Computer Technology and Application 6 (2015) 37-44
doi: 10.17265/1934-7332/2015.01.006

Performance Analysis under MAC Layer Misbehavior Attack in Mobile Ad-Hoc Networks

Mohammed-Alamine El Houssaini[1], Abdessadek Aaroud[1], Ali El Hore [1] and Jalel Ben-Othman[2]

1. LAROSERI Laboratory, Department of Computer Science Faculty of Sciences, Chouaib Doukkali University, El Jadida 24000, Morocco

2. Department of Computer Science Galilee Institute, Paris 13 University, Paris 93430, France

Abstract: This work presents a multi-criteria analysis of the MAC (media access control) layer misbehavior of the IEEE (Institute of Electrical and Electronics Engineers) 802.11 standard, whose principle is to cheat at the protocol to increase the transmission rate by greedy nodes at the expense of the other honest nodes. In fact, IEEE 802.11 forces nodes for access to the channel to wait for a back off interval, randomly selected from a specified range, before initiating a transmission. Greedy nodes may wait for smaller back-off intervals than honest nodes, and then obtaining an unfair assignment. In the first of our works a state of art on the research on IEEE 802.11 MAC layer misbehavior are presented. Then the impact of this misbehavior at the reception is given, and we will generalize this impact on a large scale. An analysis of the correlation between the throughput and the inter-packets time is given. Afterwards, we will define a new metric for measuring the performance and capability of the network.

Key words: Mobile ad-hoc networks, MAC IEEE 802.11, misbehavior, ns2 simulations.

1. Introduction

The IEEE (Institute of Electrical and Electronics Engineers) 802.11 is a set of standards for wireless networks that have been developed by the Working Group 11 of the Standards Committee LAN/MAN (Local Area Network/Metropolitan Area Network) IEEE (IEEE 802). The 802.11 protocol defines the MAC and physical layers LANs. The MAC (media access control) layer is unique, but the physical layer is divided into three categories: Frequency Hopping Spread Spectrum, Direct Sequence Spread Spectrum and Infrared. These three layers are not directly compatible with each other. IEEE 802.11 was amended several times, which gave other physical layers: IEEE 802.11b, IEEE 802.11a, IEEE 802.11g, and IEEE 802.11n [1].

One of the most significant advantages of the aforementioned standard is the fairness access to the medium that will be detailed below but instead of sharing the transmission channel makes the networks vulnerable to several attacks such as jamming, black holes, and the greedy behavior [2].

The rest of the paper is organized as follows: First we give an overview on the research works related to the IEEE 802.11 MAC layer misbehavior. Then, we present and discuss the results of an analysis and simulation regarding the IEEE 802.11 MAC layer misbehavior. After an analysis of the correlation between the throughput and the inter-packets time is given. Afterwards, we will define a new metric for measuring the performance and capability of the network. Finally, we summarize our contributions and we present the prospects for our future work.

2. Related Work

Several approaches have been proposed in the literature for the detection of the IEEE 802.11 MAC layer misbehavior.

Corresponding author: Abdessadek Aaroud, Ph.D., professor, research fields: mobility and security in wireless, communication systems and channel coding. E-mail: aaroud.a@ucd.ac.ma.

The author in Ref. [3] proposed a detection scheme based on statistical collect of all nodes RTS (request to send) retransmission due to time out, packet retransmission due to ACK (acknowledgment) timeout and throughput at receiver, then compared with the threshold values to decide that a selfish attack is occurring. This method does not require any changes in protocols but is not based on a mathematical or statistical model to define the detection thresholds, in addition to this drawback the detection scheme creates computation overhead.

In Ref. [4] authors proposed a new statistical algorithm to detect selfish nodes. In the first time it compares probability distributions of transmission intervals among all nodes using Kolmogorov-Smirnov test and then divides the nodes into groups by test results. In the second time the algorithm tries to find the greedy node groups through comparing characteristics among groups. This algorithm to pick out selfish nodes cannot be implemented in an ad hoc mode, because the making probability distribution of time intervals is performed at the access point.

In Ref. [5] the authors proposed an extension to the 802.11 CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) standards that ensures a uniformly distributed random back-off through the protocol of coin flipping by telephone.

