DESIGN AND OPTIMIZATION OF REPUTATION MECHANISMS FOR CENTRALIZED CLUSTERED AD HOC NETWORKS

Spyridon Vassilaras, Dimitrios Vogiatzis and Gregory S. Yovanof
Athens Information Technology, Markopoulo Ave., PO. Box 68, 190 02, Peania, Athens, Greece, e-mail: {svas, dvog, gyov}@ait.edu.gr

Abstract: In this paper, we present and analyze a reputation scheme aiming at reinforcing node cooperation in clustered Mobile Ad hoc Networks with centralized control. The main goal of this scheme is to differentiate between intentional misbehavior and apparent failure to cooperate due to wireless channel conditions or mobility. To this end, a statistical decision method based on the notion of a random walk is employed. Selecting the optimal parameters for this random walk is investigated in the context of time dependent events. Special care has been given to issues such as probability of detection of a misbehaving mobile node, probability of falsely accusing a legitimate node due to non-intentional failures to cooperate and fast detection of misbehaving nodes in the light of time varying behavior of such nodes.

Key words: Ad hoc networks, MANETs, Cooperation Enforcement, Misbehavior Detection, Reputation Mechanism, Random Walk.

1. INTRODUCTION

The correct execution of network functions in *Mobile Ad hoc Networks* (MANETs) relies on the cooperation of the individual nodes that constitute the network. Malicious *Mobile Nodes* (MNs) that intentionally fail to execute their part of a network protocol in order to cause damage and selfish MNs that do not cooperate in order to save precious resources (such as battery power) can severely disrupt proper network operation. Thus

providing incentive mechanisms that will convince selfish MNs to cooperate and detection mechanisms that will identify malicious MNs and isolate them from the network is a critical issue, which has received considerable attention recently from the research community ([1]-[10]).

In the literature of node cooperation enforcement, the proposed solutions can be subdivided into two main categories: *trade based* schemes and *reputation based* schemes (see [1] for a more rigorous taxonomy of incentive schemes). In trade based schemes, a node that provides some service to a peer node (e.g., packet forwarding) is rewarded by either another immediate service in exchange or some monetary token that he can later use to buy services from another node (e.g., [2]-[4]). In reputation based schemes each node keeps a reputation metric for other nodes he deals with and provides services only to nodes that exhibit good reputation (e.g., [5]-[10]).

In all reputation based mechanisms for cooperation enforcement, each node in the network performs two distinct functions: rating the behavior of neighboring nodes and using these ratings to adjust his own behavior towards them. Rating the conformance of neighboring nodes to a given network protocol is an operation that depends on the specific protocol and network architecture. For instance, in single channel MANETs rating the packet forwarding service provided by a node's neighbors is simply performed through monitoring of the common channel. However, in clustered MANETs which use different channels in each cluster and bridge nodes to relay packets between clusters (such as Bluetooth scatternets) a node cannot receive the transmissions of all of his neighbors. Hence, a different technique for rating the forwarding services provided by them is needed. Similarly, rating the conformance to a neighborhood discovery protocol or a Medium Access protocol is fundamentally different than rating packet forwarding.

On the other hand, a cooperation reinforcing reputation mechanism can be easily adapted to use such behavior ratings independently of the rated service. A crucial task for this mechanism is to distinguish between perceived and actual non-cooperative behavior. For example, a MN might receive a bad cooperation rating because of wireless link failure or mobility. Misbehaving MNs might also choose to misbehave in a probabilistic way in order to evade detection. If erroneously perceived misbehavior is permitted with a certain probability, then detecting intentional misbehavior boils down to an estimation problem.

In this paper, we are investigating reputation mechanisms that use cooperation ratings to identify malicious and selfish MNs in a special kind of MANETs: Clustered mobile Ad hoc networks which operate under the coordination and supervision of a central entity. The problem of estimating the probability with which a MN misbehaves is analyzed for both time

dependent and independent non-cooperative behavior. The design goal is to maximize the probability of detection of misbehaving MNs while keeping the probability of falsely accusing legitimate MNs to a minimum.

The rest of the paper is organized as follows: In Section 2, a brief description of the Centralized Clustered Ad hoc network architecture is provided. In Section 3, we develop a general framework for detecting non-cooperative behavior and introduce a reputation scheme for distinguishing between erroneously perceived misbehavior and malicious or selfish behavior of mobile nodes. Finally, Conclusions are presented in Section 4.

