Evaluating Selfishness Impact on MANETs

Dimitra G. Kampitaki, Eirini D. Karapistoli and Anastasios A. Economides
Interdepartmental Program of Postgraduate Studies on Information Systems
University of Macedonia
Thessaloniki, 54006 Greece
{kampitaki, karapis, economid}@uom.gr

Abstract—Mobile Ad Hoc Networks (MANETs) use many different routing protocols to route data packets between nodes. These routing protocols are designed taking for granted that all nodes are cooperative and willing to forward control and data packets from and to other nodes. However, when selfish nodes exist in the network, the network performance may degrade significantly. In previous research, selfish nodes are predetermined, meaning that a node is either selfish or not from the beginning (i.e., when deployment takes place) and retains that behavior over time. However, in reality selfishness is not static, but an outcome of restricted energy. In this paper, we investigate the operation of Dynamic Source Routing (DSR) protocol, as selfish behavior emerges in a MANET due to energy depletion. We define different levels of selfishness, and we investigate the protocol performance when the nodes inside the network exhibit different levels of selfishness.

Keywords—Mobile Ad Hoc Networks; routing protocols; DSR; selfish nodes; simulation;

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) [1] are networks that have no predefined infrastructure. Many routing protocols are currently being used in routing in MANETs, and are categorized under different criteria [2]. The most general distinction of MANET routing protocols is proactive and reactive, with hybrid protocols using principles from both of these categories. Dynamic Source Routing (DSR) protocol is an on-demand or reactive routing protocol that uses flat network topologies [3].

Nodes participating in a MANET behave cooperatively obeying the routing protocol that is used. In fact, routing protocols are designed taking for granted that all nodes participating in the network are cooperative. In some cases though, nodes might deviate from that behavior causing problems to the network. There are various types of misbehavior of a MANETs nodes. Some of them occur when specific circumstances exist, while others are the outcome of security attacks. The most common cause of unintentional misbehavior is the shortage of energy resources. When a nodes battery level gets low, that node might not cooperate as expected by the routing protocol. Instead, it may save energy resources to serve its own communication needs, and to prolong its own lifetime, regardless of the common welfare of the network.

In this paper, we contribute to the area of routing for MANETs by investigating the impact of the presence of selfish nodes in the network when the DSR protocol is employed. We provide a more realistic definition of the selfish behavior distinguishing it from intentional misbehavior. We also define various types of selfish nodes and extensively examine their impact on the network by simulating several scenarios.

The rest of the paper is organized as follows. Section II provides an overview of related work as well as existing definitions of selfishness. Section III provides an overview of the simulation environment and the parameters used, and analyzes the obtained simulation results. Section IV concludes the paper with some insightful discussion and future research directions.

II. RELATED WORK

There have been several performance evaluation studies of MANET routing protocols under various scenarios [4]–[12]. In many cases, researchers compare different types of routing protocols [4]–[11] while in others, they compare protocols of the same type [12] in order to identify the best performing protocol under certain circumstances and with respect to various metrics. Other studies test the performance of routing protocols when the nodes follow different mobility models [13], [14], or even when there are obstacles in the field [15]. Other approaches to routing protocol evaluation consider heterogeneous networks and examine the network performance when nodes of different types exist [16].

The performance of routing protocols when selfish nodes exist in the network has attracted several research studies, but in all cases, selfishness is considered as a threat or an attack instead of an expected behavior of the network nodes. Thus, research focuses on detection and suppression of selfish nodes by employing watchdogs or other central or distributed authorities. These kinds of solutions are characterized as reputation-based [17]–[20]. Other approaches, characterized as credit-based, provide incentives to cooperate in the form of virtual currency [21], [22]. There are also game theoretic approaches [23]–[25] that utilize Game Theory to model and explain selfish behavior. There is a comprehensive overview of selfishness management schemes in [26].

One of the initial definitions of node misbehavior in MANETs can be found in [17]. There, a misbehaving node is one that agrees to participate in forwarding packets (/) but then indiscriminately drops all packets that are routed through it. Following that definition, the network performance is evaluated by modifying the percentage of selfish nodes in the network (out of 50 nodes). DSR is the routing protocol used. Other researchers mostly use the above definition of node misbehavior.

In [27], the nodes selfish behavior is categorized into four different types depending on the way the various control and data packets are handled. Various scenarios with varying number of selfish nodes are examined based on the Ad hoc On-demand Distance Vector (AODV) routing protocol. The same
approach is followed in every comparative simulation that is presented in [17]–[25] disregarding the cause of selfishness which is the depletion of energy resources.

In [28], a more formal approach to categorize and investigate node behavior is attempted, forming four main categories: cooperative, inactive, selfish and malicious nodes. The most important difference between selfish and malicious nodes, is that the first category of nodes do not wish to harm the network, while the second category of nodes intentionally aim to harm the network and disrupt its protocols.

