Misbehavior Detection in the Internet of Things: A Network-Coding-aware Statistical Approach

Angelos Antonopoulos and Christos Verikoukis
Telecommunications Technological Centre of Catalonia (CTTC)
Castelldefels, Barcelona, Spain
Email: {aantonopoulos, cveri}@cttc.es

***Abstract*—In the Internet of Things (IoT) context, the massive proliferation of wireless devices implies dense networks that require cooperation for the multihop transmission of the sensor data to central units. The altruistic user behavior and the isolation of malicious users are fundamental requirements for the proper operation of any cooperative network. However, the introduction of new communication techniques that improve the cooperative performance (e.g., network coding) hinders the application of traditional schemes on malicious users detection, which are mainly based on packet overhearing. In this paper, we introduce a nonparametric statistical approach, based on the Kruskal-Wallis method, for the detection of user misbehavior in network coding scenarios. The proposed method is shown to effectively handle attacks in the network, even when malicious users adopt a smart probabilistic misbehavior.**

***Index Terms*—Security, misbehavior, packet forwarding, cooperative communications, RLNC.**

I. Introduction

The introduction of the Internet of Things (IoT) concept implies an explosive growth in the number of wireless devices. As a result of the network densification, in IoT scenarios, cooperative communication constitutes an intrinsic network mechanism, whose functional operation relies on the active participation of various intermediaries (relays) that forward the data to the final destination. However, this collaboration should not be taken for granted, as it requires valuable energy and capacity resources from the relays, especially in wireless networks, where the radio resources are limited and the nodes are typically battery-powered devices. In addition, these networks are more susceptible to security attacks by malicious adversaries due to the broadcast nature of the wireless medium.

In this context, the design of security-oriented solutions for the network protection against selfish and malicious users has become of utmost importance, motivating several research works that can be classified in two main categories [1]: i) *proactive* mechanisms [2] that base their operation on the development of a network of trust, either by providing the participating nodes with incentives to cooperate or building reputation tables that ensure the exclusion of the misbehaving users, and ii) *reactive* mechanisms [3]–[5], which adopt a real-time approach, as the wireless nodes monitor the network activity by overhearing the transmissions or employing special control packets for the end-to-end communication.

The simplicity and scalability of the reactive techniques have made them ideal candidates for security provision in current networks, whose topology is particularly volatile, with several opportunistic users participating in the network according to their temporary location and needs. However, these mechanisms suffer from increased power consumption and packet overhead, while the introduction of network coding [6] is an additional prohibitive factor for their application in current large-scale networks. More specifically, the network coded packets complicate further the network monitoring, since they are linear combinations of single packets and no longer easily tractable by conventional schemes. In addition, the explicit packet acknowledgements have been replaced by cumulative reports [7], which verify the reception of several packets and also identify the portion of information that the node has received by each relay.

The introduction of these new control packets raises a fundamental question: *How reliable are these reports?* More specifically, two types of fake reporting have been identified [2]: *i) under-reporting*, where a node (type U) acknowledges a portion of information lower than the actually received, and *ii) over-reporting*, where a node (type O) acknowledges a portion of information higher than the actually received. By trusting these reports, in the former case, a well-behaved relay can be characterized as "bad" or "selfish", while, in the latter case, a relay node that does not participate in the packet forwarding can be characterized as "good" or "cooperative". Apparently, in IoT large-scale networks the problem is escalated with the massive existence of devices that generate a plethora of reports, stressing the need for new methods for the effective detection of malicious users.

In this paper, we introduce a nonparametric statistical technique for the detection of malicious users in packet forwarding in network-coding-aided mobile networks. The proposed method is based on the Kruskal-Wallis statistical test [8] and examines whether all the control packets have been generated by a single population (i.e., honest users). It is worth noting that it does not require additional over-

head or monitoring, thus being flexible and appropriate for dynamic IoT scenarios.