The proposed approach in Ref. [6] of greedy nodes detection in IEEE 802.11 is based upon the linear regression between the instants of transmission to calculate a detection threshold and without requiring modifications to the standard, additionally it can be centralized or distributed. This idea comes from the strong linear correlation remarked between nodes in the term of transmission instants.

The authors [7] present a system for detection of greedy behavior in the MAC layer of IEEE 802.11 public networks deployed in the access point. This method uses a modular architecture which comprises individual tests and a DMC (decision making component). However, greedy node may exploit the knowledge of DOMINO in order to adapt its parameters to avoid the detection.

In the next section, we present an analysis of this misbehavior and its impact on network performance.

3. MAC Layer Misbehavior Impact

We will show through simulation, the impact of the IEEE 802.11 MAC layer misbehavior on two parameters, the average reception throughput, and the mean time between receptions. The both metrics can be adopted for the deployment of the misbehavior detection strategy. All nodes move randomly following the model Random Way Point, we have chosen the simulator ns-2 [8] with the following parameters depicted in Table 1:

As a first step we have chosen a small network of 4 nodes in total including a receiver Node 0, and we compare two scenarios with and without attack. Figs. 1 and 2 show the simulation results with a granularity of one second.

According to both Figs. 1 and 2, the three nodes are equal and oscillate about a throughput of 0.54 Mb/s, and an inter-packets time of 0.014s. The oscillatory character of the curves can be explained by IEEE 802.11 warranty in term of the access to the transmission

Table 1 Simulations parameters.

Parameter	Value
Computer	HP Compaq 6730s
Operating system	Ubuntu 10.10
Version of the simulator	ns-2.34
Trace file processing language	Perl
Graph construction tool	Microsoft Excel 2007
Transmission rate (Mb/s)	2
MAC layer	802.11
Simulation surface (m)	500x500
Transmission range (m)	250
Radio propagation model	Shadowing
Traffic generator	CBR Constant Bit Rate
Simulation time (s)	60
Packet size (byte)	1000
Routing protocol	AODV
Node speed (m/s)	15
Mobility model	Random Way Point

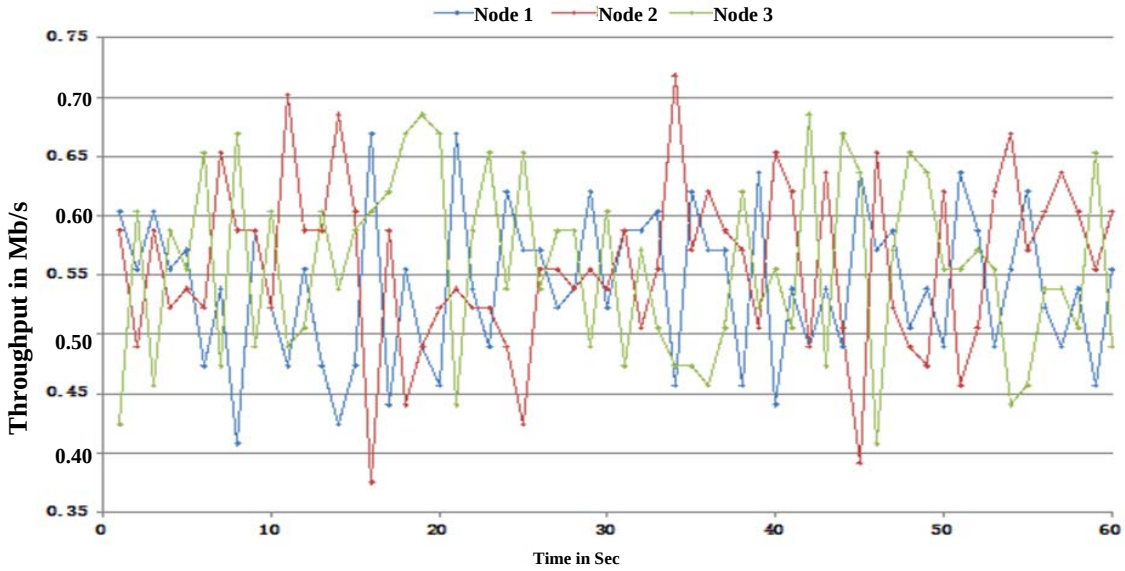

Fig. 1 Throughput in normal case.

