Wireless Personal Communications
https://doi.org/10.1007/s11277-018-5914-z

Exploiting Selfishness, Altruism and Common Welfare to Enhance Performance of Routing Protocols for Mobile Ad hoc Networks

Dimitra G. Kampitaki[1] · **Anastasios A. Economides**[1]

Abstract
Mobile Ad hoc Networks are sensitive to selfish behavior that may occur due to restricted power or other resources. Several approaches have been investigated so far to address this problem. In many of them, upon detection, a selfish node is punished with isolation from network services access and in most cases with no possibility for redemption. In this paper, we show that selfish behavior can be exploited to improve network performance. We modify an existing routing protocol by introducing an altruism coefficient to model the overall satisfaction of every node from the network services. When the altruism coefficient is increased, the selfish behavior is decreased. We extend our approach by introducing a common welfare factor, which actually enforces the nodes to cooperate when the network connectivity is critical. A network simulator is utilized to show the impact of our schemes on the performance of the routing protocol when selfish nodes are present in the network.

Keywords Altruistic behavior · MANETs · Routing protocols · Selfish behavior

1 Introduction

Mobile Ad hoc Networks (MANETs) are multi-hop, self-configuring, wireless networks consisting of wireless mobile nodes that can be deployed without any fixed infrastructure, central administration or service provision [1]. Nodes move freely in the area and can communicate with each other directly if they reside into each other's transmission range or by relaying messages through multihop wireless links using other intermediate nodes as relay nodes.

Routing protocols for MANETs [2] were initially designed to be able to provide connectivity and transmit critical data between nodes in military and rescue operations. Since

✉ Dimitra G. Kampitaki
kampitaki@uom.gr

Anastasios A. Economides
economid@uom.gr

[1] Interdepartmental Programme of Postgraduate Studies in Information Systems, Computer Networks and Telematics Applications Lab (CONTALab), University of Macedonia, 54636 Thessaloniki, Greece

Published online: 31 July 2018

they were designed to serve a common goal it was taken for granted that they were willing to cooperate fully, in an absolute altruistic manner. There have been proposed several types of routing protocols. They can be categorized as proactive, reactive and hybrid. They have different principles of operation, but their common characteristic is that they take for granted that nodes who belong to the network are cooperative. However, as MANETs evolved and expanded to commercial applications, these routing protocols proved to be insufficient, mostly due to the selfishness problem that emerged.

When the resources, e.g., energy, processing power or memory capacity of the nodes get depleted, they act selfishly by deviating from the cooperative behavior. They do so, in an attempt to conserve their resources for their own communication and other purposes. Existing routing protocols do not have the capability to distinguish between actual failures of the nodes, selfish behavior or malicious security attacks. Hence, the schemes proposed to address the selfishness issue, in most cases, aimed to detect and punish misbehaving nodes by isolating them and denying them network services. In these cases trust based [3–5], and security oriented solutions have been proposed [6–8].

In [9] the authors examine the tradeoff between selfishness and altruism in terms of the individual welfare of a node and the global welfare, to manage trust in a MANET. In their point of view, selfishness is necessary in order to extend the lifetime of the MANET.

Following that point of view in our work, selfishness is not considered to be an attack of any kind. It is considered as a feature of the network, which can be used in favor of the network operation. We take for granted that nodes with low energy are not willing to be included in the routing paths formed between source and destination nodes. The protocol could be modified to include other resource metrics except residual energy to define selfishness. Instead of isolating and punishing selfish nodes as previous research suggested, in our approach we use them in such a way as to maximize the network lifetime. Each node has the option to become selfish and drop the packets but this would not be beneficial either for the node or for the network operation, as it will harm the altruism coefficient of its neighbors, meaning that they will be less willing to serve this node in the future.

To quantify the impact of selfishness and altruism in the network operation, we introduce a common welfare factor, to enforce nodes to cooperate when network connectivity has decreased to a critical level. This factor serves as a measure to maintain some connectivity when every node has reached a state of high selfishness and it does not receive service from other nodes. To overcome such a problem, this factor is used to properly spend the last resources for critical communication needs.

Finally, we distinguish selfish behavior from malicious behavior, as the second aims to harm the network performance intentionally. Overall, we attempt to utilize selfishness, altruism and common welfare in order to boost the performance of the routing protocol. We apply our scheme to the Dynamic Source Routing (DSR) protocol for MANETs in two distinct steps. In our first approach, we introduce the Altruism Coefficient (AC) and we propose Selfishness Aware Dynamic Source Routing (SA-DSR) protocol. Then we introduce the common welfare factor (CWF) and propose Selfishness and Common Welfare Aware Dynamic Source Routing (SCWA-DSR).

The structure of the rest of the paper is the following: In Section 2 we present a brief review of the research conducted so far. In Section 3, the structure and operation of the proposed protocols are presented, while in Section 4 the setup of our simulation scenarios is defined and the performance of our modified protocols is shown in respect to several metrics. In Section 5 we discuss our findings and conclusions and set our goals for future research.