The rest of the paper is organized as follows. The system model and the evaluation of the impact of malicious activity are provided in Section II. The proposed framework is introduced in Section III and its performance is assessed in Section IV. Finally, Section V concludes this paper.

II. System Model

A. System Model

We consider the network in Fig. 1, where a given node (A) transmits network coded information to a set of M nodes $\mathcal{C} = \{C_m : 0 < m \leq M\}$. In periodic time intervals, these nodes issue a report $r_m(t) \in \{0, 1\}$ that characterizes the behavior of node A, i.e., $r_m(t) = 1$ and $r_m(t) = 0$ denote that A is a cooperative or a selfish node, respectively. Therefore, given that the time between two consecutive reports is T_r, the report generation is a discrete random process, denoted by $\{r_m(t) : t = t_0 + nT_r, n \in \mathbb{Z}\}$, where t_0 is the time when the first report was generated.

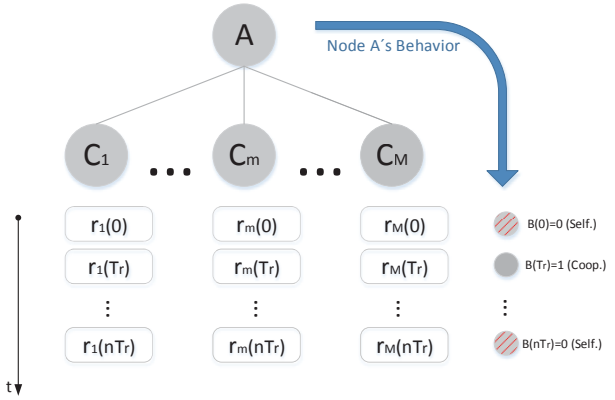


Fig. 1. System Model

Adopting a similar notation for the behavior of node A, we define the binary variable $B(t) \in \{0, 1\}$, which is either 1 or 0 in case that node A is cooperative or selfish, respectively. Assuming that all network users are honest, under ideal channel conditions, it should hold that $r_m(t) = B(t), \forall t$. However, there are unpredictable factors (e.g., the nature of the wireless medium) that could affect the communication and cause the generation of false reports, while the existence of malicious users should not be neglected. In our work, we consider potential channel errors as a probability of false reports (p_e) and we also take into account the probability of deliberate fake reports (p_f).

All generated reports at time t are collected by a central entity, which is responsible for the correct network operation (i.e., network administrator) and makes a decision $d^c(t)$ about node A. This decision is made according to the majority of these reports, which is a special but common case of the widely employed "k-out-of-n" decision rule [9], and can be mathematically expressed as

$$d^{CE}(t) = \begin{cases} 1 & \text{, if } \sum_{m=1}^{M} r_m(t) \geq M/2 \\ 0 & \text{, otherwise} \end{cases}. \quad (1)$$

B. Impact of Malicious Activity

As the central entity does not have any clue about the behavior $B(t)$ of a given node, its decision $d^{CE}(t)$ is exclusively based on the received reports from the other nodes. Therefore, the reception and analysis of fake reports could mislead the central entity and alter the correct decision, causing serious malfunctions in the network. Let us define as $\delta_m(t) = r_m(t) \bigoplus d^{CE}(t)$, $\delta_m(t) \in \{0, 1\}$ the binary variable that compares a particular report with the final decision in order to capture the potential discrepancies. Apparently, $\delta_m(t) = 0$ when the report coincides with the central decision, while $\delta_m(t) = 1$ when the report differs from the decision. However, the identification of malicious users cannot be made based only on these instantaneous reports, mainly due to the dynamic nature of the wireless medium. More specifically, there is always the possibility that some transmissions are not received owing to channel errors and the destination node may falsely characterize the corresponding relay as non-cooperative. As a result, the study of the reports' discrepancies through time is essential to improve the decision's robustness. To that end, we focus on the average value of δ_m in a sequence of L consecutive feedback periods rather than the specific $\delta_m(t)$ value. The expected value can be defined as

$$D_m = \mathbb{E}[\delta_m] = \frac{1}{L} \sum_{n=0}^{L-1} \delta_m(t - n \cdot T_r). \quad (2)$$

