A Node Control Model for the Charging and Accounting Problem in MANETs

Inna Kofman
University of Duesseldorf
Department of Computer Science
Duesseldorf, Germany
Email: kofman@cs.uni-duesseldorf.de
innavm@hotmail.com

Uyen Trang Nguyen, Hoang Lan Nguyen
York University
Department of Computer Science and Engineering
Toronto, Canada
Email: (utn, lan)@cse.yorku.ca

***Abstract*—Because of the lack of infrastructure in mobile ad hoc networks (MANETs), their proper functioning must rely on co-operations among mobile nodes. However, mobile nodes tend to save their own resources and might be reluctant to forward packets for other nodes. In this paper, we address the charging and accounting problems in MANETs. We develop a theoretical game model that offer advice to a central authority about the allocation of resources for monitoring mobile nodes. The solution provides the optimal monitoring probability, which discourages nodes from cheating because the gain would be compensated by the penalty. The solution is then extended to accommodate realistic assumptions such as finite punishments and imperfect monitoring. The effectiveness and usefulness of the deployment of monitoring mobile agents were confirmed by simulation results.**

***Index Terms*—Mobile ad-hoc networks, cooperation, security, game theory, inspection game.**

I. Introduction

Mobile ad hoc networks (MANETs) [5] are networks that consist of mobile nodes with limited transmission ranges. In order to allow communication beyond this range, nodes have to forward data on behalf of other nodes. Since a node that forwards packets sent by others spends its own resources, such as battery power, it needs to have a reason to do so. One approach to encourage node cooperation is to use a charging and accounting scheme to pay the owner of the device an amount of money for each forwarded data packet [12]. This can be implemented by allowing the sender to insert a set of coins into a packet to be sent. Every node that forwards the packet is allowed to extract one coin for the job done. A forwarding node can collect coins and redeem for a reward later.

When monetary rewards are involved, dishonest nodes may cheat to gain more than they deserve. For example, a node may take two coins for forwarding a packet instead of the allowed amount of one coin. A sender may re-use coins that were already spent on a previously sent packet. These are deemed cheating or illegal actions.

To prevent cheating, existing schemes use strong cryptography [13] [22] [27] [7] [23] [9] [24] [16] [17] [15] (which is time and power consuming for energy-constrained mobile devices), and/or tamper-proof devices [4] [14] [25] [23] [26] (which require modifications to existing devices and increased cost to device owners/buyers).

In [12] a new approach to the charging and accounting problem in MANETs was presented. Node behaviours are monitored by police nodes (PNs), and misbehaving nodes are penalized for their illegal actions, possibly with monetary punishments. The deployment, management and maintenance of PNs impose extra costs to the network owner or central authority, which should be covered by the fines collected from cheating nodes. The objective of the work presented in this paper is to advice the central authority on how much resource to allocate to network monitoring so that the cost incurred does not exceed the amount of fines collected from misbehaving nodes.

We consider this problem as an inspection game [2] between PNs (the inspectors) that represent the central authority and are trusted parties in the system and regular nodes (the inspectees). Our proposed mathematical model is based on the Passenger Ticket Control (PTC) model [1] originally proposed for the Munich Transport and Fares Tariff association (MVV). The purpose of the PTC model is to suggest how to find the optimum frequency of control through which the MVV could monitor passengers in a cost-effective manner. In this paper, we adapt the PTC model to develop a game model for the charging and accounting scheme proposed in [12]. Our proposed game model is based on a Nash equilibrium that offers a strategy for allocating PNs. We demonstrate that this strategy will discourage nodes from cheating since they will not benefit from such illegal acts.

The remainder of this paper is organized as follows. In the next section, we review the Passenger Ticket Control Model [1]. Section III summarizes the charging and accounting scheme discussed in [12]. In Section IV, we present a game model based on the PTC model and the charging and accounting scheme presented in [12]. Section V provides extensions to the proposed model using more relaxed assumptions. In Section VI, we present simulation results to illustrate the effectiveness and usefulness of PNs in monitoring network traffic. We conclude the paper and discuss future work in Section VII.

II. The Passenger Ticket Control Model

The Passenger Ticket Control Model (PTC) is presented in [1] as an example of the application of inspection games. This is a two-player game problem in which the control system is an inspector (first player) and the passenger is an inspectee (second player). The purpose of this mathematical model is to give advice to the MVV on how to make the deployment of distributed randomly inspectors economically attractive.