2. CENTRALIZED CLUSTERED MOBILE AD HOC NETWORKS

Current user needs and modern multimedia network applications require high bit rates for data transfer. Existing WLAN technologies though, like IEEE 802.11 or HIPERLAN/2 (HL/2) cannot always meet these high data rate requirements due to the nature of the wireless channel. A typical case describing this situation is in hotspot areas, where a large number of users with high traffic needs are in the transmission range of each other. To increase the total capacity of such networks, a clustered mobile ad hoc architecture can be used. In such a setting, a specific set of MNs that are closely located and want to exchange data, are organized into a cluster. Each cluster operates in a different frequency channel to avoid interference with neighboring clusters. Through the use of power control, MNs limit their transmissions to a shorter range. Thus the network is capable of accommodating more users within the same area and transmissions inside a cluster can achieve higher bit rates. Communication between MNs that belong to different clusters is achieved with the help of *Forwarding Nodes* (FNs). FNs are MNs which belong simultaneously to two adjacent clusters and serve as bridges to forward data packets among them. A FN is able to communicate in both communication channels, but at any given time he is only capable of being tuned in one of the two clusters.

The decisions about cluster formation, including assigning FNs, are made by a central entity, commonly known as the *Access Point (AP)* or *Central Controller (CC)*. Thus, the AP assumes the role of the coordinator of the system, having under its supervision the MNs of all clusters. In order to discriminate between pure Ad hoc clustered networks, from this point on we will be referring to this type of networks as Centralized Clustered Mobile Ad hoc Networks. A typical example of such type of systems is the *Centralized Ad hoc Network Architecture (CANA)* (see [11], [12] for more details). Other

network architectures that uses centralized control to assist in Ad hoc network formation are described in [13] and [14]. Under this schemes, heterogeneous Ad hoc networks are formed under the central supervision of a cellular network infrastructure. All the above architectures assume that the central authority can communicate control information directly to the MNs via wireless links. Hence the need of creating an Ad hoc network is not generated by the fact that the MNs are outside of the transmission range of the AP; multihop communication is employed in order to achieve higher capacity and centralized control helps in the network set-up and operation.

MN mobility and changing communication needs dictate a dynamic cluster formation algorithm. Network topology information is gathered by the AP during a *Neighborhood Discovery (ND)* operation, which is performed repeatedly in certain time intervals, in order to adapt to dynamic network conditions. ND takes place in a predefined channel where all MNs exchange messages at a shorter transmission range, in order to identify their one hop neighbors. When a broadcast *'NextND Phase'* message sent by the AP is received by the MNs, they all enter the ND phase and send *'hello messages'* in specific time slots assigned by the AP (so that collisions do not occur). Then each MN sends to the AP a *Neighbors list,* each row of which is filled with the source MAC address of a 'hello message' it has received and the quality of reception (link status). Based on input from all MNs, the AP then decides on the exact cluster topology and communicates it to the MNs.

3. REPUTATION BASED COOPERATION REINFORCEMENT

The AP is considered to be a trusted entity, adopting thus the role of the security manager in the network. In fact the AP is believed to be the only trusted device in the network; all the MNs may constantly or occasionally misbehave, drop packets, misroute data packets, try to mislead the AP regarding the network topology, etc.

The key mechanism for addressing these issues is a node reputation mechanism implemented by the AP. The goal of this mechanism is to keep track of misbehaving MNs so that they can be isolated from the network and penalized appropriately. In order to distinguish between perceived (e.g., due to wireless link failure or mobility) and actual non-cooperative behavior, the AP can observe each MN for a large period of time and compare their behavior to the expected behavior of a well-behaving node. One common way of keeping track of a MN's long term behavior is by assigning to it a reputation metric which will be reduced if the node is suspected to have

misbehaved and increased otherwise. A set of such reputation metrics can be maintained for each MN, to track different kinds of misbehavior. If one of these metrics falls below a given threshold, the node is considered misbehaving. This way, not only nodes that exhibit consistent misbehavior, but also nodes that misbehave with a certain probability will get detected. Although this scheme is popular in the literature ([5], [6], [10]), it has not been, to the best of our knowledge, analyzed quantitatively. In the remainder of this paper we model the evolution of a reputation metric in time as a random walk process and investigate appropriate selection of this random walk's parameters.

3.1 The reputation metric as a random walk process

Let as denote by $r_i^j(k)$ the value of the i-th reputation metric of the j-th MN at time k. All metrics should be initialized at some positive value a_i, i.e. $r_i^j(0) = a_i > 0, \quad \forall i, j$. Time is considered to be discrete and independent for each reputation metric; for each event that can contribute positively or negatively to the reputation metric r_i^j, its associated k is increased by one. Therefore after the k-th 'event' we have:

$r_i^j(k) = r_i^j(k-1) + \Delta r_i^j(k)$ with:

- $\Delta r_i^j(k) = -1$, if a suspicious event occurs and
- $\Delta r_i^j(k) = b_i$, otherwise.