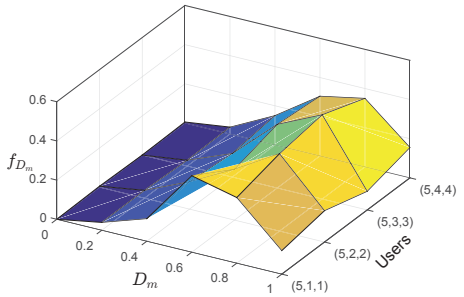
In order to study and identify the different behaviors in the network, we need to focus on the properties of D_m. Since δ_m is a binary variable, D_m can take $L + 1$ discrete values $d_i = \frac{i}{L}$, where $i \in \mathbb{Z}$ and $i \in [0, L]$. Therefore, the range of D_m can be defined as $\mathbb{D} = \{d_0, d_1, ..., d_L\}$, with probability mass function (pmf)

$$f_{D_m}(d_i) = Pr(D_m = d_i), d_i \in \mathbb{D} \quad (3)$$

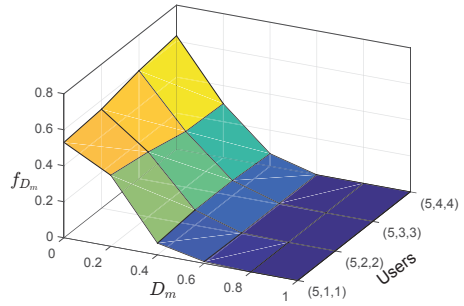
and

$$f_{D_m}(d_i) = 0, d_i \notin \mathbb{D}. \quad (4)$$

For the comprehensive demonstration of the user discrepancies, Fig. 2 provides an example of f_{D_m} in case of a malicious user of type U (Fig. 2(a)) and type O (Fig. 2(b)), considering four different combinations of $\{|U_h|, |M_U|, |M_O|\}$ users in the network, that is {5,1,1}, {5,2,2}, {5,3,3}, and {5,4,4}. The plots in Fig. 2 reveal that, in our case, the normality assumption that would allow the application of parametric statistical methods (e.g., analysis of variance or ANOVA) is too strict, thus stressing the need for nonparametric approaches.



(a) Type U



(b) Type O

Fig. 2. Probability mass function (f_{D_m}) for different types of malicious users(1000 reports, $L = 5$, $B(t) = 0$, $p_f = 0.7$, $p_e = 0.1$)

III. Cooperative Nonparametric Statistical Detection of Malicious Users

In this section, we introduce a nonparametric statistical scheme for the detection of malicious activity in network-coding-enabled wireless networks. The proposed scheme is based on the Kruskal-Wallis method, which is a rank-based statistical test, able to detect whether different sets of samples belong to the same probability distribution. The nonparametric statistical methods are mainly based on the analysis of the median, as no normality is assumed in the distribution of the samples. In particular, median is described as the numeric value separating the higher half of a probability distribution from the lower half, thus being less sensitive than the mean value to vulnerabilities such as outliers and data distribution. Defining as η_m the median of D_m, the null hypothesis H_0 and the alternative hypothesis H_1 of the statistical Kruskal-Wallis test can be expressed as

$$\begin{cases} H_0 : \eta_1 = \eta_2 = \ldots = \eta_M \\ H_1 : \eta_{m_i} \neq \eta_{m_j} \text{ for at least one } m_i \neq m_i. \end{cases} \quad (5)$$

The acceptance of the null hypothesis suggests that the differences between the medians of the different samples are not significant and, therefore, all M random variables are assumed to have been generated by the same population. On the other hand, the rejection of the null hypothesis implies that the M random variables have been generated by different populations, something that verifies the existence of malicious users in the network.