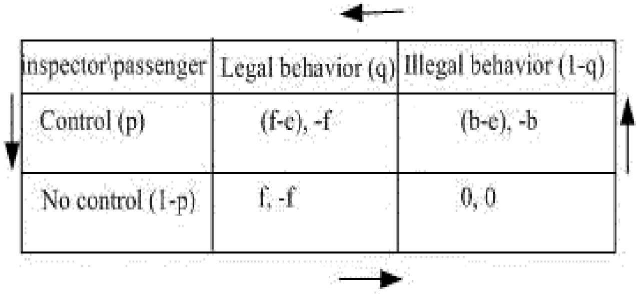
If f denotes the normal passenger fare, b denotes the fine, and e denotes the cost of control per passenger ($e < b$), then the possible payoffs (x, y) for an inspector and a passenger respectively are:

$(x, y) = (f - e, -f)$: inspectors control the system and passengers act legally
$(x, y) = (f, -f)$: inspectors do not control the system and passengers act legally
$(x, y) = (b - e, -b)$: inspectors control the system and passengers act illegally
$(x, y) = (0, 0)$: inspector do not control the system and passengers act illegally

The above payoffs are summarized in Figure 1 where the inspector controls the system with probability p, and the passenger behaves legally with probability q.

According to the game model [1], the expected payments of the inspector and the passenger, denoted by E_1 and E_2 respectively, are as follows:

$$E_1(p, q) = (f - e)pq + (b - e)p(1 - q) + f(1 - p)q$$
$$E_2(p, q) = -fpq - bp(1 - q) - f(1 - p)q$$



inspector\passenger	Legal behavior (q)	Illegal behavior (1-q)
Control (p)	(f-e), -f	(b-e), -b
No control (1-p)	f, -f	0, 0

Figure 1. The PTC game model.

Fig. 1.

To enable the MVV to perform the desirable control management, an optimum strategy of inspecting is developed using a Nash equilibrium concept [18]. There is no pure strategy equilibrium because of the cyclical preferences of the players (see the directions of the arrows in Figure 1). The pair of mixed strategy equilibrium (p^*, q^*) is comprised of the two players' strategies, where p^* is the inspector's "best response" (optimal monitoring probability) to the passenger's choice of q^* (optimal probability of behaving legally), and q^* is the passenger's "best response" to the inspector's choice of p^*.

The equilibrium payoff of the inspector is E_1^*, and that of the passenger is E_2^*. Solving the Nash equilibrium [18] we obtain:

$$p^* = \frac{f}{b}, \qquad E_1^* = f(1 - \frac{e}{b}), \qquad (1)$$
$$q^* = 1 - \frac{e}{b}, \qquad E_2^* = -f. \qquad (2)$$

In the case of a passenger's illegal conduct with a probability of $(1 - q^*) > 0$, his expected payoff, on the average, remains the same; i.e., the gain from free-riding is balanced by the imposed fine.

When the passenger chooses q^* as his strategy, the costs of inspectors, which check passengers (with any p) and collect funds in the form of fines imposed on free-riders, are ultimately compensated by the collected fines. Indeed, if ep denotes the mean costs of the inspectors controlling the system per passenger, and if $bp(1-q)$ is the profit from the collected fines, then

$$ep - bp(1 - q) = p(e - b(1 - q^*)) = 0.$$

Choosing p^* by the MVV for optimum control makes the passenger indifferent in choosing his strategy. Choosing the legal behavior strategy, the passenger pays $-f$, which is equal to the expected payoff $-bp^*$ of the passenger that chooses to behave illegally (see Eq. (1)).

III. A Charging and Accounting Scheme for MANETs

In [12], a novel and yet simple approach of combining a cooperation mechanism and a monitoring system to solve the charging and accounting problem in MANETs is proposed. The incentive for cooperation is provided by means of remuneration and it does not require to equip each node with the temper proof/resistant devices. A sender S that wants to transmit a message to a destination D estimates the number of hops h on the path from S to D. The message is encrypted by the public key of a destination to provide end-to-end message confidentiality. S then purchases h coins and insert them into the packet to be sent. Every intermediate node that forwards the packet is allowed to extract one coin from the packet as the payment for the forwarding job. Nodes collect coins and later submit to the central authority (CA) to redeem rewards.

