ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, Vol 8(21), DOI: 10.17485/ijst/2015/v8i21/71496, September 2015

Real-Time MAC-Layer Selfish Misbehavior Detection and Prevention Technique for Wireless Networks

Shery K. Thambi[1]* and N. K. Sakthivel[2]

[1]Department of Computer Science and Engineering, Nehru College of Engineering and Research Center Pampady, Thrissur - 680597, Kerala, India; sherythambi@gmail.com
[2]Nehru College of Engineering and Research Center Pampady, Thrissur - 680597, Kerala, India; vp@ncerc.ac.in

Abstract

Background/Objectives: Contention issue in the IEEE 802.11 based wireless network is resolved using CSMA/CA protocol that aims to ensure the Fair Share of the channel to each node in the network. A malicious node can manipulate the backoff parameters and gain large share of network access. **Methods/Statistical Analysis:** Since back off parameters are programmable field it can change the value any time. So real time detection of malicious behavior is required. For Real Time Detection a Markov chain-based analytical model is being used. Since the Despite of all its advantages there have been no mechanism used to monitor the MAC layer misbehavior of all the nodes in the wireless network. Only tagged nodes are being monitored. **Findings:** Adding to the challenge of identifying and isolating the malicious node from the network is the non-deterministic nature and distributed functionality of IEEE 802.11 based networks. In order to overcome the problem regarding the defensive mechanism and for better efficiency, this Research work has developed an efficient technique called Markov-RED-FT. By using this model all the nodes in the network can be monitored for malicious misbehavior and the flow trust value is calculated to penalize the malicious node. This proposed Markov-RED-FT employs the flow trust value to safe guard the legitimate flows. Malicious flows would be with lower trust values while legitimate flows would be with higher ones. **Application/Improvements:** This research work implemented the proposed Markov-RED-FT and from the results, it is established that the proposed model is performing well as compared with the existing model in terms of average detection delayand network throughput.

Keywords: Flow Trust, Markov Chain Model, Markov-RED-FT, RED-FT, Real Time Detection, Selfish Misbehavior

1. Introduction

IEEE 802.11 use Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) protocol in order to resolve the MAC (Medium Access Control) contention issue in wireless adhoc networks[1]. The aim of using this is ensures that each node in the network should get a fair share access to the network[2]. A malicious node in the network which chooses a smaller back off timer can selfishly gain large share of the network throughput. This malicious node is using other normal nodes' channel access opportunities. Moreover there are the easily programmable and reconfigurable wireless network devices are available that makes the back off misbehavior more feasible[3].

To efficiently detect the back-off misbehavior two challenges has to be addressed. They are unknown misbehavior strategy and real-time detection of the misbehavior[4]. A malicious node can first behave as a normal node and then manipulate its back-off timer to a random small value as it is programmable. So it is not possible to predict the misbehavior when the system boots up. Since the misbehaving node can drastically reduce the network throughput it has to be detected in real time. Then only it is possible to isolate the malicious node from bringing more harm to the network. The solutions that are already present cannot address both issues at the same time or the 802.11 protocols needs to be modified.

*Author for correspondence

Addressing the challenges Markov-RED-FT model is proposed that can detect the misbehavior in real-time based on the Fair Share detector (FS detector) mechanism. Once the malicious node in the network is identified that node will be penalized. An analytical model using Markov chain based detector is used to monitor the network to find the malicious node in the network. In the detector a discrete-time Markov chain is used to model the behavior of the detector, because the detector's next state depends only on its current value and the coming observation sample. This Markov chain-based model is capable of conducting rigorous quantitative analysis of the FS detector on the average detection delay and network throughput. This Markov chain modeling of the FS detector takes different transition probabilities for the normal traffic condition and also for the abnormal condition with misbehaving nodes present.

