analyze the structure and operations of the Selfish Aware Protocol we propose, namely Selfishness Aware Dynamic Source Routing (SA-DSR). By applying our scheme on one of the most well-known, widely used and researched reactive routing protocol we set a new starting point for research in this field.

A. Overview of the Dynamic Source Routing Protocol

Dynamic Source Routing (DSR) is one of the first reactive routing protocols proposed for use in Mobile Ad hoc Networks. However, it is designed by taking for granted that all the nodes that compose the network are cooperative, hence they are willing to forward packets from and to neighboring nodes to their destination.

DSR operation is based on two primary phases: the route discovery phase and the route maintenance phase. During route discovery phase the source node floods the network with Route Request Packets (RREQ) in order to find a route towards its intended destination node. Following that the route maintenance phase keeps alive discovered routes as long they are still available. The complete specification of the DSR protocol can be found in [29].

B. Selfishness Aware Dynamic Source Routing (SA-DSR)

The part of the DSR protocol, that we modify and extend to implement SA-DSR, belongs to the Route Discovery Phase and specifically to the Route Selection phase. We also modify the Route Reply (RREP) packets' structure to include the selfishness information of the nodes.

Each node depending on its remaining energy or other resource constraints has a Selfishness type that defines the percentage of the packets it forwards or drops, as can be seen in Table I, and has been thoroughly studied in [27].

We introduce a new metric to achieve optimal route selection, namely Successful Delivery Probability (SDP). Also, we define a new node property, namely Altruism Coefficient (AC), which is used to represent the satisfaction that the node has acquired from the network so far.

SDP is defined by the product of the Forwarding Probability (FP) for each intermediate node in the path(s) that connects source node S and destination node D. Each path between S and D has its own SDP. The FP of each node is defined by its selfishness level combined with the node's AC. The path selection is made by the source, as defined in the DSR specification, but instead of using *shortest path* as the path selection algorithm, SDP is calculated for each path towards the destination, and the path with the higher SDP is selected. In the case that two or more paths have the same SDP, the most recent of them in the route cache is selected.

Using these concepts, we propose a new routing scheme that exploits selfishness and altruism, and provides thus the network with the ability to overcome implications that emerge due to possible selfish behavior of some nodes. To demonstrate its effect we apply this scheme to DSR.

The proposed routing protocol operates as follows:

- When node S (source node) needs to send data to node D (destination node), it checks its routing table for existing paths;
- If there are at least two paths to the destination node D then the path with the higher SDP is selected and the data transmission starts;
- If there is only one or no path to the destination, then a RREQ packet is broadcasted into the network. The source node operates in promiscuous mode and for each retransmission of the RREQ from its neighbors it raises its AC. If no retransmission of RREQ is detected, AC decreases. If a timeout occurs without a RREP being received, AC decreases as well. In that last case, a RREQ is again broadcasted for some more times, and if

TABLE I. SELFISHNESS TYPES AND PACKET DROP PROBABILITY

Residual Energy (%)	***Selfishness Type***	***Packet Drop Probability***
80-100	Always Altruistic (AA)	0%
50-80	Sometimes Selfish (SS)	10%
20-50	Often Selfish (OS)	50%
<20	Always Selfish (AS)	100%

no path is found, the packet is dropped.

- When a relay node R receives a RREQ it has two options: to forward or to drop it.
  - If it forwards RREQ, it spends some energy e_t for the transmission but it increases the probability that source node S – which is currently considered to be R's neighbor – will in the future serve R's needs;
  - If it drops RREQ, it saves energy but in case the other neighbors also drop the RREQ packet, S's AC will decrease and S will be more selfish in future requests.
- When RREQ arrives at destination node D, a RREP packet is returned through the same path it arrived, as happens in the original DSR protocol. In that packet along with the path information that is stored, the Selfishness of each node is also stored and thus transferred towards the rest of the nodes. Since the nodes operate in promiscuous mode, selfishness information for each node is thus disseminated to other nodes in the network, and updated if required. In original DSR, when the first RREQ arrives at the destination node and the RREP is sent, other RREQ packets that arrive at a later time and originate from the same source node are ignored. In our scheme, we set a timer and all RREQ packets that arrive within specific time (depending on the size of the network) are answered with respective RREP packets. Hence, each node will have many paths to other nodes from which the path with the highest SDP can be selected.

According to the procedure described above, we modify the code of the original DSR implementation included in ns-3.24 [29], and perform a series of simulations to evaluate the performance of our scheme. Ns-3 is a discrete-event network simulator for Internet systems, targeted primarily for research and educational use. Besides the modification of DSR protocol, we also have to modify the energy module as well as the statistics framework to be able to achieve our simulation requirements and configuration and also to derive the required statistics. In the following section our simulation configuration and the simulation results are presented.