To prevent cheating (e.g., a node extracting more than one coin from the packet for a one-hop forwarding), a number of police nodes are distributed throughout the network randomly, which observe nodes' behaviours with respect to charging and accounting, document their behaviours and report the information to the CA periodically (when they have a fast connection). A PNs can be as mobile or static agents. For their distribution the existing urban infrastructure could be used that evenly covers an area. For example, PN devices could be set up on buses roofs, police cars, gas stations, traffic lights. Also, they can be set up on crowded public buildings, like exhibition halls, a university campus. The CA uses the information reported by the PNs to reward cooperating nodes as well as identify cheating nodes and impose fines. In the following, we present some examples of how common attacks could be detected by the PNs:

- Double use of coins. A node puts the same coin in two distinct packets. After a PN reports collected data, the CA can discover this after it verifies whether all coins preloaded into the packet are valid (i.e., coins were purchased by the node and were not yet used).
- Illegal action. An intermediate node takes more than one coin from the packet. A PN can notice this when checking whether the set of incoming coins is identical to the outgoing set (except for one coin that was taken by the node and the next node identifier).
- Double coin submission. An intermediate node takes one coin (as is expected) and just copies another one of the remaining coins in the packet, and then submits both. The node will be considered as a cheater if a PN has observed that the copied coin was taken by another node.

The collected fines will be used to pay for the cost of deploying and managing PNs. The theoretical game model proposed in this paper aims at providing the CA with a strategy for allocating PNs that will discourage nodes from cheating since they will not benefit from such actions.

The charging and accounting scheme in [12] is based on the following assumptions:

1) Nodes are rational. That is, nodes will only cheat or act illegally if the average gain of cheating is more than the average loss caused by punishments.
2) The penalty for misbehaving nodes is infinite (e.g., cheating nodes are expelled from the network), whereas the gain from cheating is said to be finite. Considering this assumption and the assumption that nodes are rational, it follows that there is no reason for rational nodes to behave dishonestly since the average loss is greater than the average gain derived from cheating. Therefore, nodes will not cheat if they run any risk of being caught, i.e., there is a small probability that any illegal action will be detected. In this paper, we show that the correctness of the proposed scheme is not affected when the infinite punishment is replaced by more realistic punishments. We provide an optimal strategy to the CA, thereby leading to the nodes' indifference about whether or not to act illegally.
3) The information reported by the PNs to the CA is accurate and error-free. This is not realistic in a real network. We relax this assumption and extend the game model to adapt the relaxation in Section V.

IV. The Proposed Game Model for Node Control

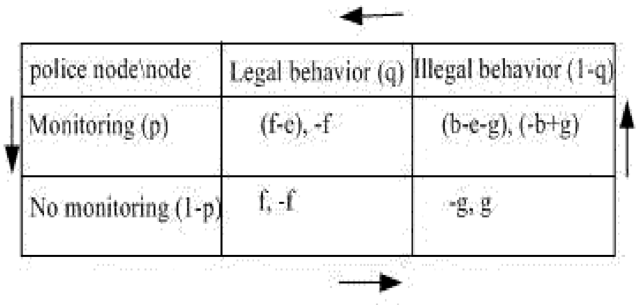
Like the PTC problem, we consider the monitoring problem of the charging and accounting scheme described in Section III to be a two-player inspection game in which a PN (representing the CA) plays the role of an inspector and a regular node is an inspectee. The PN (the first player) monitors node behaviours in the network whereas the regular node (the second player) may or may not cheat.

Monitoring of nodes in our system has a character similar to the inspection of passengers in the PTC problem. During monitoring at a certain location, a police node may observe a number of nodes which are in its reception range, similar to a number of passengers in a public transportation vehicle that are being inspected.

A solution to the problem we consider is a game solution using a Nash equilibrium, as in the PTC problem. Let f denote the average expenditure of a node when it acts legally; g, the nodes average gain from illegal actions; b denotes the penalty for a misbehaving node; and e, the cost of monitoring per node (including a deployment cost) [1] ($e < b$). Then the game can be presented in the normal form as shown in Figure 2, where $(p, 1-p)$ is the mixed strategy of the first player (the probability assigned to monitoring/no monitoring), and $(q, 1-q)$ is the mixed strategy of the second player (the probability assigned to legal/illegal behaviours).