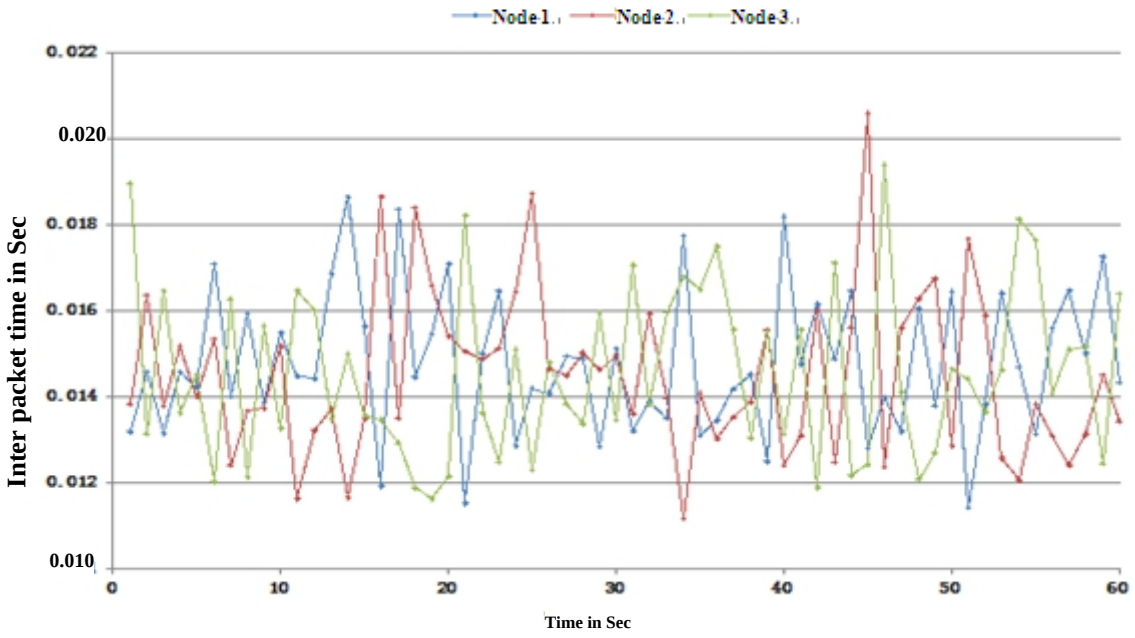

Fig. 2 Inter-packets time in normal case.

channel. The simulation results for the second case, said greedy, are shown in Figs. 3 and 4 (node 3 is the cheater and the other nodes are honest):

The greedy node 3 increases its throughput, which is now 0.94 Mb/s, and reduces its inter-packets time which becomes 0.0086s to the detriment of the other nodes Node 1 and Node 2 (throughput 0.35 Mb/s and inter-packets time 0.023 s).

The next section is dedicated for large scale simulations.

4. Large Scale Simulation

In this section we show the gap in throughput and that in inter-packets time based on honest nodes issuers. We get the same results even in Ref. [9] by introducing the mobility model Random Way Point.