Markov model is stochastic model that assumes the Markov property, which refers to the memory less property of a stochastic process. Consider the sequence $\{X_n\}$ as a set of discrete random process that takes values from a finite set A = {1,2,...,h}. This random process is said to be in state i at time n if X_n = i with i ε A. The state transition happens when a successful transmission over the network is observed. The next state X_{n+1} depends only on the current state X_n and is independent of any other previous states. Here the transition probability of this random process can be defined as

$$P_{ij} = \mathrm{P}\{X_{n+1} = \mathrm{j} \,|\, X_n = \mathrm{i}\}\ \mathrm{i, j}\ \varepsilon\ \mathrm{A} \qquad (1)$$

Thus, the random process $\{X_n\}$ satisfies the Markov property that is the lack of history. Here future depends on the present and not on the past. So this process can be modeled as a discrete-time Markov chain. This Markov chain based detector does not require any modification to the IEEE 802.11 protocols. This detector can be implemented by any node in the network by taking the role of the detection agent that monitors the network. Due to this adiscrete-time Markov chain is used to model the behavior of the detector, because the detector's next state depends only on its current value and the coming observation sample. So this type of model enables to conduct rigorous quantitative analysis of the FS detector the system configuration for guaranteed performance.

A common research issue among most of the existing schemes for misbehavior detection is their dependency on heuristic parameter configuration and statistical performance evaluation. But this approach largely limits the flexibility and robustness of the schemes. The proposed Markov-RED-FT model analyzes the network performance by using Markov model and defense the network by dropping the packets from the malicious node. The detection part of this model is developed according to the FS detector based on Markov chain Analytical Model. This analysis demonstrates performance improvement of the FS detector in real-time misbehavior detection over the original detector. The robustness of the detector is demonstrated under varying network size, against the short-term unfairness, and in the situation when both UDP and TCP traffic exists. Markov chain modeling the FS detector takes different transition probabilities under the normal traffic condition and under the abnormal condition with misbehaving nodes present, respectively.

This selfish misbehavior may leads to Denial-of-Service (DoS) attacks, only detection of misbehavior nodes in the network is not sufficient. Since the network is saturated the flow trust factor is an important decision making factor of Active Queue Management (AQM) of the network. Floyd et al.[5] proposed the Random Early Detection (RED) algorithm firstly. The RED calculates the dropping probability of packets according to the average queue length and acquires a better queue stability. Further-more, the adaptive RED[6]improved the weight controlling. Similar to the RED, a Blue algorithm [7] used the packets loss events and the link idle events to handle the link congestion. Recently, Kim et al.[8] proposed a queue management algorithm according to the weighted fairness of flows in wireless networks.

Most AQM algorithms are unsuitable for networks environments under DoS attacks because of the impact of attacks were not considered. Recently a letter which presents a RED with Flow Trust (RED-FT)[9] using networks flow characteristics to ensure the legitimate users' communications and the fairness of the queue as much as possible has been published. This networks flow trust is integrated with this detection scheme as an important decision-making factor of AQM and improve the robustness of previous algorithms, e.g. the RED, in complex networks environment under DoS attacks.

The problem of detecting back off misbehavior over the802.11-based Medium Access Control (MAC) protocol has been widely studied in the literature. In IEEE 802.11 protocol, a sender transmits an RTS (Request to Send) after waiting for a randomly selected number of slots in the range [0, CW]. Consequently, the time interval between consecutive transmissions by the sender can be any value within the above range. Hence, a receiver that observes the time interval between consecutive transmissions from the sender cannot distinguish a well behaved sender that legitimately selected a small random back off from a misbehaving sender that maliciously detect sender misbehavior by observing the behavior of senders over a large sequence of transmissions. This approach results in a large delay in detection of misbehavior[10]. In addition, it may not be feasible to monitor the behavior of senders over a large sequence of transmissions when host mobility is high. Furthermore, two hosts may obtain the same throughput share over the long term, but one host may achieve significantly lower delay by misbehaving (the misbehaving host may immediately access the channel, but the well-behaved host may have a significant contention resolution delay, especially at higher loads). IEEE 802.11 is modified to enables a receiver to identify sender misbehavior within a small observation interval.