According to the game model, the expected payments E_1 and E_2 of the PN and the regular node, respectively, are as follows:

$$E_1(p,q) = (f-e)pq + (b-e-g)p(1-q) + f(1-p)q - g(1-p)(1-q)$$
$$E_2(p,q) = -fpq + (g-b)p(1-q) - f(1-p)q + g(1-p)(1-q)$$



police node\node	Legal behavior (q)	Illegal behavior (1-q)
Monitoring (p)	(f-e), -f	(b-e-g), (-b+g)
No monitoring (1-p)	f, -f	-g, g

Figure 2. The nodes control game in Ad Hoc Networks.

Fig. 2.

Like the PTC problem, the game has no pure strategy equilibrium because of the cyclical preferences of the players. Let (p^*, q^*) be the mixed strategy equilibrium of the two players, as defined in Section II. Then the resulting mixed strategy Nash equilibrium is:

$$p^* = \frac{f+g}{b}, \qquad (3)$$
$$q^* = 1 - \frac{e}{b}. \qquad (4)$$

The obtained optimal control probability p^* makes the node indifferent about his two possible action choices, based on the same explanation given in the PTC model in Section II. In fact, equation (3) holds when probability p^* is chosen for monitoring. Indeed a node which behaves legally pays $-f$, on the one hand, and pays $-bp^* + g$ when it behaves illegally, on the other.

As previously mentioned in the PTC model, the expenditure outlay for control is compensated by the penalty collected when a node chooses q^*. In fact, the difference between the expenditure for monitoring per node (ep) and the gain from the penalty ($bp(1-q)$) is zero for any p only if the node chooses q^*.

The equilibrium expected payoffs E_1^* and E_2^* of the PN and the regular node respectively, given the mixed strategy pair (p^*, q^*), are:

$$E_1^*(p^*, q^*) = f(1 - \frac{e}{b}) - \frac{eg}{b},$$
$$E_2^*(p^*, q^*) = -f.$$

The expected payoff of the regular node given its mixed strategy $(1-q^*) > 0$ remains the same. Thus we can draw the same conclusion as in the case of the PTC model: the payoff of a legally behaving node is the same as that of a node that behaves illegally and whose illegally achieved gain is negated by the imposed penalty.

V. Solution Extensions

The charging and accounting scheme [12] for which the above game model is developed assumes infinite penalty and error-free monitoring results (see Section III). These assumptions are not applicable in real networks. Therefore we relax the assumptions and extend the game model to adapt the relaxation.

A. Optimal Penalty

The desired deterrence effect in the system could be achieved by the trade-off between frequency of monitoring and severity of punishment, when the CA may change both the probability of control p and the punishment b periodically. As is usual in economics and legal literature, in order to determine a punishment as severe as possible, under the assumption that individuals are risk neutral (e.g., [20], [6]), we choose the optimal punishment as the maximal one, i.e the punishment should be as high as possible. An alternative is to

[1] Additional costs/gains are not taken into account, since they do not affect players directly.

increase the punishment in order to save on monitoring costs [6].

B. Imperfect Monitoring

In real ad-hoc networks, a PN may observe, collect, or report inaccurate information to the CA (e.g., due to interference, receiving errors, etc). As a result of possible errors, an honest node could be mistakenly penalized – let us assume that this happens with probability ϵ_C – and an offender could be mistakenly exonerated – let us assume that this happens with probability ϵ_A. Moreover, it could become attractive for nodes to act illegally if the gain derived from cheating minus the fine is greater than the loss caused by a false accusation [20], i.e.,:

$$\begin{aligned} &g - p(1-\epsilon_A)b > -p\epsilon_C b \Leftrightarrow \\ &g > (1-\epsilon_A-\epsilon_C)pb \Leftrightarrow \\ &p < \tfrac{g}{(1-\epsilon_A-\epsilon_C)b} \end{aligned} \qquad (5)$$

Thus, the monitoring probability p, must satisfy the following inequality[2] to discourage nodes from cheating:

$$p \geq \tfrac{g}{(1-\epsilon_A-\epsilon_C)b} \qquad (6)$$

The deterrence decreases due to both false exoneration and false accusation (see the right-hand side of (5)) and could be improved by increasing the frequency of monitoring [20]. Besides increasing deterrence, the additional cost of monitoring would decrease the probability of penalizing the node falsely, thereby decreasing the node's disinclination to cooperate, which may then be advantageous to the CA [19].

