Selfishness as a Virtue in Mobile Ad Hoc Networks

As Related to the 2013 MANIAC Challenge

Isaac Supeene
Department of Electrical and Computer Engineering
University of Alberta
Edmonton, Canada
isupeene@ualberta.ca

Asanga Udugama
Faculty of Electrical Engineering
University of Bremen
Bremen, Germany
adu@comnets.uni-bremen.de

***Abstract*—Using Mobile Ad Hoc Networks as a way to break the dependency of mobile communications on permanent infrastructure has been an active area of research for several years, but only more recently has consideration been given to the economics of a distributed mobile service. In particular, the topic of handling nodes that act selfishly or maliciously has not yet been explored in detail. In this paper, we discuss strategies for mobile offloading under the rules of the 2013 MANIAC Challenge, and then look into possible exploits of the MANIAC framework and how to address them.**

Keywords—Ad Hoc Networks; Packet Dropping Attack; Credit System; Selfish Nodes; Mobile Offloading

I. Introduction

This work developed from the perceived need to introduce a credit-based approach to Mobile Ad Hoc Networks (MANETs) [2]. A credit based system is one in which either a source or destination node must pay some sort of virtual currency to send or receive a packet, which is somehow distributed amongst the intermediate nodes for their service. Such an approach is intended to combat the problem of uncooperative nodes, which can typically be divided into three categories: selfish, malicious, and erroneous/malfunctioning [3]. Selfish nodes participate in the network only to send their own packets, and avoid contributing to the network in order to save their own resources [4]. Malicious nodes, on the other hand, are nodes which actively attempt to disrupt a network, for example by flooding the network with useless packets, or dropping all packets routed through it in a "black hole" attack [1].[1] Malfunctioning nodes are nodes which cannot participate in, or which inadvertently disrupt the operation of a MANET, due to erroneous software or hardware. The observable effects of such nodes are not believed to be qualitatively distinct from those of a malicious node, and we will therefore not consider them further in this paper [2].

The remainder of this paper is structured as follows. In the next section, we discuss how a MANET node can maximize throughput under the credit-based system which forms the basis for the 2013 MANIAC Challenge [5]. Section III discusses practical improvements that can be made to the MANIAC bidding system to avoid exploits and ensure that no node can simultaneously advantage itself while harming the MANET. In section IV, we present our conclusions and briefly discuss the open problems left by this paper.

1 Other types of maliciousness, such as actively interfering with the wireless communications channel, are not discussed here.

II. Maximizing a Node's Balance in the MANIAC Challenge

A. Victory

The MANIAC Challenge[2] victory conditions are based on two criteria: (a) the maximum balance above 0, and (b) the highest packet delivery ratio [5]. Since in the most realistic scenario, a totally selfish node is concerned only with its own balance, we will focus on criterion (a). (Note that for our purposes, we also do not consider attempting to minimize the balance of the other nodes, since this is only desirable under the artificial constraints of the Challenge itself.)

B. Maximizing Total Probabilistic Gain

A node performs two main actions to fulfill its role as a forwarding relay: acquiring packets (by bidding on packets auctioned by adjacent nodes) and forwarding packets (by holding its own auctions). Our strategy for maximizing a node's balance is based on modularizing these two components – in particular, we observe that the optimal strategy for forwarding a packet is independent of how we acquired the packet. Following this line of reasoning, we derive an equation for *total probabilistic gain* G_{tot} as follows:

$$G_{tot} = P_{bid}G_{bid} \ , \qquad (1)$$

where P_{bid} is the probability of winning a bid, and G_{bid} is the *conditional probabilistic gain*, which is the node's prediction of the balance increase it would expect, on average, from packets identical to the one in question, assuming its bid is successful. Our goal is to maximize the total probabilistic gain for each bid.

We further expand G_{bid} as follows:

$$G_{bid} = P_{succ}G_{succ} + P_{fail}G_{fail} + P_{end}G_{end}$$

2 The rules of the 2013 MANIAC Challenge are not given in this text, since the primary audience for this paper is already familiar with them. A full description of the rules can be found in [5].

Here, P_{succ}, P_{fail} and P_{end} are the probabilities of successfully delivering the packet, forwarding the packet to another node which eventually fails to deliver the packet, and being unable to forward the packet at all, respectively. These three probabilities also sum to 1, since they cover all possibilities within the rules of the framework. G_{succ}, G_{fail} and G_{end} are the gains associated with each outcome, and are simple to derive from the rules of the Challenge.

$$G_{bid} = P_{succ}(C_U - C_D) + P_{fail}(C_U - C_D - F_U + F_D) + P_{end}(C_U - F_U)$$

C_X is a cost for which a packet is delivered as the result of an auction, and F_X is the corresponding fine for that packet. The subscripts U and D stand for *upstream* and *downstream*, respectively, where *upstream* indicates that the value is associated with the auction at which the packet was acquired, and *downstream* indicates that the value is associated with the auction through which the packet will be forwarded. Lastly, we are able to factor out C_U and summarize all the other terms with a constant k (that is, a constant with respect to C_U), since we already have sufficient information to prepare our forwarding auction and estimate the necessary probabilities before we even bid on the packet.

$$G_{bid} = C_U - P_{succ}C_D + P_{fail}(F_D - F_U - C_D) - P_{end}F_U$$
$$G_{bid} = C_U + k \quad (2)$$

Thus, provided we have already set the parameters for our own auction in advance, the bidding problem is reduced to a simple maximization of $P_{bid}(C_U + k)$, where k is known, and P_{bid} is a function of C_U. The remainder of the work lies in accurately finding the relationship between P_{bid} and C_U.