If the i-th reputation metric of a node becomes smaller than or equal to 0, this node is considered to have performed a type-i protocol attack. Clearly, each random process $\{r_i^j(k)\}$ is a random walk in which the event of a node getting accused for misbehavior is a threshold crossing event [15]. For a well-behaving node, we expect suspicious events (also known as false positives) of different types to occur in a variety of time patterns; false positives of a certain type might be i.i.d., whereas false positives of another type might exhibit strong time dependencies.

Let us first consider the case where false positives are i.i.d. with probability P_{loss}. Then $\{r_i^j(k)\}$ for a well-behaving node is a random walk with i.i.d. steps. Assuming that we can estimate P_{loss} with a reasonable accuracy[1] we want to set the parameters of the random walk in such a way that the threshold crossing probability (i.e., the probability of wrongly accusing a well behaving node) does not exceed a very small value P_{wrong}. A logical choice for the value of b_i is:

[1] In any case, a conservative estimate of P_{loss} can be used instead, e.g., the upper end of a 99% confidence interval.

$$b_i = \frac{P_{loss}}{1 - P_{loss}} \quad (1)$$

which results in a zero drift random walk by making the mean value of the per step change in the reputation metric equal to 0. It is well known that a zero drift random walk with infinite horizon will eventually cross any finite threshold with probability 1. To avoid this, we can select an appropriate window size n, and update the reputation metric for k>n, as follows:

$$r_i^j(k) = r_i^j(k-1) + \Delta r_i^j(k) - \Delta r_i^j(k-n)$$

An upper bound to the threshold crossing probability for a random walk in a finite horizon is given by (see [15]):

$$P_{good}(r_i^j(k) \le 0) \le \exp[n\gamma(\theta^*) - \theta^* \cdot a_i] \quad (2)$$

where θ^* is the minimizing θ in $\min_{\theta \ge 0}[n\gamma(\theta) - \theta \cdot a_i]$, $\gamma(\theta) = \ln E[\exp(-\theta \cdot \Delta r_i^j(k))]$ and a_i the initial value of r_i^j.

3.2 Dealing with time dependent suspicious events

In the case of time dependent suspicious events there exist generalizations of Eq. 2 for several classes of random processes. A simple case is when the time dependence of false positives can be modeled as a Markov chain process with two states (state 0 corresponds to a suspicious event and state 1 to normal operation) and transition probability matrix $\mathbf{P} = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix}$.

Then, $\{r_i^j(k)\}$ is a Markov modulated random walk in which the upper bound to the 0 crossing probability in a finite horizon n is given by Eq. 2 with (see [15]):

$$\gamma(\theta) = \ln \rho\left(\begin{bmatrix} p_{00}e^{\theta} & p_{01}e^{-b_2\theta} \\ p_{10}e^{\theta} & p_{11}e^{-b_2\theta} \end{bmatrix}\right)$$

where $\rho(A)$ denotes the largest eigenvalue of matrix A.

In order to illustrate the applicability of these theoretical results, we provide the following example: Assume that the transition probability matrix

for the false positives process has been estimated to be $P=\begin{bmatrix} 0.6 & 0.4 \\ 0.005 & 0.995 \end{bmatrix}$ and the marginal probability of a well behaving node to be in the apparent misbehavior state $p_0 \approx 1.23 \cdot 10^{-2}$. For zero mean increments we set $b_i = \frac{p_0}{1-p_0} = 0.0125$. Then requiring the upper bound in Eq. 2 to be equal to $P_{wrong} = 10^{-3}$, we calculated the values of a_i for window sizes of n=1,000, 5,000 and 25,000 respectively. Using these parameters, we ran simulations to estimate the actual probability of ruin of a well behaving node in a time period of length n. The results are shown in Table 1. They show that in all three cases the actual probability of ruin is indeed lower than its theoretical upper bound (by an order of magnitude). At this point we should stress the obvious fact that the cumulative probability of ruin in a growing number of successive sliding windows tends to 1 for any value of P_{wrong}. For example, the cumulative probabilities of ruin, for the above mentioned window sizes and random walk parameters, in a total time period of 100,000 events were estimated experimentally and the results are given in Table 1.