IV. PERFORMANCE EVALUATION

In order to evaluate the performance of our proposed protocol we conduct some sets of simulations. In this section, we present the simulation configuration and the obtained results.

TABLE II. SIMULATION CONFIGURATION

Parameter	*Value*
Simulation Time	Until the battery of at least one node runs out
Simulation Area	1500m x 500m
Number of Nodes	10 – 20 – 30 – 40 – 50
Transmission Range	250m
Mobility Model	Random Way Point
Node Speed	0 – 2m/s
Traffic Generator	CBR
Packet Bytes	64 bytes
Data Rate	2 MBps

A. Simulation scenario

The general simulation parameters are denoted in Table II. All simulations are averaged over 10 runs. The simulation space consists of an open-space area of 1500m x 500m inside which a varying number of nodes is moving, according to a Random Way Point Mobility Model with a speed ranging from 0-2m/s. The transmission range for each node is set to 250m. To avoid congestion, we use 64B packets sent with a rate of 4 packets/sec.

Three cases are examined:

a) Original DSR without selfish nodes

In this case we use the original implementation of DSR and only cooperative altruistic nodes are present in the network. The results from this case are used as a comparison reference measure for better understanding.

b) Original DSR with selfish nodes

In this case we use the original implementation of DSR but a number of selfish nodes is present in the network from the beginning of the simulation and as time passes by and the energy of the nodes gets depleted, the number of selfish nodes increases. The simulation stops when the battery of at least one node runs out. To accomplish that, we had to make several modifications to the energy module.

c) SA-DSR with selfish nodes

In this case we use our modified DSR implementation, namely SA-DSR, while a number of selfish nodes is present in the network from the beginning of the simulation and as time passes by and the energy of the nodes gets depleted, the number of selfish nodes increases. The simulation stops when the battery of at least one node runs out. We set properly the seeds and the random generators in the simulator so as to have

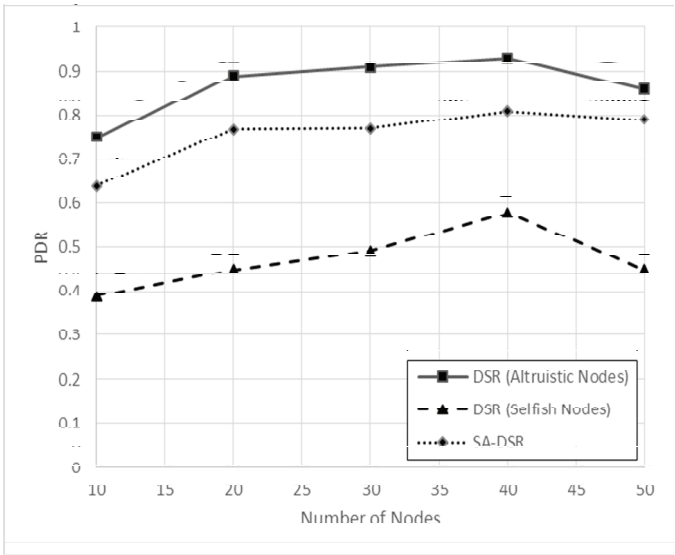

Fig. 1. Packet Delivery Ratio vs Number of nodes

similar conditions between cases b and c. Also, we use the modified energy model we used in case b.

For each of the aforementioned cases we extract the following metrics to measure and compare the performance of our proposed protocol:

- Packet Delivery Ratio (PDR): This metric is the percentage of successfully received packets and is computed by dividing the total number of packets received by destination nodes with the total number of data packets sent from source nodes.
- Average End-to-End Delay (AEED): This metric is the average time a data packet needs to be delivered to its destination. It is computed by averaging the end-to-end delay for all successfully delivered packets in the network.
- Normalized Routing Overhead (NRO): This metric is computed by dividing the total control packets with the total packets received in the network.

B. *Simulation results*

As stated earlier, we execute the simulation for three cases and three metrics, i.e., PDR, AEED and NRO. In this section we present the results of our simulations. In Figs. 1-3, PDR, AEED and NRO are respectively presented for each of the three cases.

As expected, the original DSR has better performance when there are only altruistic nodes in the network and no selfishness occurs. PDR is close to 100% when the number of nodes is about 40, with lower values for less nodes, due to restricted connectivity and reachability. When the nodes are increased in number, PDR lowers again due to high node density which causes more interference between nodes.

When selfish nodes appear in the network, the original DSR's performance dramatically drops. In terms of PDR, less than half of the total packets get delivered to their respective destinations. AEED appears to have lower values, but this fact is not due to better performance but due to limited connectivity that occurs because of the presence of selfish nodes. In simple terms, longer paths are less likely to exist, hence resulting in less end-to-end delay. In the presence of selfish nodes, the proposed scheme seems to achieve PDR and AEED values close to those achieved by the original DSR when only altruistic nodes are present.