The process of setting the parameters for our own auction are similar, though somewhat more complicated. Instead of manipulating one variable, C_U, we manipulate both F_D and our budget, from which we must estimate P_{succ}, P_{fail}, P_{end}, and C_D. The core of the problem is predicting the willingness and ability of other nodes to continue forwarding our packets, which is at this time left open.

It is notable (though not surprising) that G_{fail} cannot be positive. This means that bias towards minimizing P_{fail} is one of this equation's properties. Though a detailed explanation is out of the scope of this paper, we assert that in computing these probabilities, we will have computed the probability of success for each possible forwarding node. Thus, our selection procedure for packet-forwarding will take into account these probabilities, and tend to avoid uncooperative nodes, once their unwillingness to forward packets has been established.

III. Vulnerabilities of the MANIAC Framework

In principle, a credit-based system for forwarding packets is an excellent way to solve the problem of selfishness, and – to varying degrees – certain types of maliciousness [2]. However, such a system risks opening up new possibilities for maliciousness by taking advantage of the framework itself. In this section, we will address an issue with the MANIAC framework which we call the "black hole exploit" [1].

Above, we noted that in (2), G_{fail} cannot be positive. Unfortunately we cannot make the same claim for G_{end}. In other words, given two nodes A and B, it is possible in principle, for node B to bid for packets at a price higher than the fine set by A for that packet, and then simply drop them, at a net profit. This exploit is a direct result of the restriction that the fine in any auction be lower than that auction's budget [5].

This in and of itself is relatively harmless. Since we consider the probability of each node successfully forwarding our packet, A will quickly realize that B is a black hole, and will either start preferring other nodes, or stop sending packets altogether, if B is his only connection to the MANET. In either case, B is reduced to a passive observer after only having stolen virtual pocket change. However, in the case where B is A's only connection to the MANET, a much more dangerous exploit is possible, which we call the "partial black hole exploit". Simply, B forwards just enough of A's packets that A will continue to trust B, and drops the rest, forcing A to resend those packets (once again paying B for his "service"). Thus, B is providing minimal throughput to A, but at a premium price.

This is fortunately a simple exploit to address: one simply allows the fine to be greater than the budget. However, this seems to open up yet another exploit. Suppose node A sends a packet through node B. Seems harmless – but now suppose the packet goes from B to C, who is in cahoots with A and drops the packet. Assuming the fine and budget remain proportional to each other, A's gain will be greater than C's loss, and the pair will have successfully scammed B.

The important distinction to make is that in the first scenario, if B is A's only connection to the MANET, A's only options are to give the packet to B, or simply not send anything. In the second scenario, B has no obligation to send A's packet through C, and even if A and C are his only connections to the MANET, he can simply decline to accept A's packet to begin with. Furthermore, since B is in control of the fine imposed on C, our assumption about the constant proportionality of fine and budget may not hold. This is still not an ideal situation, but it is in our opinion an improvement over the first scenario, and serves to demonstrate that creating a scam-proof system is not a trivial problem.

IV. Conclusion

Mobile Ad Hoc Networks (MANETS) rely strongly on cooperation between nodes due to their distributed nature, which naturally makes them highly vulnerable to the effects of selfish and malicious nodes. This can be controlled by a credit-based system, but only to the extent that the system itself does not open further opportunities for exploitation.

In this paper, we have seen how the MANIAC framework permits a node to act entirely in its own interest, while still contributing positively to the package delivery rate of the MANET. We have also demonstrated some of the limitations of the MANIAC framework, and explored the difficulties of preventing the framework from introducing new exploits. The open questions which remain are (a) how to accurately predict the probability of a package successfully reaching its destination when forwarded to a particular node, and (b) how to eliminate the type of maliciousness which takes advantage of the rules of the framework itself. These questions will form the basis of our future research in this area.

REFERENCES

[1] S. Djahel, F. Naït-abdesselam, and Z. Zhang , "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges," IEEE Communications Surveys & Tutorials, vol. 13, no. 4, fourth quarter 2011 , pp. 658–672

[2] S. Zhong, J. Chen , and Y. R. Yang , "Sprite: a simple, cheat-proof credit-based system for mobile ad hoc networks," IEEE INFOCOM 2003

[3] M. Schütte , "Detecting selfish and malicious nodes in MANETs," Seminar: Sicherheit in Selbstorganisierenden Netzen, HPI/Universität Potsdam, Sommersemester 2006 .

[4] K. Balakrishnan, J. Deng , and P. K. Varshney , "TWOACK: preventing selfishness in mobile ad hoc networks," Wireless Communications and Networking Conference, 2005 IEEE (Volume: 4) .

[5] MANIAC 2013 Challenge, http://2013.maniacchallenge.org/