2 Related Research

A concise review of previous research in this field is included in this section. Routing for MANETs is a very popular research field that has attracted many researchers, who have studied and implemented various routing protocols, and even more have been proposed in the literature but remained at an experimental form, without being implemented for actual use. The common categorization for routing protocols for MANETs is proactive, reactive and hybrid. Proactive routing protocols form a routing table upon their initialization and keep it always updated. Reactive routing protocols search for a path to a specific node if and only if it is needed. Hybrid routing protocols are a composition of the former two categories, taking advantage of the strong aspects of each of them. Many researchers have evaluated the performance of MANET routing protocols in comparison to each other [10–15] and examine them in terms of many different metrics by modifying various parameters. In [16], the Internet Engineering Task Force (IETF) suggested some of the metrics and the parameters that can be studied in MANETs.

Selfishness is a problem that occurred in MANETs after the mobile handheld devices became commonly used and commercial applications of MANETs became a reality. About two decades ago Marti in [17] identified and defined misbehavior in MANETs, however the selfishness problem has not been completely addressed yet. Following that, several researchers have studied selfishness in MANETs [18–28] under various settings. In most cases, the proposed solutions to the selfishness problem focused on the detection and isolation of selfish nodes, while in others the aim was cooperation enhancement, using either credit-based or reputation-based schemes [27, 28], and a comprehensive review for these proposed solutions can be found in [29]. An interesting presentation of the proposed solutions for the problem of packet dropping in MANETs in general can be found in [30].

Another important part of research concerns methods to model selfishness. In [31] a formal description of selfishness is attempted using a game-theoretic model with static Bayesian Games, and a simple strategy to enforce packet forwarding is presented. Other studies employed evolutionary game theory modeling, like in [32], where a genetic algorithm is employed. In [33] a semi Markov process has been used to model the behavior of nodes into four types: those who cooperate, those who behave selfishly, those who are malicious and those who are defective.

Selfishness as an outcome of energy depletion was studied in [34]. In that work, each node's selfishness is defined as a function of its remaining energy, and the performance of the DSR protocol is examined, when nodes with four different selfishness-defined behaviors exist simultaneously in the network. Four types of selfishness are distinguished by three thresholds, as seen in Table 1. Following that work, SA-DSR was firstly proposed in [35] as an enhanced version of DSR that makes routing decisions by taking into account

Table 1 Selfishness type and forwarding probability

Remaining energy (%)	Selfishness type	Forwarding probability (%)
80–100	Always altruistic (AA)	100
50–80	Sometimes selfish (SS)	90
20–50	Often selfish (OS)	50
< 20	Always selfish (AS)	0

the Selfishness Type of each node in combination with a newly introduced factor called *Altruism Coefficient*. In the present work, SA-DSR is properly modified to enhance its performance.

The approach presented in [34] set the starting point for this work, taking advantage of the low overhead it produces, by using only two bits to express the Selfishness Type of each node. In addition, this work introduces a new factor called *common welfare factor* to evolve SA-DSR into SCWA-DSR, which is expected to exhibit improved performance.

3 Proposed Protocols

In this section we present the modifications applied on the structure and operations of the DSR protocol, in order to evolve it to Selfishness Aware Dynamic Source Routing (SA-DSR) and its expanded version that takes into account the common welfare factor, namely Selfishness and Common Welfare Aware Dynamic Source Routing (SCWA-DSR). We decided to use DSR protocol to test our scheme among other routing protocols for MANETs because it is one of the first proposed and more researched reactive routing protocols. Moreover, its operation is rather simple and due to its source routing nature, it is a good choice for demonstrating our scheme.

3.1 Overview of the Dynamic Source Routing Protocol

DSR is a well-known reactive routing protocol designed for use in MANETs, under the assumption that the nodes composing the network are cooperative and willing to relay messages for other nodes, regardless of their current state concerning energy or other resources.

DSR operates in two phases: the route discovery and the route maintenance phase. When a source node needs to send data to a destination node and there is no routing information for that node in its routing cache, route discovery is initiated by flooding the network with route request packets (RREQ). The route maintenance phase maintains alive the previously discovered routes that are still available. DSR protocol complete specification is very well documented in [36].

The route selection process in the original DSR protocol is based on a *shortest-path* algorithm. Although this algorithm has been proven to be efficient in wired networks, in wireless networks it might not be the best choice. The wireless medium is noisy and the nodes are constantly moving around so the topology of the network is under constant change. Hence, choosing the shortest path might not be the optimal choice, in respect to end-to-end delay or it might cause congestion problems in the network and higher packet loss rates.

3.2 Selfishness Aware Dynamic Source Routing (SA-DSR)

We apply several modifications to the original DSR structure of packets and protocol operation in order to evolve it to SA-DSR. We briefly describe our modifications, as full implementation details are out of the scope of this paper.

The most important modification we apply is in the route selection process of the route discovery phase. As mentioned earlier, the original DSR protocol employs a shortest-path algorithm to select the best route for a packet from the source node towards the destination

node. In our approach, the route selection process is replaced by an algorithm that utilizes a new metric, namely Successful Delivery Probability (SDP).