In this work, we examine the performance of the DSR routing protocol considering selfishness as an expected behavior of the nodes. We define four levels of selfishness to describe selfish behavior, with each level depending on the nodes residual energy. Our simulations begin with nodes having different initial energy levels, so their expected selfishness level is different. In this way, we approach the problem of selfishness in MANETs more realistically.

III. SIMULATION SETUP AND RESULTS

In this section, we first present the simulation configuration and then analyze the obtained results. For the purposes of our analysis, we used the OMNeT++ 4.4.1 [29] with the addition of the inetmanet-2.0 framework [30]. We used the dsr-uu implementation provided by the inetmanet-2.0 framework in order to simulate the DSR protocol. Several modifications were conducted to this model mainly concerning the statistics collection. The AdhocHost node module implementation and the Battery module implementation included in inetmanet-2.0 framework are also modified to serve our needs.

A. Simulation Parameters

In Table I, the general simulation parameters are denoted. All the simulations are averaged over 10 runs. Each simulation runs until the energy of at least one node is completely depleted. The simulation area is 1500m x 500m and the nodes move inside this area following a Random Way Point mobility model with a speed ranging between 0-2m/s (low mobility scenario). The transmission range for each node is set to 250m. To avoid congestion, we use 64B packets that are sent with a rate of 4 packets/sec.

We examine four cases that are summarized in Table II. In Case A (No Selfishness), nodes act cooperatively and there is no selfish behavior. This case is used as a reference and comparison measure for better understanding.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simulation Time</td>
<td>Time until the first node’s energy runs off</td>
</tr>
<tr>
<td>Simulation Area</td>
<td>1500m x 500m</td>
</tr>
<tr>
<td>Number of Nodes</td>
<td>10-20, 30-40-50</td>
</tr>
<tr>
<td>Transmission Range</td>
<td>250m</td>
</tr>
<tr>
<td>Mobility Model</td>
<td>Random Way Point</td>
</tr>
<tr>
<td>Node Speed</td>
<td>0-2m/s</td>
</tr>
<tr>
<td>Traffic Generator</td>
<td>CBR</td>
</tr>
<tr>
<td>Packet Bytes</td>
<td>64 bytes</td>
</tr>
<tr>
<td>Data Rate</td>
<td>2 MBps</td>
</tr>
</tbody>
</table>

In case B (Constant Selfishness), we examine the impact of selfishness in a way that it has been examined in previous research studies, i.e., by specifying at the beginning of the simulation a percentage of selfish nodes. This percentage remains constant all the time and does not change according to the energy depletion of the nodes. To compare this case with the other cases, we set a 20% of the total nodes to be selfish. As stated in [17], considering 40% of the total nodes to be selfish seems unrealistic, so we selected a more realistic scenario with 20% of the total nodes to be selfish for our simulations, which is about equal to the time-averaged percentage of selfish nodes present in the network at simulation Cases C and D.

In Case C (Single Threshold Selfishness), time is considered as a new parameter. As time progresses and the nodes energy gets below a specific percentage of their nominal energy, they instantly become selfish dropping all data packets that arrive to them. This should be the case for all similar evaluations, as selfishness emerges when the residual energy levels are low. We name nodes that behave in this manner as Threshold Selfish nodes. The threshold can take any desired value depending on the nodes needs. We arbitrarily set that threshold at 20% for the purpose of our study.

Finally, in Case D (Multi-Threshold Selfishness) the nodes act more selfishly as their energy dissipates, dropping packets with some probability. We define the Residual Energy Percentag $RE\%$ as follows:

$$RE\% = \frac{\text{Residual Battery Capacity}}{\text{Nominal Battery Capacity}}$$

Then, we define four Selfishness Levels (SL) based on three energy thresholds $T_1$, $T_2$, $T_3$ where $T_1 > T_2 > T_3$, that orientate the behavior of the nodes, as follows:

$$SL = \begin{cases} 
\text{Always Altruistic (AA)}, & \text{if } RE\% \geq T_1, \\
\text{Sometimes Selfish (SS)}, & \text{if } T_2 > RE\% \geq T_3, \\
\text{Often Selfish (OS)}, & \text{if } T_2 > RE\% \geq T_3, \\
\text{Always Selfish (AS)}, & \text{if } T_3 > RE\%.
\end{cases}$$

Each Selfishness Level corresponds to a Packet Drop Probability (PDP), which is defined by the individual nodes needs, with $PDP_{AA} = 0\%$ and $PDP_{AS} = 100\%$. The $PDP_{SS}$ and $PDP_{OS}$ can take any value that suits the nodes needs, as long as $PDP_{SS} > PDP_{OS}$. In our simulation, we define the thresholds and the PDP for each SL as declared in Table II.