The objective of the following analysis is to estimate a node's behaviour when both errors and the social welfare are taken into account. Since both false exoneration and false accusation decrease the deterrent factor, the social welfare is also decreased [20]. Once again, a node will cheat if and only if $g \geq pb$. The social welfare is represented by[3] [6], [19]:

$$\textstyle\int_{pb}^{\infty}(g-m)z(g)dg - r(p),$$

where m denotes the expected harm to the society[4]; $z(g)$ is a density function of gains; and $r(p)$ denotes a function that shows the amount of resources required to achieve probability p ($r' > 0, r'' \geq 0$). The first-order condition to find the optimal detection probability is:

$$(m-pb)(Z'(pb)) = r'(p), \qquad (7)$$

where $Z'()$ is the cumulative distribution function of $z()$. From (7) it follows that:

$$m > pb, \qquad (8)$$

which means that the expected punishment (see the right-hand side of inequality (8)) is less than the value of the harm (left-hand side of inequality (8)) which is incurred by the society due to the node's cheating. In other words, some ”under-deterrence” is optimal ([6], [19]). After substituting (6) for p into (8), we get:

$$m > \tfrac{g}{1-\epsilon_A-\epsilon_C}. \qquad (9)$$

From (9) we can see that the right-hand side is increased in $(1-\epsilon_A-\epsilon_C)$. If g is increased to the point of $m \leq g$, then it will be beneficial for a node to behave illegally [20]. Thus, as long as (9) is satisfied, a node will have no incentive to cheat. Also, the percentage of erroneous monitoring is, at most, identical to the percentage of interference/errors.

VI. Experimental Results

It may be argued that the monitoring capabilities of PNs are not the same those of human inspectors in a transportation system, and mobile nodes and human passengers have different characteristics. Therefore, we carried out simulations to ascertain the capability of PNs in monitoring network traffic. Our objective is to verify that the deployed PNs are capable of observing the majority of network traffic. Note that the observation rate does not have to be 100% because the primary purpose of the proposed monitoring scheme is not to punish cheaters, but to encourage cooperation and deter cheating.

A. Simulation Environment and Parameters

We used the GloMoSim Network Simulator [8], developed at the University of California at Los Angeles (UCLA), for our simulations. It provides a graphical environment for scalable simulation and prototyping of wireless network systems and protocols.

[2] It is assumed that $(1-\epsilon_A) > \epsilon_C$ [19].

[3] This is the conventional social welfare function that is used in legal and economics literature [6], [19].

[4] “expected” because it is not always possible to estimate the exact value of harm [19]

Routing protocol	DSR
MAC protocol	CSMA/CA with RTS/CTS/DATA/ACK
Terrain size	1200 m x 800 m
Number of nodes	30
Simulation time	900 seconds per experiment
Propagation model	Two-ray [21]
Transmission range	272 m
Channel capacity	2 Mbps
Mobility model	Random way-point [10]
Data traffic	CBR
Payload size	512 bytes
Confidence interval	95%

TABLE I
SIMULATION PARAMETERS SETTINGS.

We simulated a mobile ad-hoc network that consists of 30 regular mobile nodes randomly distributed in an area of size 1200 m X 800 m. Nodes use the DSR routing protocol [11] and IEEE 802.11 medium access control protocol to transmit and forward packets. The transmission range of mobile nodes is 272 m. Node mobility follows the random way-point model. Intervals between transmissions of successive packets are based on a CBR traffic generator and chosen randomly from 0.005 s, 0.01 s and 0.015 s. The size of each packet, excluding the header, is 512 bytes.

In our simulations, the PNs have the same technical characteristics as regular mobile nodes, and are distributed evenly in the network. We also assume that all nodes in the network, regular and police nodes, have an unlimited queue size in order to avoid packet losses due to congestion so that we can obtain accurate observation rates of PNs. (There were still packet losses caused by channel errors and collisions, but these loss rates were small.)

Each data point in the graphs is the average of 10 runs (experiments). In each of those experiments, the PNs were relocated, but still distributed evenly in the network. The duration of each experiment is 900 seconds in simulated time. The graphs were plotted with a confidence interval of 95%. The common simulation parameters are summarized in Table I.