Also, due to packet drop that occurs when selfish nodes exist in the network, NRO also decreases in comparison to its respective values achieved in the case of the original DSR without selfish nodes. By applying our scheme, NRO becomes comparable to that of the original DSR without selfish nodes. This increment mainly happens due to the increased RREP packets utilized by the protocol.

V. Conclusion And Future Work

We managed to improve the performance of DSR protocol for MANETs by utilizing information concerning Selfishness and Altruism of the nodes. Without significantly increasing routing overhead, we are able to improve the PDR and the AEED, in comparison to the performance of original DSR when selfish nodes are present in the network.

In the future, we plan to apply our scheme to other routing protocols, such as Ad hoc On-Demand Distance Vector (AODV), as well as to extend it and further improve it.

References

[1] C. Siva Ram Murthy and B. S. Manoj. *Ad Hoc Wireless Networks: Architectures and Protocols,* Pearson Education, 2004.

[2] M. Abolhasan et al., "A review of routing protocols for mobile ad hoc networks," Ad Hoc Networks, Vol. 2, Is. 1, pp. 1-22.

[3] C. Samara, E. Karapistoli, and A. A. Economides. "Performance Comparison of MANET Routing Protocols based on real-life scenarios." Ultra Modern Telecommunications and Control Systems and Workshops

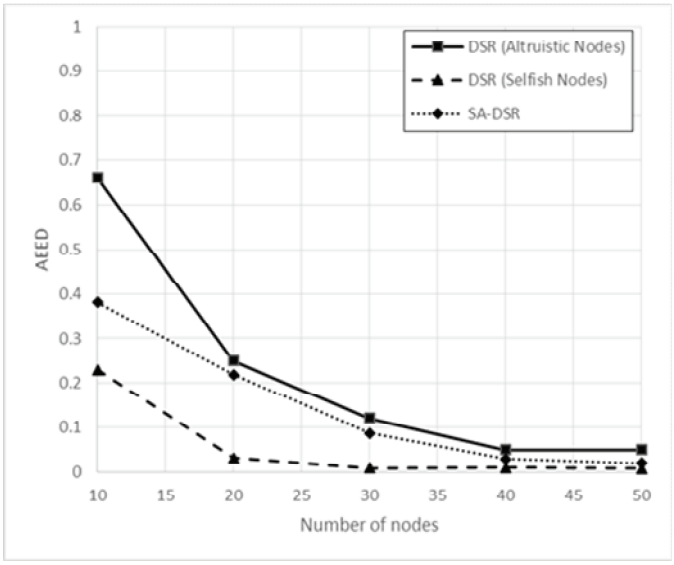

Fig. 2. Average End-to-End Delay vs Number of nodes

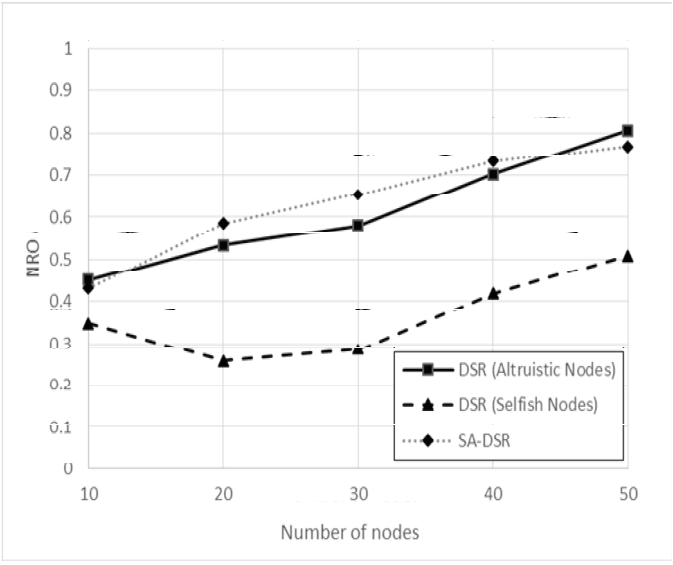

Fig. 3. Normalized Routing Overhead vs Number of nodes

(ICUMT), 2012 4th International Congress on. IEEE, 2012.

[4] D. G. Kampitaki and A. A. Economides, "Simulation Study of MANET routing protocols under FTP traffic", presented at the Conf. Elec., Telecom. Comp., CETC2013, Lisbon, Portugal.

[5] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva. 1998. "A performance comparison of multi-hop wireless ad hoc network routing protocols". Proc. ACM/IEEE MobiCom 1998, pp. 85-97.