Let P_{SD} be the set of paths connecting the source node (S) and the destination node (D). For each path $p_i \in P_{SD}$, the SDP is defined as

$$SDP_{p_i} = \prod FP_{n_k}$$

where n_k is each intermediate node that belongs to the path p_i. The FP of every intermediate node n_k is computed by the FP due to the Selfishness Type (ST) combined with the FP due to the node's Altruism Coefficient (AC),

$$FP_{n_k} = (FP_{ST})_{n_k} * (FP_{AC})_{n_k}$$

The FP due to ST, FP_{ST} of each intermediate node n_k is defined at any given time as a function of its residual energy or other available resources. Actually, ST determines the percentage of the packets the node will forward or drop, as denoted in Table 1, and has thoroughly been studied in [34]. For the needs of this work, ST is simply defined as a function of each node's residual energy and the FP_{ST} is equal to the values in Table 1. AC is a new property of each node, which represents the overall satisfaction the node has received from the network until that moment. AC value is computed by the detected retransmissions of the nodes RREQ packets, or absence of them, and the timeouts that occur when no RREP packets have been received after several time a RREQ has been broadcasted. The FP due to AC, FP_{AC} is a probability between 0.0 and 1.0 that modifies the total FP of each intermediate node n_k.

The source initiates the path selection algorithm, as specified in the DSR operation, however instead of choosing the shortest path, SDP is computed for every path that connects S and D, and the path that has the higher SDP is the one that will be used. When more paths have identical SDP, the algorithm selects the one that was more recently added in the route cache. This procedure is depicted in the flow chart in Fig. 1.

Also, Route Reply (RREP) packets' structure is modified in order to add the selfishness type of the nodes. This information is included in a special additional field of the RREP packet structure, which carries ST of each intermediate node between S and D.

Using these concepts, the proposed scheme operation is the following:

- A source node S needs to send an amount of data to node D;
- Source node S checks its routing cache for previously discovered paths to destination node D;
- If there are at least two paths to D, then the path with the higher SDP is selected and data transmission starts;
- If there are no paths to D or there is only one, a RREQ is broadcasted. Nodes operate in promiscuous mode. When node S detects a retransmission of the RREQ packet from its neighbors, AC value is increased, else AC value is decreased. AC value is also decreased when no RREP is received after a specified time interval. Then, after a while, a RREQ packet is rebroadcasted, and if no path is discovered again, the packet is dropped;
- When a RREQ is received by an intermediate node R, the node can choose from two actions: it can drop it or it can forward it.
    - In order to avoid loops and to encourage the formation of disjoint paths, RREQ packets that have already been received from R are dropped.

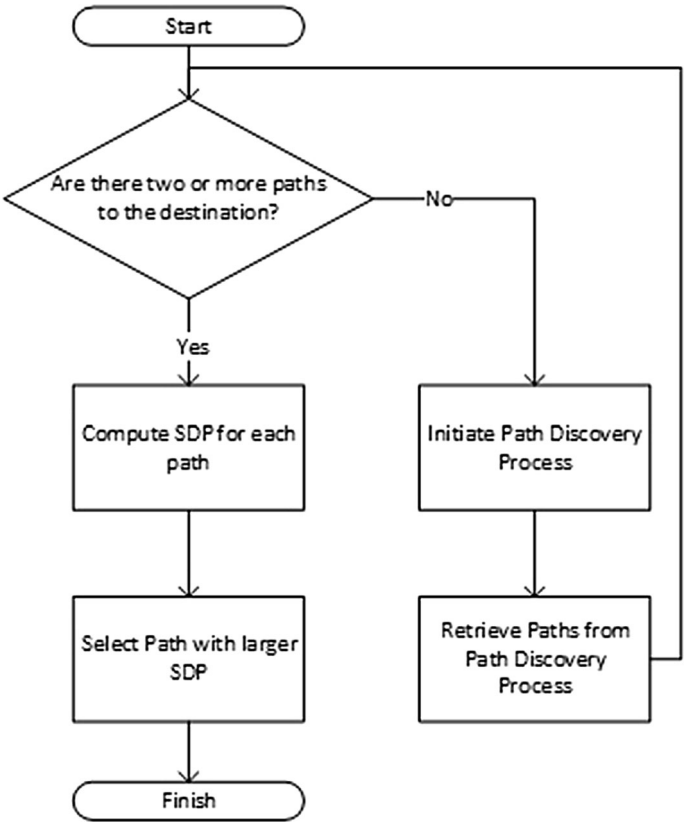

Fig. 1 Path selection flow chart

- If the RREQ packet is dropped, R conserves power but if the other neighboring nodes also choose to drop the RREQ, S's AC will be decreased and S will behave more selfishly in the future.
- If the RREQ packet is forwarded, then some energy is spent by R, but source node S—which currently is in R's neighborhood—will behave less selfishly in the future and is more probable that it will serve R's requests;

- When the RREQ packet arrives at D, a RREP packet is formed and sent back to S through the same path it arrived, as happens in the original DSR protocol.
  The RREP packet contains the path information and ST of each node. Since nodes overhear all the messages that pass through their transmission range, selfishness information for each node is available and updated if required. In DSR, when a RREQ packet is received at D a RREP packet is formed and sent. If another RREQ packet is received after that, due to following another longer or slower route, from the same S, it is dropped. In our protocol, upon reception of a RREQ a timer starts and the RREQ packets that are received before the timer expires are replied by corresponding RREP packets. Thus, many routes are formed from each node to other nodes, and the one with the highest SDP will be chosen, as needed.