B. Performance Metric and Simulation Scenarios

In each experiment, we first measured the total number of packets T transmitted in the network. T included both the original packets transmitted by the sources, as well as the copies forwarded by intermediate nodes. Every regular node i maintained a counter t_i, which was incremented every time the node transmits a packet. At the end of an experiment, we took the sum of the counters t_i of all regular nodes. We also measured the total number of packets R observed (overheard) by the PNs. Every PN j maintained a counter r_j, which was incremented every time the node observed (overheard) a packet transmitted by a regular node, the packet was not damaged, and it was not recorded by another PN. That is, if a packet was observed by several PNs simultaneously then only one observation was included in the result. At the end of an experiment, we took the sum of the counters r_j of all PNs.

The performance metric is the average *packet observation rate* $POR = R/T$.

We conducted three sets of simulations by varying the following parameters:

1) the number of PNs, which are 4, 6, 8, 10 and 12 nodes (equivalent to 13% to 40% of the network population).
2) node mobility speed, which ranges from 0 m/s to 20 m/s (equivalent to 0 m/h to 72 km/h).
3) the average sending rate of the sources, which varies from 2.06 packets/s to 10.3 packets/s.

Following are the results of the three sets of simulations.

C. Simulation Results and Discussions

1) Varying the number of PNs: In the first experiment, we varied the number of PNs in the range of 4, 6, 8, 10 and 12, equivalent to 13% to 40% of the network population. The mobility speed of mobile nodes ranged from 0 m/s to 1 m/s, and the average transmission rate of the sources was 2.06 packet/s.

Fig. 3 shows the results of this set of experiments. As the number of PNs increases, the POR also increases accordingly, from about 80% to 98%. When the number of PNs is 20% of the network population, the POR is 92%. That is, with a reasonable amount of resources (6 PNs), the CA can observe a majority of network traffic to enforce the rules. The CA can achieve an optimal monitoring probability (p^*) by taking into account parameters f, b and g in Eq. (3).

2) Varying node mobility speed: In the second experiment, node mobility speed increased from 0 m/s to 20 m/s, equivalent to 0 m/h to 72 km/h. There were 6 PNs monitoring the network and the average transmission rate of the sources was 2.06 packet/s.

The result in Fig. 4 shows that the average POR varied between 88% and 92%. If we take into account the confidence intervals, we can see that node mobility

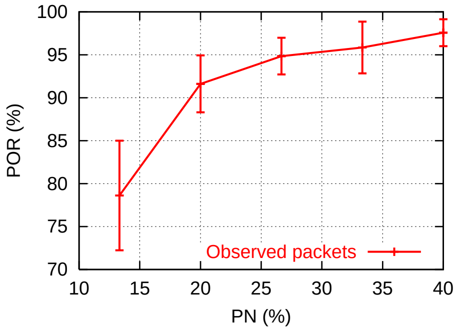


Fig. 3. Varying the number of PNs

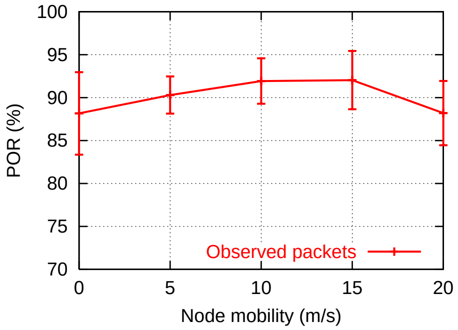


Fig. 4. Varying node mobility speed

speeds do not have much impact on the POR of the PNs. As the mobility speed increases, the POR goes up slightly, because as nodes move, more of them will get close to the PNs (since the PNs are distributed evenly in the network), increasing the observation rate. However, if the mobility speed is too high, the connection between a regular node and a PN may be broken before the PN has a chance to overhear a packet sent by the regular node. That explains the lower POR when the mobility speed is 20 m/s.