[6] C. Mbarushimana and A. Shahrabi, "Comparative Study of Reactive and Proactive Routing Protocols Performance in Mobile Ad Hoc Networks," Advanced Inf. Netw. App. Workshops, 2007, AINAW '07, pp.679-684.

[7] N. Bilandi, and K. V. Harsh K. "Comparative Analysis of Reactive, Proactive and Hybrid Routing Protocols in MANET." Int'l J.l Electr. Comp. Sc. Eng., Vol. 1, Is. 03, pp. 1660-1667, 2012.

[8] C. E. Perkins et al., "Performance comparison of two on-demand routing protocols for ad hoc networks," Personal Commun., IEEE, vol.8, no.1, pp.16-28.

[9] F. Maan and N. Mazhar, "MANET routing protocols vs mobility models: A performance evaluation," Ubiquitous and Future Networks (ICUFN), Third Int'l. Conf., 2011, pp.179-184.

[10] B. Fan, N. Sadagopan and A. Helmy, "IMPORTANT: a framework to systematically analyze the Impact of Mobility on Performance of Routing Protocols for Adhoc Networks," Proc. INFOCOM 2003, pp.825-835.

[11] Y. H. Ho, A. H. Ho and K. A. Hua, "Routing protocols for inter-vehicular networks: A comparative study in high-mobility and large obstacles environments", Comp. Commun., Vol. 31, Is. 12, pp. 2767-2780.

[12] Sergio Marti, T. J. Giuli, Kevin Lai, and Mary Baker. 2000. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (MobiCom '00). ACM, New York, NY, USA, 255-265.

[13] Buchegger, Sonja, and Jean-Yves Le Boudec. "Performance analysis of the CONFIDANT protocol." Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing. ACM, 2002.

[14] Michiardi, Pietro, and Refik Molva. "Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks." Advanced Communications and Multimedia Security. Springer US, 2002. 107-121.

[15] Zhong, S.; Chen, J.; Yang, Y.R., "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, no., pp.1987-1997 vol.3, 30 March-3 April 2003.

[16] El-Haleem, Ahmed M. Abd, et al. "TRIDNT: Isolating Dropper nodes with some degree of Selfishness in MANET." Advances in Computer Science and Information Technology. Springer Berlin Heidelberg, 2011. 236-247.

[17] K. Balakrishnan, J. Deng, and P. K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," Proc. IEEE Wireless Commun. And Net. Conf. 2005, pp. 2137-2142.

[18] L. Anderegg and S. Eidenbenz, "Ad Hoc-VCG: A Truthful and Cost-Efficient Routing Protocol for Mobile Ad hoc Networks with Selfish Agents," Proc. ACM MobiCom 2003, pp. 245-59.

[19] V. Srinivasan et al., "Cooperation in Wireless Ad Hoc Networks," Proc. IEEE INFOCOM 2003, pp. 808-17.

[20] D. Hales, "From Selfish Nodes to Cooperative Networks – Emergent Link-Based Incentives in Peer-to-Peer Networks," Proc. IEEE Int'l. Conf. Peer-To-Peer Comp. 2004, pp. 151-58.

[21] M. Naserian and K. Tepe, "Game theoretic approach in routing protocol for wireless ad hoc networks," Ad Hoc Networks, Volume 7, Issue 3, May 2009, pp. 569-578.

[22] S. Yokoyama et al., "Evaluation of the Impact of Selfish Nodes in Ad Hoc Networks and Detection and Countermeasure Methods," 7th Int'l Conf. Mobile Data Manag., MDM 2006.

[23] Younghwan Yoo; Agrawal, D.P., "Why does it pay to be selfish in a MANET?," in Wireless Communications, IEEE , vol.13, no.6, pp.87-97, Dec. 2006

[24] Urpi, A., Bonuccelli, M., & Giordano, S. (2003). Modelling cooperation in mobile ad hoc networks: a formal description of selfishness. In WiOpt'03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (pp. 10-pages).

[25] Komathy, K., & Narayanasamy, P. (2007, February). Study of co-operation among selfish neighbors in MANET under evolutionary game theoretic model. In Signal Processing, Communications and Networking, 2007. ICSCN'07. International Conference on (pp. 133-138). IEEE.

[26] Azni, A. H., Ahmad, R., Noh, Z. A. M., Basari, A. S. H., & Hussin, B. (2012). Correlated node behavior model based on semi Markov process for MANETS. arXiv preprint arXiv:1203.4319.

[27] D. G. Kampitaki, E. D. Karapistoli and A. A. Economides, "Evaluating selfishness impact on MANETs," Telecommunications and Multimedia (TEMU), 2014 International Conference on, Heraklion, 2014, pp. 64-68.

[28] Johnson, D., The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4, RFC4728, February 2007, retrieved online from: https://www.ietf.org/rfc/rfc4728.txt

[29] https://www.nsnam.org/