The creation of the database of these samples is fundamental for the application of the proposed method. More specifically, at a given time instant t, the central entity collects the reports of M nodes and makes a decision about node A according to the majority of these reports. Subsequently, as also explained in Sec. II-B, it compares this decision with the individual reports and generates M δ_m binary variables and, after L received reports by each node, we obtain one single sample for the variable D_m. However, the application of statistical methods requires several samples, hereafter denoted by Q, while the non-parametric statistics are based on the ranks of the samples, rather than their actual values. Hence, given a set of samples $\mathcal{S} = \{D_m(t - qT_D) : 1 \leq m \leq M, 0 \leq q \leq Q-1\}$, the rank of each sample $D_m(t - qT_D)$ is denoted by $r_m(t - qT_D)$ and is equal to the number of observations in the set $\mathcal{S}$ that are smaller or equal to $D_m(t - qT_D)$. Accordingly, the test statistic can be written as [8]

$$H = \frac{1}{\sigma^2}\left[\sum_{m=1}^{M}\frac{R_m^2}{Q} - \frac{N(N+1)^2}{4}\right], \quad (6)$$

where N corresponds to the total number of samples (i.e., $N = MQ$), σ^2 is the variance of the ranks, calculated as

$$\sigma^2 = \frac{1}{N-1}\left[\sum_{q=}^{Q-1}\sum_{m=1}^{M} r_m(t - qT_D)^2 - \frac{N(N+1)^2}{4}\right], \quad (7)$$

and R_m is the total sum of the individual ranks for node m, equal to

$$R_m = \sum_{q=0}^{Q} r_m(t - qT_D). \quad (8)$$

In practice, the behavior of H can be approximated by the chi-square distribution with $M-1$ degrees of freedom. Hence, since high values of H imply that H_0 is false, the null hypothesis is rejected if

$$H \geq \chi^2_{\alpha, M-1}, \quad (9)$$

where α denotes the significance level.

IV. Performance Assessment

We consider the system model in Fig. 1, where M nodes receive random linear combinations of the data packets by a particular intermediate node A. In regular time periods, each one of the M nodes generates a report r_m that characterizes the behavior of node A (i.e., either selfish or cooperative). A central entity creates the database and, gradually, every L samples computes the value of D_m. Upon the collection of Q samples of D_m, the central entity applies the Kruskal-Wallis method in order to detect any malicious actions in the network. Regarding the nature of the reports r_m, we assume that the honest users provide

false reports with a probability p_e due to channel errors, while malicious users of type U and O provide deliberately false reports with a probability p_f when node R behaves well and bad, respectively.

Fig. 3 presents the detection probability for different significance levels, assuming two malicious users and various cases of malicious user activity (i.e., $p_f = 0.15$, $p_f = 0.20$, $p_f = 0.25$ and $p_f = 0.30$). We may observe that low values of significance level imply low detection probability, especially when the malicious users are not particularly aggressive (i.e., low p_f). However, as the malicious users become more aggressive and the probability of transmitting false reports increases, the algorithm is able to detect them. More specifically, the proposed algorithm detects any malicious activity with probability equal to 1 when the malicious users have adopted a $p_f = 0.3$. This practically means that even if (nearly) only one out of three reports is fake, the central entity will detect this activity.

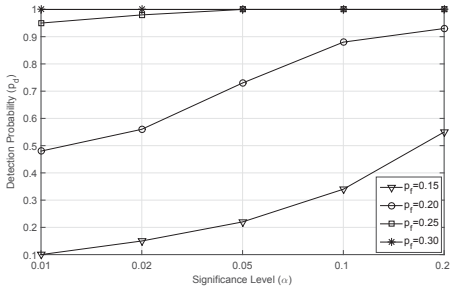


Fig. 3. Detection Probability vs. Significance Level α ($|U_h| = 7, |M_U| = 2, Q = 15, L = 10$)