3) Varying the average sending rate of the sources: In the third experiment, we varied the average sending rate taken over all sources in the range of 2.06 packet/s, 4.12 packet/s, 6.18 packet/s, 8.21 packet/s and 10.30 packet/s. The number of PNs in the system was 6 (20% of the population) and the mobility speed was from 0 m/s to 1 m/s. The results in Fig. 5 indicate that the POR of the PNs is not impacted much by the network traffic load, varying between 92% and 94%. That shows the effectiveness of the PNs in monitoring network traffic. To further confirm this fact, we also measured the total number of packets R observed (overheard) by the PNs. The graph in Fig. 6 shows that the total number of

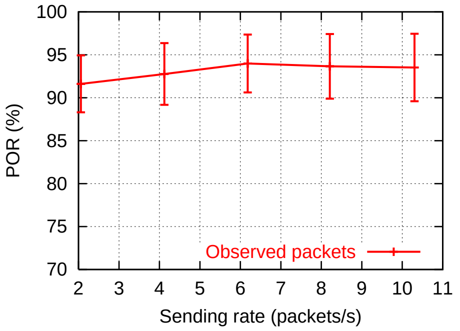


Fig. 5. Varying the average sending rate of the sources; POR result

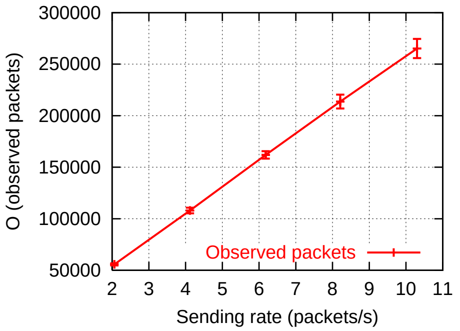


Fig. 6. Varying the average sending rate of the sources; total number of observed packets

packets R observed by the PNs increases linearly as the network traffic load increases. The result asserts the effectiveness of network monitoring by the PNs.

Finally, it is worth noting that the average POR of the PNs depend on the packet delivery ratios of the flows, which in turn depend on the routing algorithm [3]. In our future work, we will investigate the performance of the PNs with different routing algorithms (e.g., DSR vs. AODV [3]).

VII. Conclusion and Future Work

We present a theoretical game model that offers advice to the central authority about the allocation of resources for node monitoring in a charging and accounting scheme [12]. The solution provides the optimal monitoring probability, which discourages nodes from cheating because the gain would be compensated by the penalty. The solution is then extended to accommodate realistic assumptions such as finite punishments and imperfect monitoring. We confirm the effectiveness and usefulness of the proposed monitoring scheme via simulation results.

In our future work, we will investigate methods to optimally distribute police nodes in a network. In addition, non-monetary punishment schemes will be studied, as well as a combination of both kinds of penalties. We will implement the full algorithm of the proposed charging and accounting scheme and evaluate its performance under various network conditions and different routing algorithms. We will also measure the network performance in terms of packet delivery ratio, throughput, and end-to-end delay in the presence of the charging and accounting algorithm to evaluate the overheads of the algorithm when being deployed in a real network.

ACKNOWLEDGMENT

We are grateful to Professor Shmuel Zamir for his general comments on the game theory segments in this paper. Also, we would like to thank to Dr. Shifra Hochberg for her editorial assistance.

REFERENCES

[1] R. Avenhaus. Applications of inspection games. *Mathematical Modelling and Analysis, 9(3):179 192*, 2004.

[2] R. Avenhaus, B. von Stengel, and S. Zamir. Inspection games. *In R.J. Aumann and S. Hart (Eds.), Handbook of Game Theory, Volume 3, North-Holland, Amsterdam, 1947 - 1987*, 2000.

[3] S. Baraković, S. Kasapović, and J. Baraković. Comparison of MANET Routing Protocols in Different Traffic and Mobility Models. *Telfor Journal*, 2(1):8–10, 2010.

[4] L. Buttyán and J.-P. Hubaux. Enforcing service availability in mobile ad-hoc WANs. In *MobiHoc 2000*, pages 87–96, 2000.

[5] I. Chlamtac, M. Conti, and J. J. Liu. Mobile ad hoc networking: Imperatives and challenges. *IEEE Networks*, 1(1), 2003.

[6] N. Garoupa. Optimal Magnitude and Probability of Fines. In *European Economic Review*, pages 45:1765–1771, 2001.

[7] J. Herrera-Joancomarti and H. Rifa. A Forwarding Spurring Protocol for Multihop Ad Hoc Networks (FURIES). *Lecture Notes in Computer Science, 4712*, pages 281–293, 2007.