Normally sender is selecting back off values but the receiver selects an arbitrary back off value and sends it in the CTS (Clear to Send) and ACK packets to the sender[11]. The sender takes this new back off value in the next transmission to the receiver. With these modifications, a receiver knows the exact back off value a sender is expected to use. Hence, receivers can verify whether the sender is involved in misbehaving by observing the number of idle slots between consecutive transmissions. Receiver counts the number of idle slots and if it is less than the assigned back off, then the sender may not be behaving properly. Receiver measures the deviations over a small history of received packets is used to predict the sender misbehavior with high probability. This technique attempts to negate any throughput advantage that the misbehaving hosts may obtain. Misbehaving senders are penalized, thereby discouraging misbehavior. When the receiver perceives that a sender has waited for less than the back off value assigned by the receiver, it adds a random value to the next back off assigned to that sender. If the sender does not back off for the duration specified by the penalty value, it significantly increases the probability of detecting misbehavior. On the other hand, a misbehaving sender which backs off for the duration specified by the penalty (or a large fraction of it) does not obtain significant throughput advantage over other well-behaved hosts. Hence, with this scheme, it is difficult for a misbehaving host to obtain an unfair share of the channel while eluding detection. This technique requires a modification to the IEEE 802.11 protocol to detect this type of back off selfish misbehavior. This model requires a trustworthy receiver, since the receiver assigns the back-off value to the sender that has to be used. This approach depends on the trust worthy receiver and modifying the already existing IEEE 802.11 protocol are its drawbacks.

Kolmogorov-Smirnov significance test for back off misbehavior detection is used to determine the statistical performance of the network and relies on expert knowledge to set up and maintain the set of heuristic rules for the detector[6]. The successful transmissions are observable from a node and in the event of a collision it is very difficult to determine which nodes are involved in it for a larger network. Then this model requires an ideal scenario in which the misbehavior strategy is completely known before hand, but it may not be possible. For those reasons, this misbehavior detection model proposed is not that user friendly to use. An inaccurate simplification there is to consider that packets from the misbehaving node and those from the normal nodes have the same collision probability[12]. Such inaccuracy impacts both the performance of false positive rate and detection delay. The K-S test has lot of drawback when it is used as a batch test method[13]. For that fixed-size data samples are needed to perform the test each time, that is very difficult and it makes real-time detection difficult.

Another approach to deal with the back off misbehavior is to develop protocols based on the game-theoretic techniques. The goal is to encourage all the nodes to reach Nash equilibrium. As a result, a malicious node is not able to gain an unfair share compared to well be have nodes and, thus, discouraged from the misbehavior. However, this category of approaches assumes that all the nodes are willing to deviate from the protocol when necessary, and the standard protocol needs to be modified. A heuristic sequence of conditions is proposed in to test multiple misbehavior options over the 802.11 MAC based on simple numerical comparisons.

Once the misbehaving node is detected in the network it is required to defend the network against such selfish misbehavior. Konorski[14] designs game theoretic approaches for WLANs which are resilientto selfish misbehavior. All the defense approaches need greatly modify the standard IEEE 802.11 MAC protocol. Since this type of attacks are more critical to saturated networks. So it important to use better Active Queue Management (AQM) technique intelligently. Random Early Detection (RED) scheme is being widely used but it is more or less maintaining the stability of the queues. But considering the criticality of the DoS attacks that can happen due to malicious attacks just RED is insufficient and needs more robust technique.

2. Identified Problems

The increased transmission probability of the malicious node causes more collisions and normal nodes are forced to further exponentially defer their transmissions as they operate according to the protocol[15]. The back off misbehavior can drastically decrease the transmission probability of normal nodes and subsequently severely reduce their throughput. In an extreme case where a malicious node sets its own back off timer to a very small constant value, it will lead to Denial of Service (DoS) of the whole network. Thus, a detection scheme capable of quickly identifying the misbehaving malicious node is highly desired.