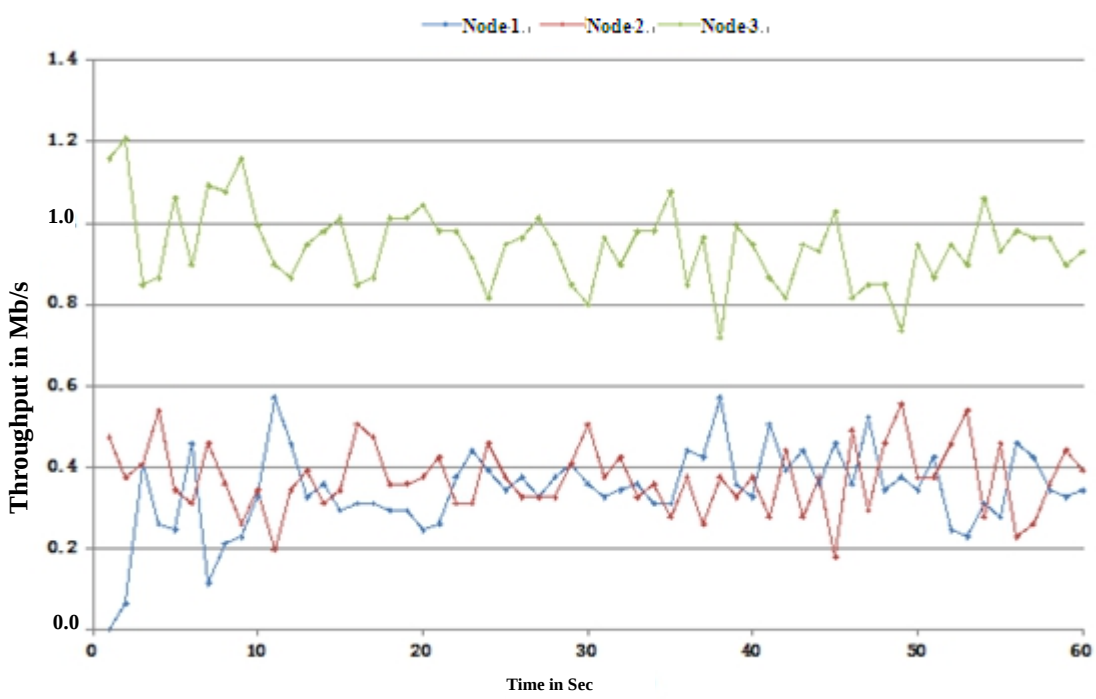

Fig. 3 Throughput in greedy case.

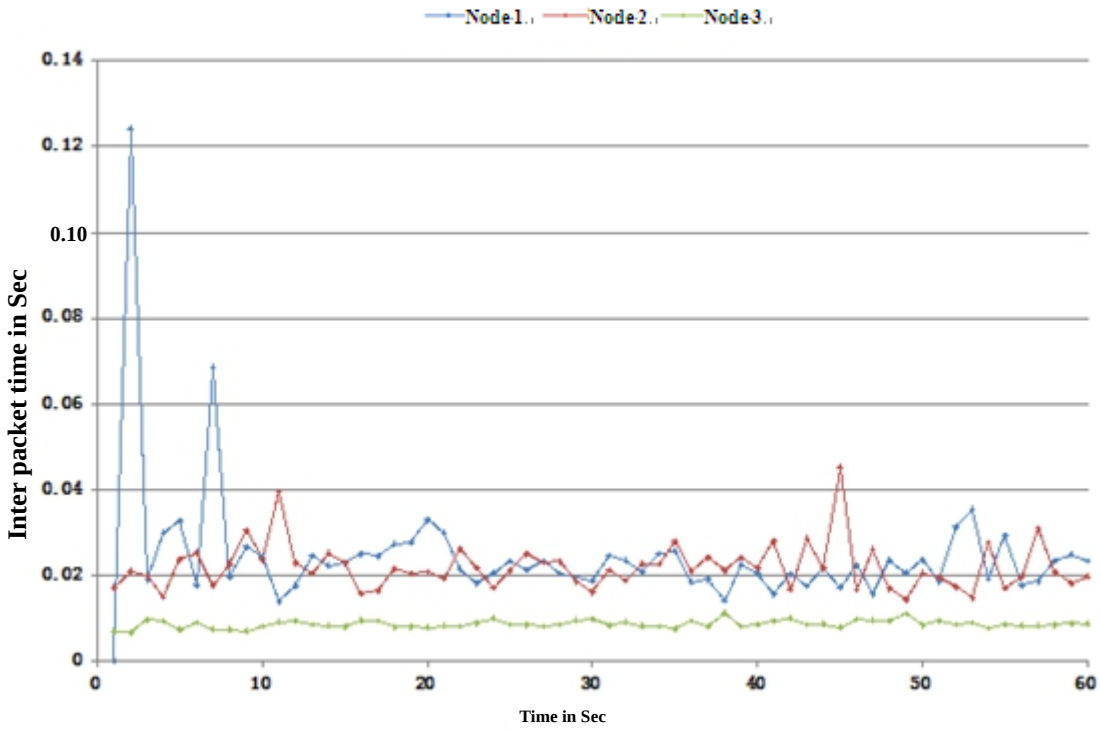

Fig. 4 Inter-packets time in greedy case.

Our results are presented in Figs. 5 and 6.

We also simulate the impact of handling the contention window on the throughput. Fig. 7 shows the simulation results.

To determine the correlation between throughput and inter packets time, Section 5 presents this relationship.