Table 1. Actual probabilities of ruin of a well behaving node for different window sizes and constant P_{wrong}

N	1,000	5,000	25,000
a_i	39.09	71.61	144.65
P_{ruin} prior to n	$9.9 \cdot 10^{-5}$	$1.2 \cdot 10^{-4}$	$1.4 \cdot 10^{-4}$
P_{ruin} prior to 100,000	$4.6 \cdot 10^{-2}$	$1.5 \cdot 10^{-2}$	$2.5 \cdot 10^{-3}$

Table 2. Actual probabilities of ruin of a well behaving node for different window sizes and constant P_{wrong}/n

N	1,000	5,000	25,000
P_{wrong}	10^{-5}	$5 \cdot 10^{-5}$	$2.5 \cdot 10^{-4}$
a_i	55.24	88.76	159.76
P_{ruin} prior to n	$8.4 \cdot 10^{-7}$	$5.4 \cdot 10^{-6}$	$3.5 \cdot 10^{-5}$
P_{ruin} prior to 100,000	$4.6 \cdot 10^{-4}$	$6.6 \cdot 10^{-4}$	$7.5 \cdot 10^{-4}$

An alternative empirical approach to selecting the parameter a_i for different values of n would be to fix the ratio P_{wrong}/n aiming at approximately equal cumulative probabilities over a longer period of time. By requiring $P_{wrong}/n = 10^{-8}$ and repeating the same procedure as above, we obtained the results shown in Table 2. Note that all probabilities of ruin prior

to n are smaller than the respective P_{wrong} and that all probabilities of ruin prior to 100,000 are smaller than $100{,}000 \cdot P_{wrong}/n = 10^{-3}$.

Then, using the parameters shown in Table 1 (for fixed P_{wrong} over different n), we calculated the probability of ruin of a malicious node which misbehaves with probability P_{mal} (and independently of previous behavior) when in state 1. The results are plotted in Figure 1. We observe that as the window size increases, a malicious node gets detected with probability approaching 1 for lower values of P_{mal} when P_{wrong} is kept constant. This is a direct result of the fact that the accuracy of any estimation (and our ability to make estimation based decisions) improves as the sample size increases.

On the other hand, if a well behaving node suddenly turns malicious and misbehaves with a relatively high P_{mal} (so that the probability of ruin is close to 1 for two window sizes $n_1 < n_2$) this change in behavior will most probably get detected sooner if the sliding window with the smaller size is used. Take for example the case where $P = \begin{bmatrix} 0.7538 & 0.2462 \\ 0.0538 & 0.9462 \end{bmatrix}$, $p_0 = 0.1793$, $P_{wrong} = 10^{-2}$, and a malicious node exhibits $P_{mal} = 0.02$ for $t \le 1200$ and $t > 3000$ and $P_{mal} = 0.2$ for $1200 < t \le 3000$. In Figure 2 we plot the probability of this node getting detected in a sliding window of size n as time progresses for different values of n. It can be seen that a sliding window of a smaller size reacts faster to this sudden change of behavior.

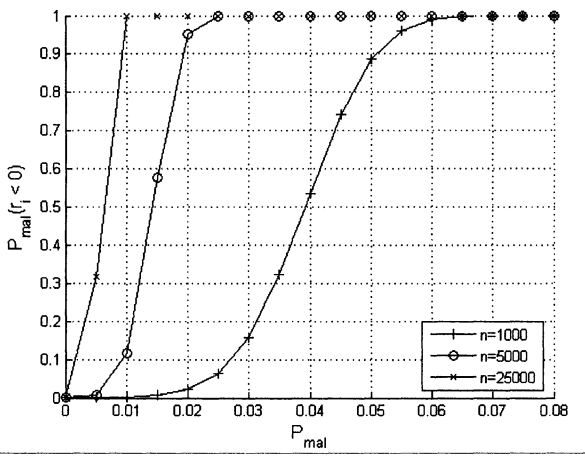

Figure 1. Probability of a malicious node getting detected as a function of his misbehavior probability, for n=1,000, 5,000 and 25,000

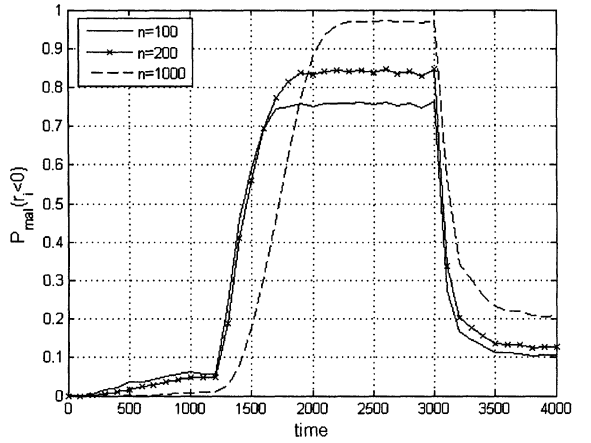

Figure 2. Probability of a malicious node with changing behavior getting detected for different window sizes