When the network is close to full utilization, the data buffer in every node has a very small probability to be empty, where the saturated model is a good approximation. So it is very important to manage the queues for getting better network throughput.

In order to demonstrate the criticality of this problem a network with 10 Nodes is taken. Here a malicious node say Node 3 is manipulating its contention window size to 16. Then the transmission probability of Node 3 is very high compared to all other nodes in the network. This is being analyzed in the Figure 1. This shows the presence of a malicious node in the network affect very worst on the throughput of the whole network. This leads to the Denial of Service attack. So it is very important to identify and isolate the malicious nodes in the network and secure it from the malicious misbehavior attack. Once a node is determined as a selfish node, a penalty scheme has to applyto the selfish node by decreasing its throughput.

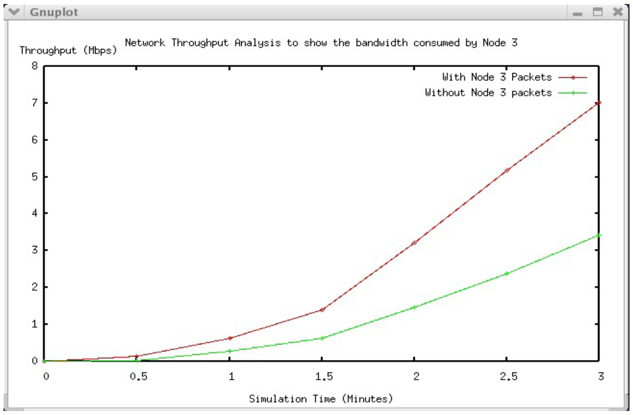

Figure 1. Network throughput anlyzis to show bandwidth usage by malicious node, Node 3 in the network.

3. Proposed Technique

Suppose that the initial value of the detector is $X_0 = 0$. If a successful transmission upon the nth observation is from the tagged node, i.e., $I_n = 1$, the detector X_n increases by N –1, otherwise, $I_n = 0$, and X_n decreases by 1 until it reaches 0. The intuition of this design is as follows: If the node is behaving properly, each node roughly takes turn to transmit, the increase of X_n caused by one successful transmission from the tagged node can then be equally offset by the successful transmissions from other N –1 non tagged node. Thus, the detector X_n will fluctuate around a low value close to zero in the normal situation. On the other hand, when the node turns to misbehave and obtain more chances to transmit, it is not difficult to see that X_n is going to quickly accumulate to a large positive value. If the same node is observed to be misbehaving all the times, then deactivate that node from the entire network depends upon the application. This way fairness of the detection is maintained. Using this method all the nodes in the network are being monitored so a more secured and distributed ad hoc network can be guaranteed by this method.

This transition probability matrix can be divided into three distinct groups based on the operation of the FS detector.

Group 1 is related to the transitions from system initialization (state 0) to other states. According to the state transition (1), the detector variable X_n jumps out of state 0 only when the observed successful transmission is from the tagged node, that is, I_n =1. Further, X_n makes a transition to either N –1 or h depending on whether N –1 is greater than h or not. Note that the state h in fact incorporates all possible states $X_n \geq$ h, as the detector will raise an alarm when the state hits h. Group 1 consists of P_{ij} for i = 0 and j ε [0, h] with

$$P_{0j} = \begin{cases} P\{I_n = 0\} \;\; \text{if j} = 0 \\ P\{\mathrm{I}_n = 1\} \;\; \text{if j} = \text{N-1 and N-1} \leq h, \\ P\{I_n = 1\} \;\; \text{if j} = \text{h and N-1} \; > \; \text{h}, \\ 0 \text{ otherwise} \end{cases} \tag{2}$$