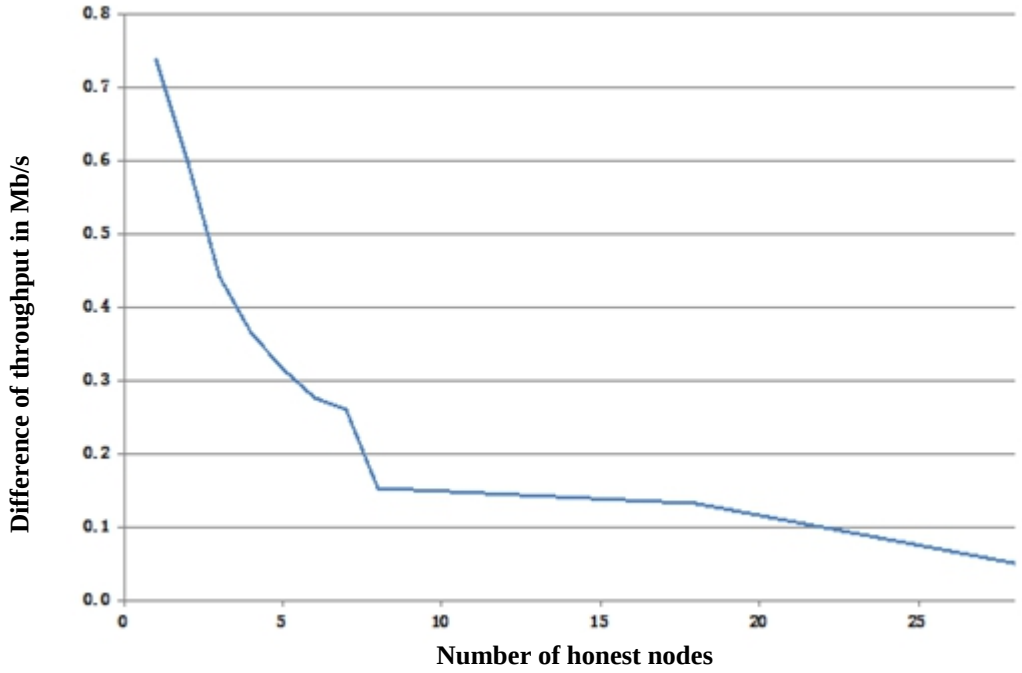

Fig. 5 Difference between honest and greedy throughput.

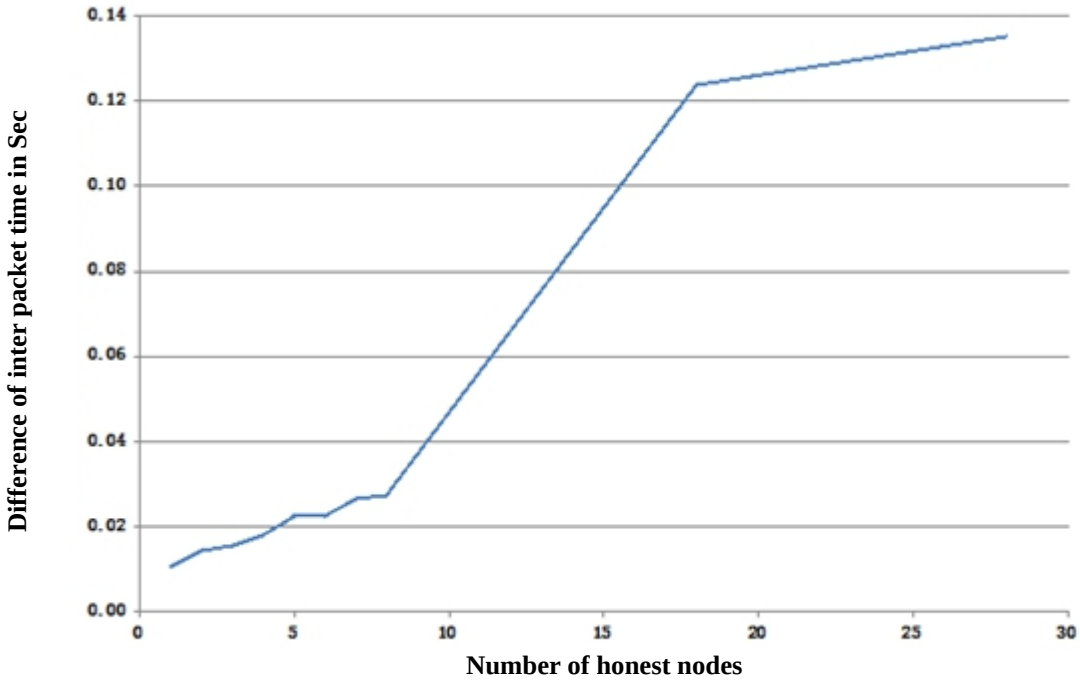

Fig. 6 Difference between honest and greedy inter-packets time.