3.3 Selfishness and Common Welfare Aware Dynamic Source Routing (SCWA-DSR)

To further improve the performance of SA-DSR, we introduce the common welfare factor (CWF) which we add to the SA-DSR protocol and evolve it into SCWA-DSR. CWF is promiscuously defined by overhearing the packets submitted into the network. It is actually a counter installed into each node that monitors how many RREQ, RREP, RERR and DATA packets are transmitted near the node. For each RREP and an amount of DATA packets CWF is increased, while for each RREQ and RERR it is decreased. Therefore, it provides a measure of the total traffic and the types of data and control packets exchanged between nodes at any given time, and its value is computed by:

$$CWF = k * \#RREQ + l * \#DATA - m * \#RREQ - n * \#RERR$$

where k, l, m and n are numerical constants whose values have been defined by simulation experiments.

Network traffic mainly composed of DATA and RREP packets implies good connectivity, meaning that the network operates well. On the contrary, traffic mainly composed of RREQ and RERR packets implies that the connectivity of the network has been damaged, since paths are not found to destination nodes and existing paths deteriorate. In this case, the network does not operate well and is in a critical state. When this happens, even when node's ST is Always Selfish, this state is overridden and the node forwards the RREQ packets that arrive to it in order to revive network connectivity, until CWF becomes again greater than a certain threshold.

According to the above specifications, the DSR implementation included in ns-3.24 [37] is modified using information from [38] and [39], and a simulation set is executed to investigate the performance of our proposed schemes. Ns-3 is a discrete-event network simulator targeted primarily for research and educational use. It has several modules that implement network operations in all layers from the physical to the application layer. We have also modified several other modules of ns-3 were also modified besides the DSR protocol implementation, including the energy module and the statistics framework.

4 Simulation and Performance Evaluation

In this section, the simulation configuration is presented, along with the performance evaluation of our modified protocols and the respective results.

4.1 Simulation Scenario

In Table 2 we denote the general simulation parameters used in our simulations. Simulations are averaged over 100 runs. Nodes move according to the Random Way Point Mobility Model in an open-space area of 1500 m x 500 m with a speed ranging from 0 to 2 m/s. There is a varying number of nodes in the field (i.e., 10, 20, 30, 40 or 50), which remains constant throughout the simulation duration. The transmission range of every node is 250 m. The traffic generator sends 64B packets with a rate of 4 packets/sec, to prevent congestion.

Four cases are investigated:

a. Non-modified DSR without selfishness
b. Non-modified DSR with selfishness

Table 2 Simulation configuration

Parameter	Value
Simulation time	Until the first node's energy is depleted
Simulation area	1500 m × 500 m
Number of nodes	10–20–30–40–50
Transmission range	250 m
Mobility model	Random Way Point
Node speed	0–2 m/s
Traffic generator	CBR
Packet bytes	64 bytes
Data rate	2 Mbps

c. SA-DSR with selfishness
d. SCWA-DSR with selfishness

In the case *a*, all nodes are always altruistic, so packet loss that happens is due to other reasons and not selfishness. We study this case just to obtain reference values for comparison reasons and better understanding of the acquired results. In cases *b*, *c* and *d*, the nodes' residual energy is initialized using a normal distribution. Consequently, there are some selfish nodes in the network from the start of the simulation and their number increases with time. ST is initialized for each node as a function of its residual energy. In Figs. 2 and 3 the distribution of the initial residual energy and the ST of the nodes are presented respectively, for the case of 50 nodes. Other number of nodes follow the same distribution also. As time passes by their energy gets depleted and they change their ST to more selfish behavior, as there is no recharging available. The energy consumption follows the energy model implemented in the ns3 Energy Framework Implementation [39]. In Fig. 4 the number of nodes and their behavior vs time is shown, in a run for 50 nodes case. The simulation stops when at least one node's power gets depleted. We define that time as the Network Lifetime. We take special care to properly set the seeds and the random generators in the simulator to have exactly the same start conditions and pseudo-random decisions between cases *b*, *c* and *d*.