In Fig. 4, we study the impact of the number of malicious users on the detection probability. More specifically, we examine a topology with three honest users and a variable number (i.e., one to nine) of malicious users. In all scenarios, the significance level has been defined equal to $\alpha = 0.05$ and various cases for the probability of fake reports p_f are considered. It is worth noting that the number of malicious users slightly affects the detection probability when p_f is relatively low (e.g., $p_f = 0.15$), something that can be explained taking into account that the probability of false reports due to channel errors is very close to this value (i.e., $p_e = 0.10$), hindering the distinction between malicious users and users with bad channel conditions. In this case, the reports seem to be generated by a single population, especially when there is only one malicious user in the system. On the other hand, as the probability of misbehavior grows, the detection probability significantly increases.

V. Conclusion

In this paper, we introduced a novel cooperative non-parametric statistical method for the mitigation of user misbehavior in network-coding-aided scenarios. The operation of the proposed scheme is based on the processing of existing control packets and does not require any additional overhead. Through extensive experiments, we have shown that the proposed method detects efficiently the malicious users in the network, even when they adopt a flexible probabilistic misbehavior (e.g., by transmitting only one out of three fake reports). In our future work, we plan to extend our method in order to identify the malicious activity.

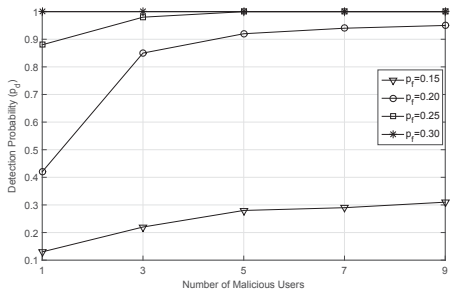


Fig. 4. Detection Probability vs Number of Malicious Users ($\alpha = 0.05, Q = 15, L = 10$)

Acknowledgements

This work has been supported by the research projects CellFive (TEC2014-60130-P), COPCAMS (332913), IoSense (692480) and AGAUR (2014-SGR-1551).

References

[1] S. Djahel, F. Nait-abdesselam, and Z. Zhang, "Mitigating packet dropping problem in mobile Ad Hoc networks: Proposals and challenges," *IEEE Communications Surveys Tutorials*, vol. 13, no. 4, pp. 658–672, Fourth 2011.

[2] T. Chen and S. Zhong, "An enforceable scheme for packet forwarding cooperation in network-coding wireless networks with opportunistic routing," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4476–4491, Nov 2014.

[3] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile Ad Hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00. New York, NY, USA: ACM, 2000, pp. 255–265. [Online]. Available: http://doi.acm.org/10.1145/345910.345955

[4] K. Liu, J. Deng, P. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536–550, May 2007.

[5] E. Shakshuki, N. Kang, and T. Sheltami, "EAACK - a secure intrusion-detection system for manets," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 3, pp. 1089–1098, March 2013.

[6] R. Ahlswede, N. Cai, S.-Y. Li, and R. Yeung, "Network information flow," *IEEE Transactions on Information Theory*, vol. 46, no. 4, pp. 1204–1216, Jul 2000.

[7] D. Koutsonikolas, C.-C. Wang, and Y. Hu, "Efficient network-coding-based opportunistic routing through cumulative coded acknowledgments," *IEEE/ACM Transactions on Networking*, vol. 19, no. 5, pp. 1368–1381, Oct 2011.

[8] W. H. Kruskal and W. A. Wallis, "Use of ranks in one-criterion variance analysis," *Journal of the American Statistical Association*, vol. 47, no. 260, pp. pp. 583–621, 1952. [Online]. Available: http://www.jstor.org/stable/2280779

[9] Q. Zhang, P. Varshney, and R. Wesel, "Optimal bi-level quantization of i.i.d. sensor observations for binary hypothesis testing," *IEEE Transactions on Information Theory*, vol. 48, no. 7, pp. 2105–2111, Jul 2002.