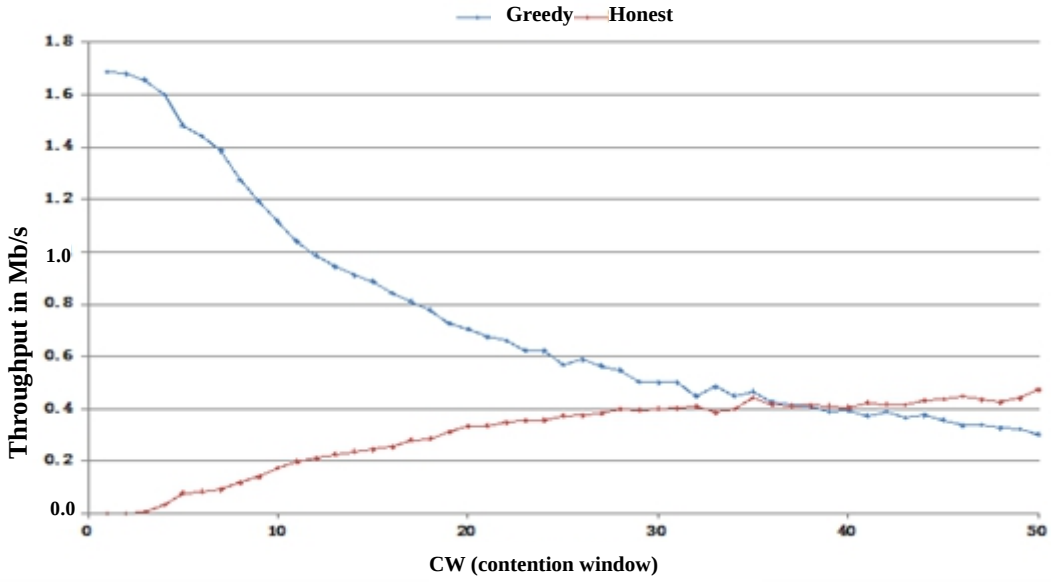

Fig. 7 Throughput according to the contention window.

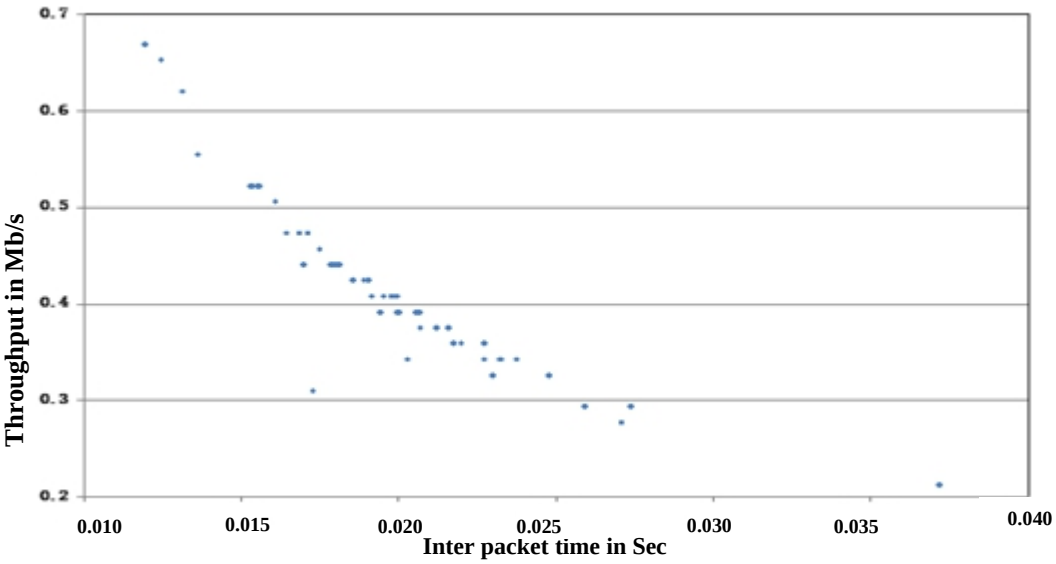

Fig. 8 Correlation between throughput and inter-packets time.