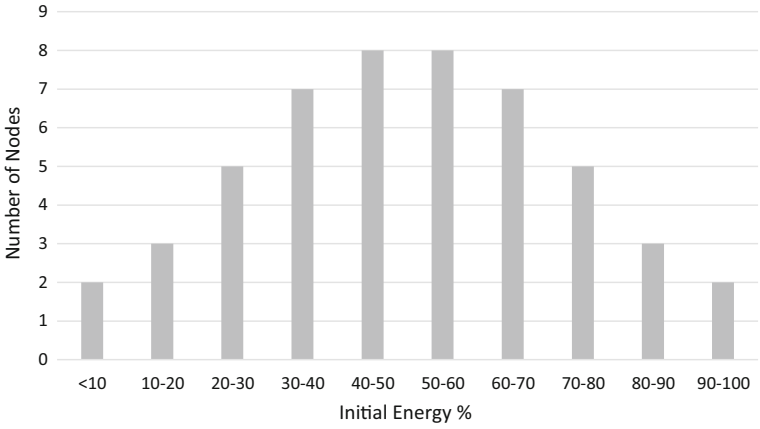

Fig. 2 Initial energy of nodes distribution

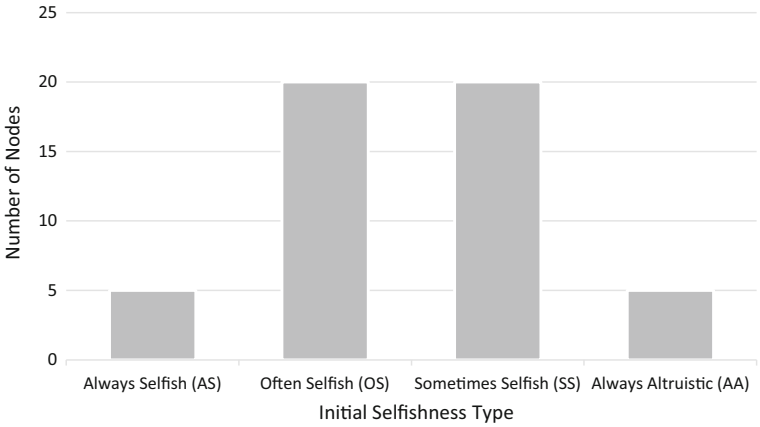

Fig. 3 Initial selfishness type of nodes distribution

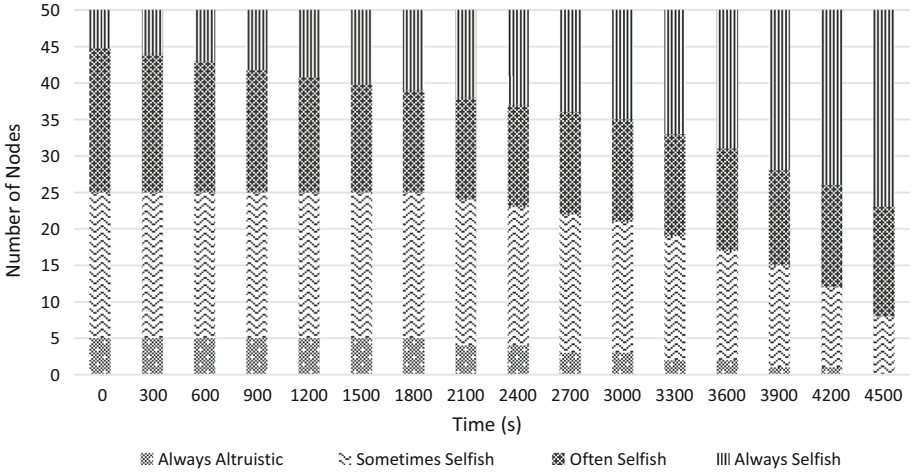

Fig. 4 Number of nodes for each selfishness type vs time

For each case, the performance of our proposed protocols is evaluated by the following metrics:

- Packet Delivery Ratio (PDR) is defined as the ratio of the total packets received to the total packets sent.
- Average end-to-end delay (AEED) is defined as the average end-to-end delay of the packets that were successfully delivered to their respective destinations.
- Normalized routing overhead (NRO) is defined as the ratio of control packets to the total packets that were received.
- Network lifetime (NL): This metric represents the total time from the beginning of the simulation until the first node's energy is depleted.

4.2 Simulation results

We execute the simulation for the four cases previously described and record the above four metrics, namely PDR, AEED, NRO and NL. The results of our simulations are presented in the figures shown below. In particular, Figs. 5, 6, 7 and 8, illustrate respectively PDR, AEED, NRO and NL, which are comparatively extracted from the simulations.

Non-modified DSR performs very well when there are no selfish nodes in the network. Altruistic nodes cooperate and forward the packets they receive, and no intentional packet drops occur. PDR is almost maximum when there are about 40 nodes in the area, and has smaller values for less nodes, due to decreased reachability and connectivity. When the density of the nodes is increased, PDR value drops due to interference. Non-modified DSR's performance dramatically drops (approximately half of the packets get delivered to their destinations) in the presence of selfish nodes. It seems that it achieves the lowest values of AEED, but this occurs due to the limited connectivity that selfish nodes bring to the network. In other words, longer paths are less common, so end-to-end delay decreases. Both our proposed schemes improve the PDR and AEED values in the presence of selfish nodes in the network.

Also, the drop rate recorded in the presence of selfish nodes is greater than the drop rate when all nodes are altruistic. Therefore, the existence of selfish nodes make NRO decrease. Using our proposed protocols, NRO values are similar to there of the non-modified DSR when selfish nodes are absent. This occurs due to more RREP packets sent back, and in some extent to the additional information (ST of nodes) that RREP packets carry.