Group 2 consists of P_{ij} for i ε [1, h −1] and j ε [0, h], with values. This group describes the typical behavior of the detector. The state can transit to left (i.e., to a smaller value) when I_n= 0 or to right (i.e., to a larger value) when I_n=1, according to the state transition (1).

$$P_{ij} = \begin{cases} P\{I_n = 0\} & \text{if } j = i\text{-}1 \\ P\{I_n = 1\} & \text{if } j = i + N\text{-}1 \text{ and } i + N\text{-}1 \le h, \\ P\{I_n = 1\} & \text{if } j = h \text{ and } i + N\text{-}1 > h, \\ 0 \text{ otherwise} & \end{cases} \tag{3}$$

Finally, group 3 consists of P_{ij} for i = h and j ε [0, h] with values.

$$P_{hj} = \begin{cases} 1 \text{ if } j = 0, \\ 0 \text{ otherwise} \end{cases} \tag{4}$$

This group is related to the transitions out of state h. Since the detector value will be reset to 0 as soon as it reaches or exceeds h, P_{h0} = 1. This is the group which is important that the detection, once the node crossed the threshold it will be in the state h.

It is very important to isolate the network from malicious attacks by discarding the packsts from the malicious node. So in the Markov-RED-FT mechanism the trust of the packet flow in the network is evaluated. Once the node is identified as malicious that node has to be penalized by discarding the packets from that node until they receive another decision notice indicating that this node is not selfish any more. In the RED like algorithms the stability of the queue was only considered and the network flow trust was not involved. The core steps of the Markov-RED-FT are listed as follows. Firstly each packet flow from each node is monitored. Secondly depends on the packet flow compared to the threshold calculated above and the trust values are calculated. Three strategies are selected according to the network flow trust value: 1. A network flow is trusted and standard RED operation is carried out. 2. A network flow is distrusted and packets are dropped by using RED-FT

Figure 2 illustrates the framework of Markov-RED-FT. In this paper the malicious node detection is done in the Network Flow Detection Module (NFDM) using Markov-chain based analytical model. In the Trust Evaluation Module each flow is compared against the threshold value and if it crosses the threshold, that flow is marked as malicious. Malicious flow details are entered to the RED Module (REDM) and all packets from that flow are being dropped. The REDM executes adaptive RED operations according to the current queue length and the trust value.

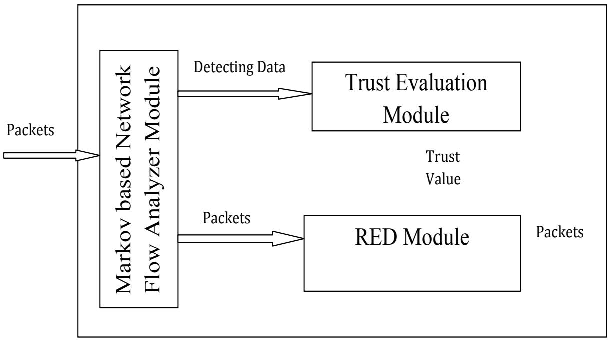

Figure 2. Framework of the proposed Markov-RED-FT.

Algorithm: Markov-RED-FT

- Mark the flow trust value of packet flow from each node in the network as high.
- Use RED algorithm for AQM in the network.
- Count the number of successful packet transmission from each node using Markov-chain based analytical method.
- In the given time if a node cross the given threshold mark that node as malicious.
- Mark the flow trust value of that malicious node as low.
- Call the RED-FT AQM mechanism to drop all the packets with the marked low flow trust packets.