5. Correlation between Throughput and Inter-packets Time

In this section we study the correlation between the two metrics defined in the first section. The scatter plot depicted Fig. 8 shows the relationship between two quantitative variables throughput and the inter-packets time, as measured on the same statistical unit.

It can be seen from Fig. 8 that there is a strong correlation between the two metrics throughput and inter-packets time. We can say that there is a negative linear relationship, to prove this behavior, the correlation coefficient was calculated, which is defined by: $\rho = \text{cov}(X,Y)/(\sigma X.\sigma Y)$.

Where X and Y are two random variables, cov(X,Y) is the covariance of X and Y, σX and σY are respectively the standard deviations of X and Y. We have calculated the correlation coefficient in several scenarios. We have found that this coefficient is very

near to -1 in all the scenarios. Thus, we can say that by using statistical notions it really exists a strong decreasing linear correlation between our two metrics, the throughput and the inter-packets time.

Now we are going to define a new metric for measuring the network performance which called the Capability Ratio.

6. Concept of Capability

Capability is measured by the ratio between the real performance and the required performance of a process. The use of a number to characterize the capability is fundamental and objective, because the use of vocabulary to describe a situation is still blurry. In our work we focus on short-term indicators that reflect the dispersion on a very short time—process capability [10].

The natural tolerance limits of a process fall at $\mu+3\sigma$ and $\mu-3\sigma$, respectively with a mean μ and a standard deviation σ

Upper natural tolerance limit (UNTL) = $\mu+3\sigma$

Lower natural tolerance limit (LNTL) = $\mu-3\sigma$

We can express process capability through the process capability ratio expressed by the symbol C_P (coefficient of performance) [10]:

$C_P = (USL-LSL)/6\sigma$

USL (upper specification limit) and LSL (lower specification limit).

The previous equation assumes that the process has both upper and lower specification limits. For one-sided specifications, one-sided process-capability ratios are defined as follows:

$C_{PU} = (USL-\mu)/3\sigma$

The rules to be applied to decide the capability level are the following [9]:

If CP < 1.33 there is a bad capability

If CP > 1.67 there is a good capability

If 1.33 < CP < 1.67 the capability is acceptable

Our results of simulations are depicted in Fig. 9.

As we can see in the previous figure, the capability coefficient is always greater than 1.67, because the transmission rate is always lower than the theoretical throughput defined by the IEEE 802.11 standard, in other words, the rate is below the upper specification