Finally, the non-modified DSR protocol seems to deplete network resources very quickly in comparison to our proposed schemes. When there exist selfish nodes in the network they manage to maintain some of their resources for longer, even when the original DSR is in use. However, NL is significantly increased when we apply our schemes, because there is better utilization of the network resources and fairer sharing of the network traffic between nodes.

Overall, with the modifications that we made to the original DSR protocol, we managed to significantly improve all the network critical metrics.

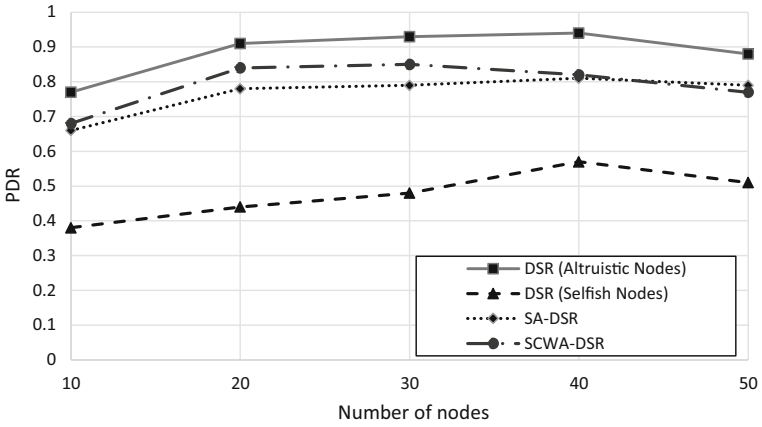

Fig. 5 Packet delivery ratio versus number of nodes

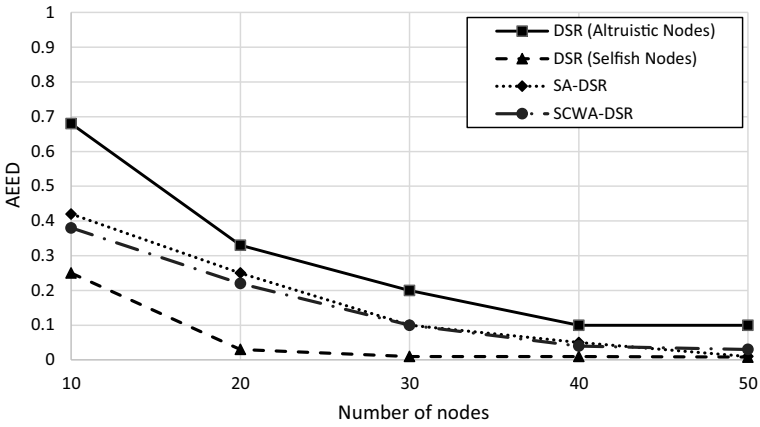

Fig. 6 Average end-to-end delay versus number of nodes

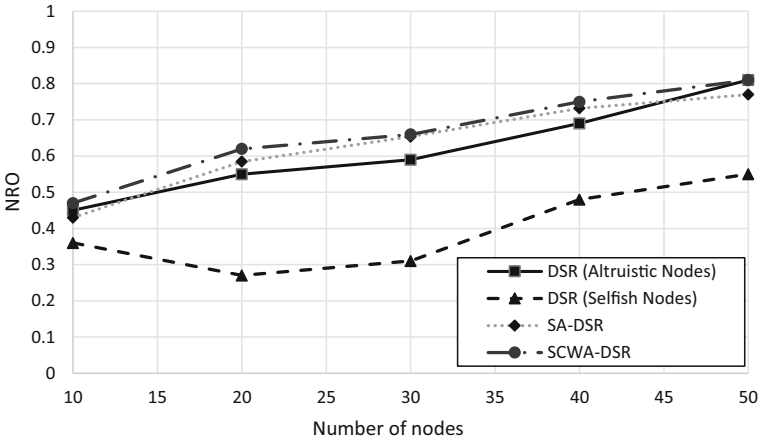

Fig. 7 Normalized routing overhead versus number of nodes

5 Conclusion and Future Work

In this work, two improved versions of the DSR protocol for MANETs are proposed by introducing Selfishness, Altruism and Common Welfare. We managed to keep NRO at low levels and improve PDR in comparison to non-modified DSR in the presence of selfish nodes.. In addition, we kept AEED close enough to non-modified DSR. Finally, the comparison between SA-DSR and SCWA-DSR reveals that the use of CWF enhances the protocol performance in respect to PDR and NL.