[8] M. J. GloMoSim. Global mobile information systems simulation library. In *UCLA Parallel Computing Laboratory*, Available at: http://pcl.cs.ucla.edu/projects/glomosim/, 2001.

[9] M. Jakobsson, J.-P. Hubaux, and L. Buttyán. A Micro-Payment Scheme Encouraging Collaboration in Multi-Hop Cellular Networks. *In Proceedings of International Financial Cryptography Conference. Gosier, Guadeloupe*, January, 2003.

[10] D. Johnson and D. Maltz. Dynamic Source Routing in Ad Hoc Wireless Networks. *Mobile Computing, Kluwer Academic Publishers., Norwell, MA*, pages 153–181, 1996.

[11] D. B. Johnson, D. A. Maltz, and Y.-C. Hu. The dynamic source routing protocol for mobile ad hoc networks (dsr). In *In Proceedings of the 12th Workshop on Parallel and Distributed Simulations– PADS '98*, April 2003.

[12] I. Kofman and M. Mauve. Light-Weight Charging and Accounting in Mobile Ad-Hoc-Networks. *ACM SIGMOBILE MobiCom 2005 Poster Session*, Cologne, Germany, September 2005.

[13] B. Lamparter, K. Paul, and D. Westhoff. Charging support for ad hoc stub networks. *Elsevier Journal of Computer Communications, 26(13):1504–1514*, August, 2003.

[14] L.Buttyán and J.-P. Hubaux. Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks. In *ACM Mobile Networks & Applications, 8(5)*, 2003.

[15] M. Mahmoud and X. Shen. RISE: Receipt-Free Cooperation Incentive Scheme for Multihop Wireless Networks. In *Proc. IEEE ICC'11*, Kyoto, Japan, June 5 - 9 2011.

[16] M. Mahmoud and X. Shen. DSC: Cooperation Incentive Mechanism for Multi-Hop Cellular Networks. *Proc. of IEEE ICC09, Dresden, Germany*, June 14–18, 2009.

[17] M. E. Mahmoud and X. Shen. Secure Cooperation Incentive Scheme with Limited Use of Public Key Cryptography for Multi-Hop Wireless Network. In *GLOBECOM'2010*, pages 1–5, 2010.

[18] J. Nash. Noncooperative games. *Annals of Mathematics, 54(2), 286-295*, 1951.

[19] A. M. Polinsky and S. Shavell. The Theory of Public Enforcement of Law. *HANDBOOK OF LAW AND ECONOMICS, A. Mitchell Polinsky, Steven Shavell, eds., Available at SSRN: http://ssrn.com/abstract=850264*, 1, 2006.

[20] A. M. Polinsky and S. Shavell. Public Enforcement of Law. *Stanford Law and Economics Olin Working Paper No. 322. Available at SSRN: http://ssrn.com/abstract=901512*, May 2006.

[21] T. S. Rappaport and L. B. Milstein. Effects of Radio Propagation Path Loss on DS-CDMA Cellular Frequency Reuse Efficiency for the Reverse Channel. *IEEE Transactions on Vehicular Technology*, 41 (3), 1992.

[22] B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks. In *Proceedings of ACM International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)*, Annapolis, MD, USA, 2003.

[23] N. B. Salem, L. Buttyán, J.-P. Hubaux, and M. Jakobsson. Node cooperation in hybrid ad hoc networks. *IEEE Transactions on Mobile Computing*, 5(4):365–376, 2006.

[24] H. Tewari and D. OḾahony. Multiparty micropayments for ad-hoc networks. *In IEEE Wireless Communications and Networking Conference, WCNC03, New Orleans, Louisiana, USA*, 2003.

[25] A. Weyland and T. Braun. Cooperation and Accounting Strategy for Multi-hop Cellular Networks. In *Proceedings of IEEE Workshop on Local and Metropolitan Area Networks (LANMAN 2004)*, pages 193–198, Mill Valley, CA, USA, 2004.

[26] Y. Zhang, W. Lou, W. Liu, and Y. Fang. A secure incentive protocol for mobile ad hoc networks. *Wireless Networks (WINET)*, 13, issue 5, October, 2007.

[27] S. Zhong, J. Chen, and Y. R. Yang. Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. In *Proceedings of IEEE INFOCOM*, San Francisco, CA, USA, March-April 2003.