<table>
<thead>
<tr>
<th>Case</th>
<th>Residual Energy (%)</th>
<th>Selfishness Type</th>
<th>Packet Drop Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Not Important</td>
<td>Not Applicable</td>
<td>0%</td>
</tr>
<tr>
<td>B</td>
<td>Not Important</td>
<td>Selfish (constant number of selfish nodes)</td>
<td>100%</td>
</tr>
<tr>
<td>C</td>
<td>&lt;20</td>
<td>Selfish</td>
<td>100%</td>
</tr>
<tr>
<td></td>
<td>20-100</td>
<td>Always Altruistic (AA)</td>
<td>0%</td>
</tr>
<tr>
<td>D</td>
<td>50-80</td>
<td>Sometimes Selfish (SS)</td>
<td>10%</td>
</tr>
<tr>
<td></td>
<td>20-50</td>
<td>Often Selfish (OS)</td>
<td>50%</td>
</tr>
<tr>
<td></td>
<td>&lt;20</td>
<td>Always Selfish (AS)</td>
<td>100%</td>
</tr>
</tbody>
</table>
In order to investigate the impact of selfishness on the network performance, we used the following metrics:

1) **Average Packet Delivery Ratio (PDR):** This metric is computed by dividing the total number of packets received by destination nodes with the total number of packets sent from the source nodes.

2) **Average End-to-End Delay (AEED):** This metric is computed by averaging the end-to-end delay of all successfully delivered packets in the network.

3) **Average Normalized Routing Overhead (NRO):** This metric is computed by dividing the total control packets with the total packets received in the network.

4) **Network lifetime:** This is the lifetime of the network, until at least one node’s energy is depleted.

Additionally to the metrics that consider routing protocol performance, we also recorded the percentage of selfish nodes versus time during our simulations for better understanding of the underlying mechanisms of Single- and Multiple-Threshold Selfishness.

**B. Simulation Metrics**

As expected, the best performance for all metrics is recorded when no selfish nodes exist in the network, i.e., in Case A. The PDR is close to 100% when the nodes are 30 with less values for less nodes, due to restricted connectivity and reachability. For more nodes, the PDR drops again due to the high node density of the network that leads to more interference between the nodes.

Cases B, C and D have similar results in all metrics except for the PDR, which in Case D seems to be more affected than in the other two cases. Generally, case D, i.e. Multiple-Threshold Selfishness seems to affect all metrics more than all the other cases, so we can assume more strain is put on the routing protocol when that kind of model is used. Additionally, in Case D nodes do not become suddenly selfish, but go through multiple levels of selfishness before they become completely selfish. Therefore, this information can be passed through multiple levels of selfishness before they become completely selfish. Therefore, this information can be passed.
towards the routing protocol to be able to distinguish which nodes are going to be selfish soon and to avoid them during the routing process.

In Fig. 5 the percentage of selfish nodes over time is presented for Cases B, C and D for a representative case. In Case B the percentage of selfish nodes is constant throughout the simulation. In Case C the percentage of selfish nodes gets bigger sooner than in Case D. This happens because in Case D there are multiple levels of selfishness, which help sustain nodes with lower energy for more time.

Finally, in Fig. 6, the total number of nodes that correspond to each level of selfishness is illustrated for one representative simulation of Case D. Initially, there are no selfish nodes at all (AS), while many altruistic nodes exist (AA). In addition, nodes with SS and OS selfishness levels exist, depending on the initial energy of each node. As time progresses, the residual energy of the nodes decreases and their selfishness level increases, as defined in Eq. (2). After some time, no AA nodes remain, and solely selfish nodes of various levels of selfishness emerge. Finally, just before the simulation halts, more than 1/3 of the nodes become of AS selfishness level.

Summarizing the results, we assume that the model of Multiple-Threshold Selfishness is more appropriate for routing protocol evaluation purposes than the other two, since it highlights the increased effect of selfishness on the routing process in a more prominent way. Therefore, it can be used for performance evaluation studies of proposed selfishness suppression protocols, instead of the standard Constant Selfishness model (i.e. Case B), that is used until now.

IV. CONCLUSIONS AND FUTURE WORK

As expected, the impact of the presence of selfish nodes in a MANET is small when there are few selfish nodes present, and gets higher the more they become. When the available energy is restricted, and as time passes by, more nodes adopt selfish behavior, affecting more the network performance metrics. The most affected metric seems to be PDR followed by AEED and NRO. We proved by simulation that by defining multiple levels of selfishness we are able to extend nodes and consequently network lifetime in comparison to defining only two levels for selfishness, selfish or not selfish.

In the future, we intend to utilize the aforementioned analysis in order to design and implement a routing protocol based on DSR that will minimize the effect of the presence of selfish nodes on the network performance, concentrating our efforts to ensure high PDR and low AEED and NRO. Another interesting approach is the development of an analytical model to describe selfishness over time when battery resources are constrained.

REFERENCES