In the future, our scheme will be applied to other popular routing protocols, including Ad hoc On-Demand Distance Vector (AODV), several extensions will be investigated and further performance improvement is expected. We have also initiated a study that includes modelling our scheme using a game theoretic formulation. Our scheme can and will be applied to other more specific application network paradigms, such as opportunistic

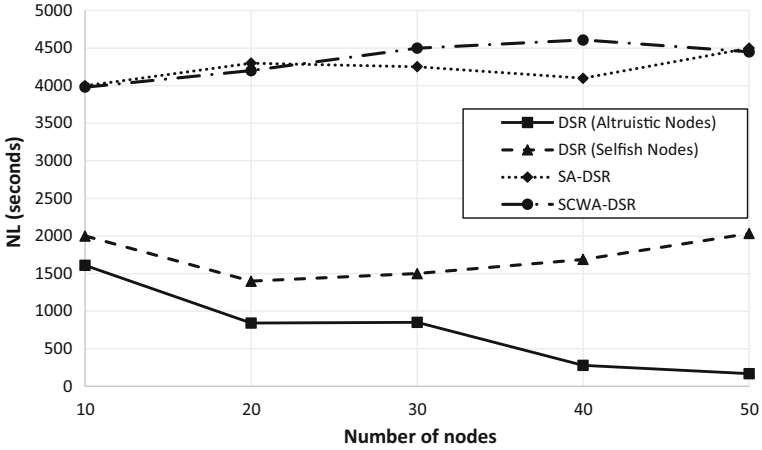

Fig. 8 Network lifetime versus number of nodes

networking, crowd-sensing applications, wireless sensor networks in environmental monitoring, etc.

References

1. Siva Ram Murthy, C., & Manoj, B. S. (2004). *Ad Hoc wireless networks: Architectures and protocols*. London: Pearson, Education.
2. Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks, 2*(1), 1–22.
3. Cai, R. J., Tan, W. C. W., & Chong, P. H. J. (2017). An overview of trust-based routing design under adversarial mobile ad hoc network environment. *Wireless Personal Communications, 96*(3), 3923–3946.
4. Kshirsagar, V. H., Kanthe, A. M., & Simunic, D. (2018). Trust based detection and elimination of packet drop attack in the mobile ad-hoc networks. *Wireless Personal Communications, 100*(2), 311–320.
5. Velloso, P. B., Laufer, R. P., Cunha, D. D. O., Duarte, O. C. M., & Pujolle, G. (2010). Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management, 7*(3), 172–185.
6. Sivakami, R., & Nawaz, G. K. (2016). A radical block to byzantine attacks in mobile ad hoc networks. *Wireless Personal Communications, 87*(2), 485–497.
7. Poongodi, T., & Karthikeyan, M. (2016). Localized secure routing architecture against cooperative black hole attack in mobile ad hoc networks. *Wireless Personal Communications, 90*(2), 1039–1050.
8. Ubarhande, S. D., Doye, D. D., & Nalwade, P. S. (2017). A secure path selection scheme for mobile ad hoc network. *Wireless Personal Communications, 97*(2), 2087–2096.
9. Cho, J. H., & Chen, R. (2013). On the tradeoff between altruism and selfishness in MANET trust management. *Ad Hoc Networks, 11*(8), 2217–2234.
10. Samara, C., Karapistoli, E., & Economides, A. A. (2012). Performance comparison of MANET routing protocols based on real-life scenarios. In *2012 4th International congress on ultra-modern telecommunications and control systems and workshops (ICUMT)* (pp. 870–877). IEEE.
11. Kampitaki, D., & Economides, A. A. (2014). Simulation study of MANET routing protocols under FTP traffic. *Procedia Technology, 17,* 231–238.
12. Kaur, P., Kaur, D., & Mahajan, R. (2017). Simulation based comparative study of routing protocols under wormhole attack in manet. *Wireless Personal Communications, 96*(1), 47–63.