4. Results and Discussions

Establish an 802.11 DCF based wireless network. Both TCP and UDP traffic can be used by the wireless network. The ad hoc network is being saturated with competing traffic. The wireless network consisting of 10 competing nodes (N = 10) with common destination. This common destination acts as the Access Point in the ns-2 simulation[16]. The nodes are located close enough to sense the transmissions from each other and by this way the hidden terminal problem can be avoided. There is one misbehaving node among the 9 competing nodes, which accesses the wireless channel using the binary exponential back off scheme but can manipulate its minimum contention window $CW_{\min}$ to any value between 1 and 32, and is taken as 16. In a wireless ad hoc network, a node that has just accomplished a successful transmission will have advantages in grabbing the channel for next transmission in a short period. This characteristic of the ad hoc networks is referred to as short-term unfairness. This issue implies correlations among the channel accesses probability, which impact the accuracy of the transition probability calculation based on the assumption of independent channel access. The system configuration based on an inaccurate model can lead to inaccurate detection results.

4.1 Average Detection Delay

The average detection delay is the average number of samples observed from the moment that the tagged node starts to misbehave until the misbehavior is detected. With the Markov chain under the abnormal condition (abnormal Markov chain), can be computed as the expected number of transitions required for the state variable to hit state h, starting from the moment when the misbehavior starts. To carry out the analysis, the transition probabilities of the abnormal Markov chain and determine the initial state of the FS detector when the misbehavior starts.

From the Figure 3, it is noted that the proposed simulation model is verifying each and every Node which are present in the Network to predict malicious Nodes and consequently the Average Detection Delay of our simulation is smaller than that of existing Markovi an and analytical values. It shows that our Simulation Results ensure the reliability of the Network and also noted that the existing Analytical Value didn't verify all existing Nodes in Network. If the Markovi an model wants to monitor all the nodes in the network then it has to scale the delay. So this paper presents a modified model of very efficient average detection delay. The Average Detection Delay increases with h value as expected. Then from the above graph it is noted that threshold 40 gives maximum performance.

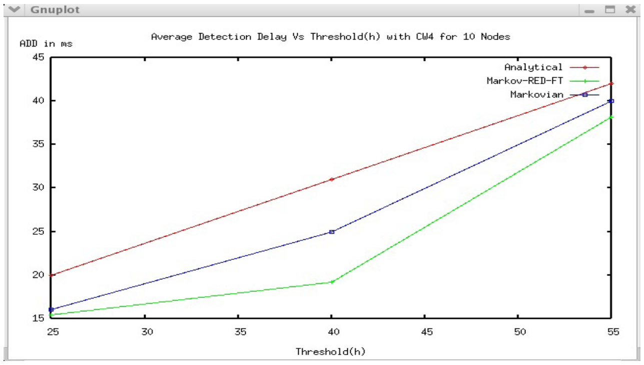

Figure 3. Average Detection Delay of malicious node using Markov-RED-FT.

From the Figure 4, it is noted that for all different Contention Window Sizes (CW_{min}), our proposed Markov-RED-FT Mechanism is continuously achieving better performance as compared with existing Markovi an model. It is also observed that the when the nodes shows intense misbehavior that leads to a shorter Detection Delay and hence if the node selects smaller contention window size then the detection is faster.

4.2 Throughput

Figure 5 shows the simulation result on average throughput and simulation time on normal RED and RED-FT algorithm. This graph is printed by analyzing the trace files. Here in this project the RED algorithm is used in the beginning till the malicious node has been identified.

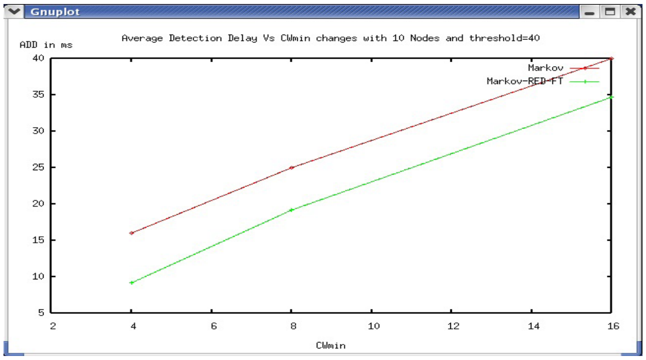

Figure 4. Impact of CW_{min} changes on Detection Delay with 10 Nodes using Markov-RED-FT.