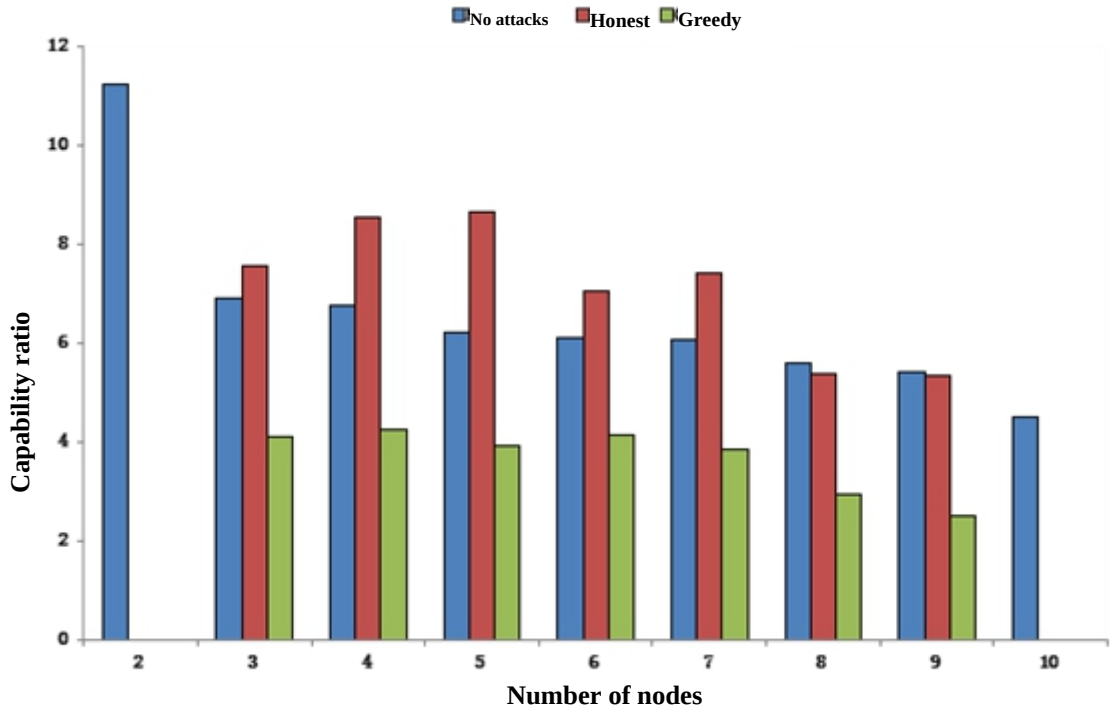

Fig. 9 Capability coefficient according to the number of nodes.

limit. The fall of the capability coefficient with the growth of the number of nodes can be justified by the congestion phenomenon due to the sharing of bandwidth by transmitting nodes, so the cause is the reduction in the throughput. In the presence of MAC layer misbehavior, capability ratio for the greedy node is greater than the honest node, this difference is due to the increased throughput of greedy node, so it is so close to the upper specification limit, and due to the decreased throughput of honest node, so in contrast it is more far to the upper specification limit.

7. Conclusion and Perspectives

The simulation of the misbehavior of the IEEE 802.11 MAC layer shows that the cheater nodes increase their throughput and reduce their inter-packets time to the detriment of the other nodes even if they move randomly depending on the Random Way Point mobility model. We also show that the difference in throughput decreases and the inter-packets time increases according to the number of the honest nodes.

We also put in evidence the strong correlation between these metrics, and we defined a new parameter for measuring the capability of a network. The whole of these metrics will be used in our future work to develop a detection mechanism of greedy nodes in wireless networks.

References

[1] IEEE Standards Association. 2012. “IEEE 802.11 Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.” *IEEE Standards Association* (March): 818-40.

[2] Gupta, V., Krishnamurthy, S., and Faloutsos, M. 2002. “Denial of Service Attacks at the Mac Layer in Wireless Ad Hoc Networks.” Presented at IEEE MILCOM, Anaheim, California.

[3] Tiwary, O. N. 2012. “Detection of Misbehaviour at MAC Layer in Wireless Networks.” *International Journal of Scientific and Engineering Research* 3 (5), May: 909-12.

[4] Han, Y., Seok, S., Song, W., Choi, D., and Huh, J. 2013. “Detection of Greedy Nodes in Wireless LAN through Comparing of Probability Distributions of Transmission Intervals.” *International Journal of Multimedia and Ubiquitous Engineering* 8 (1), January: 175.

[5] Cardenas, A. A., Radosavac, S., and Baras, J. S. 2004. “Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks.” In *Proceedings of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks*, 17-22.

[6] Hamieh, A., Ben-Othman, J., Gueroui, A., and Naït-Abdesselam, F. 2009. “Detecting Greedy Behaviors by Linear Correlation in Wireless Ad Hoc Networks.” Presented at the IEEE International Conference on Communications (IEEE ICC), Dresden, Germany.

[7] Raya, M., Hubaux, J. P., and Aad, I. 2006. “DOMINO: Detecting MAC Layer Greedy Behavior in IEEE 802.11 Hotspots.” IEEE Transaction Mobile Computing 5 (12): 1691-705.

[8] Information Sciences Institute. 1995. “The Network Simulator –ns-2.” Information Sciences Institute. Accessed July 10, 2015. http://www.isi.edu/nsnam/ns/.

[9] El Houssaini, M., Aaroud, A., Elhore, A., and Ben-Othman, J. 2014. “Analysis and Simulation of MAC Layer Misbehavior in Mobile Ad-Hoc Networks.” In *Proceedings of the 5th International Workshop on Codes, Cryptography and Communication Systems*, 10.

[10] Douglas Montgomery, C. 2008. Introduction to Statistical Quality Control, 6th ed. United States of America: John Wiley & Sons, Inc.