13. Purohit, K. C., Dimri, S. C., & Jasola, S. (2017). Performance evaluation of various MANET routing protocols for adaptability in VANET environment. *International Journal of System Assurance Engineering and Management, 8*(2), 690–702.
14. Singh, S. K., Duvvuru, R., & Singh, J. P. (2014). Performance impact of TCP and UDP on the mobility models and routing protocols in MANET. In D. Mohapatra, & S. Patnaik (Eds.), *Intelligent computing, networking, and informatics. Advances in Intelligent Systems and Computing* (Vol. 243, pp. 895–901). New Delhi: Springer.
15. Alslaim, M. N., Alaqel, H. A., & Zaghloul, S. S. (2014, April). A comparative study of MANET routing protocols. In *2014 Third international conference on e-Technologies and networks for development (ICeND)* (pp. 178–182). IEEE.
16. Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations, IETF request for comments 2501.
17. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking* (pp. 255–265). ACM.
18. Hernandez-Orallo, E., Serrat, M. D., Cano, J. C., Calafate, C. T., & Manzoni, P. (2012). Improving selfish node detection in MANETs using a collaborative watchdog. *IEEE Communications Letters, 16*(5), 642–645.
19. Subramaniyan, S., Johnson, W., & Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. *EURASIP Journal on Wireless Communications and Networking, 2014*(1), 205.
20. Kang, N., Shakshuki, E. M., & Sheltami, T. R. (2010, November). Detecting misbehaving nodes in MANETs. In *Proceedings of the 12th international conference on information integration and web-based applications & services* (pp. 216–222). ACM.
21. El-Haleem, A. M. A., Ali, I. A., Ibrahim, I. I., & El-Sawy, A. R. H. (2011). TRIDNT: Isolating Dropper nodes with some degree of Selfishness in MANET. In *International conference on computer science and information technology* (pp. 236–247). Springer, Berlin.
22. Hernandez-Orallo, E., Olmos, M. D. S., Cano, J. C., Calafate, C. T., & Manzoni, P. (2015). CoCoWa: A collaborative contact-based watchdog for detecting selfish nodes. *IEEE Transactions on Mobile Computing, 14*(6), 1162–1175.
23. Tarannum, R., & Pandey, Y. (2012, March). Detection and deletion of selfish MANET nodes-a distributed approach. In *2012 1st international conference on recent advances in information technology* (RAIT) (pp. 152–156). IEEE.
24. Das, D., Majumder, K., & Dasgupta, A. (2015). Selfish node detection and low cost data transmission in MANET using game theory. *Procedia Computer Science, 54,* 92–101.
25. Naserian, M., & Tepe, K. (2009). Game theoretic approach in routing protocol for wireless ad hoc networks. *Ad Hoc Networks, 7*(3), 569–578.
26. Djenouri, D., & Badache, N. (2009). On eliminating packet droppers in MANET: A modular solution. *Ad Hoc Networks, 7*(6), 1243–1258.
27. Menaka, R., Ranganathan, V., & Sowmya, B. (2017). Improving performance through reputation based routing protocol for manet. *Wireless Personal Communications, 94*(4), 2275–2290.
28. Sengathir, J., & Manoharan, R. (2017). Co-operation enforcing reputation-based detection techniques and frameworks for handling selfish node behaviour in MANETs: A review. *Wireless Personal Communications, 97*(3), 3427–3447.
29. Yoo, Y., & Agrawal, D. P. (2006). Why does it pay to be selfish in a MANET? *IEEE Wireless Communications, 13*(6), 87–97.
30. Djahel, S., Nait-Abdesselam, F., & Zhang, Z. (2011). Mitigating packet dropping problem in mobile ad hoc networks: Proposals and challenges. *IEEE Communications Surveys & Tutorials, 13*(4), 658–672.
31. 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).
32. Komathy, K., & Narayanasamy, P. (2007). Study of co-operation among selfish neighbors in MANET under evolutionary game theoretic model. In *International conference on signal processing, communications and networking, 2007. ICSCN'07.* (pp. 133–138). IEEE.
33. 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.
34. Kampitaki, D. G., Karapistoli, E. D., & Economides, A. A. (2014). Evaluating selfishness impact on MANETs. In *2014 international conference on telecommunications and multimedia (TEMU)*, (pp. 64–68). IEEE.

35. Kampitaki, D. G., & Economides, A. A. (2016). Novel routing protocol for mobile ad hoc networks with selfish and altruistic nodes. In *2016 International conference on telecommunications and multimedia (TEMU)* (pp. 1–5). IEEE.
36. Johnson, D., Hu, Y. C., & Maltz, D. (2007). The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4 (No. RFC 4728). Retrieved online from: https://www.ietf.org/rfc/rfc4728.txt.
37. https://www.nsnam.org/.
38. Cheng, Y., Çetinkaya, E. K., & Sterbenz, J. P. (2012, March). Dynamic source routing (DSR) protocol implementation in ns-3. In *Proceedings of the 5th international ICST conference on simulation tools and techniques (pp. 367–374)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).
39. Wu, H., Nabar, S., & Poovendran, R. (2011, March). An energy framework for the network simulator 3 (ns-3). In *Proceedings of the 4th international ICST conference on simulation tools and techniques (pp. 222–230)*. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering).

Dimitra G. Kampitaki was born in Heraklion, Crete, Greece in 1980. She received the B.S. in Electronics Engineering and M.Sc. in Information Systems in Thessaloniki, Greece in 2004 and 2008 respectively. Since 2012 she is a Ph.D Student in University of Macedonia, Thessaloniki, Greece in the field of wireless communications routing protocols. From 2004 to 2010, she was a Lab Instructor with the Department of Electronics Engineering of TEI of Thessaloniki, where she also contributed to research projects as a Research Associate. She has authored and co-authored many journal and conference papers. Her research interests include Game Theory and Optimization Methods for Wireless Communications, Routing Protocols for Wireless Networks, Wireless Sensor Networks and Environmental Monitoring Applications.

Anastasios A. Economides is a professor on Computer Networks and Telematics Applications and director of CONTA lab (http://conta.uom.gr) at the University of Macedonia, Thessaloniki, Greece. He received the Dipl. Eng. Degree in electrical engineering from Aristotle University of Thessaloniki, in 1984. Holding a Fulbright and a Greek State Fellowship, he received the M.Sc. and the Ph.D. degrees in computer engineering from the University of Southern California, Los Angeles, in 1987 and 1990, respectively. His Ph.D. thesis, A unified game-theoretic methodology for the joint load sharing, routing and congestion control problem, was the first research to formulate, model and solve routing (load balancing, load sharing) problems in computer and communication networks. He has published over two hundred (200) peer-reviewed papers. He has over 3000 citations by other researchers. He is an IEEE senior member. Finally, he has been the principal investigator of 10 funded projects and participated in 25 EU and National funded projects.