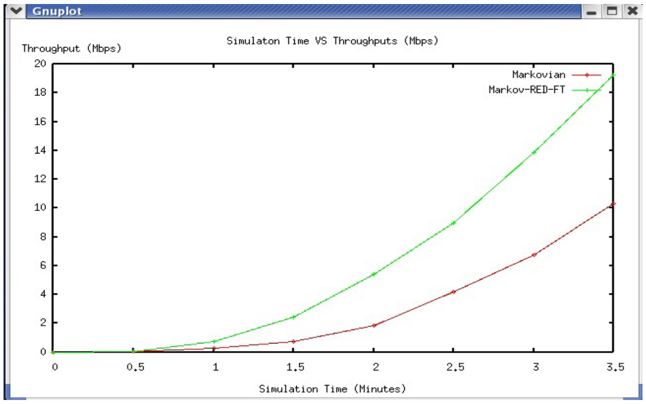

Figure 5. Network throughput increases after using Markov-RED-FT.

Once the malicious node has been identified and the flow trust value from that node is calculated and then RED-FT algorithm is being used. With this graph, we can clearly see the throughput of the network increases by using RED-FT algorithm.

Now the drop rate of the malicious node 3 can be analyzed. As already mentioned above the network consider for this scenario is saturated. The saturated scenario is more meaningful concern in the context of selfish misbehaving. There are always packet dropping happens from all nodes especially from the misbehaving node, Node 3. Now let us analyze the packet dropping from Node 3, with and without RED-FT algorithm.

From the Figure 6 it is very clear that more number of packets from the malicious node, Node number 3 is being dropped. This way network is being protected from the DoS attack. All other nodes in the network have higher probability to transmit their packets and the average throughput of the network is increasing.

It is clear from Figure 7 that the packet Delivery Ratio of the proposed Markov-RED-FT model is higher than that of the existing Markov model. Here the PDR is not taken for the malicious node, Node 3 packets. So the packets from the well behaved nodes are lost in the network due to the presence of malicious node in the network.

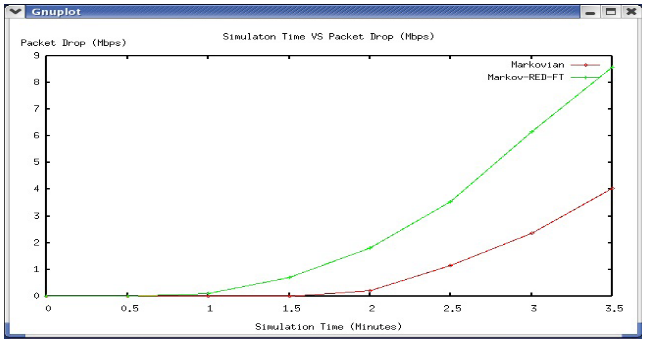

Figure 6. The average Packet Dropping Analysis of Malicious Node, Node 3.

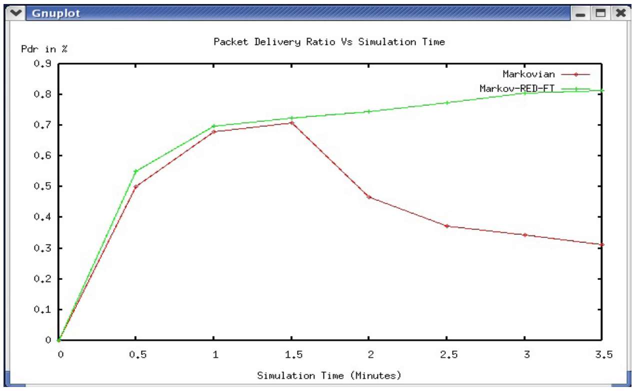

Figure 7. The PDR of proposed Markov-RED-FT.