4. CONCLUSIONS

In this paper, we have investigated a cooperation enforcement scheme based on scalar reputation metrics and performed a quantitative analysis on methods for selecting step sizes and threshold values. We have treated the evolution of the reputation metric over time as a stochastic process. Both time dependent and independent stochastic models have been considered and the results have been evaluated with simulation experiments. Our work has shed some new light into the issue of detecting malicious behavior with certain probability while keeping the probability of wrongfully accusing a well behaving node below a given upper bound. We have also studied the effect of using different window sizes for the detection of malicious behavior. The trade-off between detecting nodes that misbehave with lower probabilities but reacting more slowly to changes in the behavior as the window size increases has been illustrated.

Although our cooperation reinforcement mechanism has been designed for clustered Ad hoc networks with centralized supervision, the issue of appropriately selecting the parameters of a reputation scheme (initial value/ruin threshold, step value and sliding window size) is not different

regardless of this scheme being distributed or centralized. Thus, the introduced random walk model for the reputation metric and the associated parameter selection technique can be applied to distributed reputation mechanisms for pure Ad-hoc networks, as well.

5. REFERENCES

[1] P. Obreiter, J. Nimis, "A Taxonomy of Incentive Patterns - the Design Space of Incentives for Cooperation", Technical Report Nr. 2003-9, May 21, 2003, http://www.ipd.uka.de/DIANE/en/index.html

[2] L. Buttyan, J.P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks", ACM/Kluwer Mobile Networks and Applications, Vol. 8, No. 5, October 2003

[3] N. Salem, et al., "A Charging and Rewarding Scheme for Packet Forwarding in Multi-hop Cellular Networks", MobiHoc'03, June 2003, Annapolis, Maryland, USA

[4] S. Zhong, J. Chen, and R. Yang, "Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad-hoc Networks," In IEEE INFOCOM, San Francisco, USA, 2002. IEEE Press.

[5] S. Marti, et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. ACM Int'l Conf. Mobile Computing & Networking, Mobicom 2000

[6] S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad hoc Networks," Research Report cs.NI/0307012, Stanford University, 2003.

[7] P. Michiardi, R. Molva , "Analysis of Coalition Formation and Cooperation Strategies in Mobile Ad hoc Networks", Ad-hoc Networks Journal (Special Issue), Elsevier, 2003

[8] S. Buchegger, J. Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes - Fairness In Dynamic Ad-hoc NeTworks)", Proceedings of MobiHoc 2002, Lausanne, June 2002, pp. 226-236.

[9] S. Buchegger, J.Y. Le Boudec, "The effect of rumor spreading in reputation systems for mobile ad-hoc networks," In WiOpt'03: Modeling and Optimization in Mobile Ad Hoc and Wireless Networks (2003).

[10] H. Miranda and L. Rodrigues. "Preventing Selfishness in Open Mobile Ad Hoc Networks," .In Proceedings of the International Workshop on Mobile Distributed Computing (MDC), pages 440–445, Providence, Rhode Island USA, May 2003. IEEE. (Proceedings the 23rd International Conference on Distributed Computing Systems Workshops).

[11] K. Oikonomou, A. Vaios, S. Simoens, P. Pellati, I. Stavrakakis, "A Centralized Ad-Hoc Network Architecture (CANA) Based on Enhanced HiperLAN/2," 14th IEEE PIMRC 2003, Beijing, China, September 7-10, 2003.

[12] S. Vassilaras, D. Vogiatzis, T. Dimitriou, G. Yovanof, "*Security Considerations for the Centralized Ad-Hoc Network Architecture*", IEEE Int'l Workshop on Ad-Hoc Networks (IWWAN'04), Oulu, Finland, June 2004.

[13] M. Danzeisen, et al., "Heterogeneous Network Establishment Assisted by Cellular Operators", 5th IFIP TC6 Int'l Conference on Mobile and Wireless Communication Networks, Singapore, October 2003.

[14] B. Bhargava et al. "Integrating Heterogeneous Wireless Technologies: A Cellular Aided Mobile Ad Hoc Network (CAMA)," Mobile Networks and Applications 9, 393–408, 2004 Kluwer Academic Publishers.

[15] R.G.Gallager, "Discrete Stochastic Processes", Kluwer Academic Publishers.