5. Conclusions

The proposed Markov-RED-FT is a novel Fair Share Detector for Real-Time Back off Misbehavior Detection in IEEE 802.11-based Wireless Networks. Also, a Markov chain based model to theoretically analyze the detection performance of the scheme was developed. Most of the existing work for back off misbehavior detection depends on heuristic parameter settings and statistical performance evaluation; it is able to use this model for a quantitative study to achieve guaranteed detection performance based on parameters like Average Detection Delay and Network Throughput. The potential work on the Markov-RED-FT includes the analysis and propagation of flows trust in networks, the enhancement of the detection accuracy and the defense of more network-layer attacks. For future work it is planned to systematically study the generic scenario with multiple misbehaving nodes in an Ad Hoc Wireless Network.

6. References

1. Tang J, Cheng Y, Zhuang W. Real-Time Misbehavior Detection in IEEE 802.11-Based Wireless Networks: An Analytical Approach. IEEE Transactions on Mobile Computing. 2014 Jan;13(1).
2. Bianchi G. Performance Analysis of the IEEE 802.11 Distributed Coordination Function. IEEE J Selected Areas in Comm. 2000 Mar; 18(3):535–47.
3. Toledo, Wang X. Robust Detection of Selfish Misbehavior in Wireless Networks. IEEE J Selected Areas in Comm. 2007 Aug; 25(6):1124–34.
4. Li M, Li P, Sun J, Huang X. MAC-Layer Selfish Misbehavior in IEEE 802.11 Ad Hoc Networks: Detection and Defense. IEEE Transactions on Mobile Computing. 2014; 14(6):1203–17.
5. Floyd S, Jacobson V. Random early detection gateways for congestion avoidance. IEEE/ACM Trans Networking. 1993; 1(4):397–413.
6. Floyd S, Gummadi R, Shenker S. Adaptive RED: an algorithm for increasing the robustness of RED's active queue management; 2001 Aug. Available from: http://www.icir.org/floyd/papers/adaptiveRed.pdf

7. Feng W, Kandlur D, Saha D et al. Blue: A new class of active queue management algorithms. IEEE/ACM Trans Networking. 2002; 10(4):513–28.
8. Toledo, Wang X. A Robust Kolmogorov-Smirnov Detector for Misbehavior in IEEE 802.11 DCF. Proc IEEE Int'l Conf Comm (ICC); 2007. p. 1564–69.
9. Kim D, Kim J, Yoon H et al. AQM for weighted fairness in wireless LANs. IEEE Commun Lett.2011; 15(11):1199–201.
10. Jiang X, Yang J. RED-FT: A scalable RED scheme with Flow Trust against DoS Attacks. IEEE Communications Letter. 2013 May; 17(5)
11. Kyasanur P, Vaidya N. Detection and Handling of MAC Layer Misbehavior in Wireless Networks. Proc IEEE Int'l Conf Dependable Systems and Networks (DSN '03); 2003. p.173–82.
12. Rong Y, Lee S, Choi H. Detecting Stations Cheating on Back off Rules in 802.11 Networks Using Sequential Analysis. Proc IEEE INFOCOM; 2006. p. 1–13.
13. Radosavac S, Baras JS, Koutsopoulos I. A Framework for MAC Protocol Misbehavior Detection in Wireless Networks. Proc ACM Workshop Wireless Security; 2005. p. 33–42.
14. Radosavac S, Moustakides G, Baras J, Koutsopoulos I. An Analytic Framework for Modeling and Detecting Access Layer Misbehavior in Wireless Networks. ACM Trans Information and Systems Security. 2008 Jul; 11(4):19.
15. Konorski J. Protection of fairness for multimedia traffic streams in a non-cooperative wireless lan setting. PROMS, Springer; 2001; 2213 of LNCS.
16. Available from: http://www.isi.edu/nsnam/ns/tutorial/ tutorial for network simulator "ns"