ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

Detecting MAC Layer Misbehavior in Wifi Networks By Co-ordinated Sampling of Network Monitoring

M.Shanthi[1], S.Suresh[2]

Dept. of Computer Science and Engineering, Adhiyamaan college of Engineering, Hosur, India[1, 2]

Abstract—We present an approach to detect a selfish node in a wireless network by passive monitoring. This does not require any access to the network nodes. Our approach requires deploying multiple sniffers across the network to capture wireless traffic traces among multiple channels. IEEE 802.11 networks support multiple channels and a wireless interface can monitor only a single channel at one time. Thus, capturing all frames passing an interface on all channels is an impossible task, and we need strategies to capture the most representative sample. When a large area is to be monitored, several sniffers must be deployed, and these will typically overlap in their area of coverage. The goals of effective wireless monitoring are to capture as many frames as possible, while minimizing the number of those frames that are captured redundantly by more than one sniffer. The above goals May be addressed with a coordinated sampling strategy that directs neighboring sniffer to different channels during any period. These traces are then analyzed using hidden markov model to infer the misbehavior node in wifi networks.

Keywords— Hidden markov model, selfish carrier sense, coordinated sampling.

I. INTRODUCTION

With the advent of programmable radios, different MAC protocol parameters can be manipulated in various ways to gain unfair share of the available wireless bandwidth. Several radio interfaces and corresponding device drivers allow the user to choose the clear channel assessment(CCA) threshold and /or the back off window size[7]. Manipulation of CCA and back off can deliver an unfair bandwidth advantage to a selfish node[7].Thus, the selfish node gains more transmission opportunities.

Selfish node detected by sniffers which can monitors all channels with one radio device using coordinated sampling mechanism. In our knowledge, this type of monitoring mechanism has been explored only in one paper[10],that provides solution for intrusion detection. The task of monitoring multiple channels is difficult because 'N' no of channels are used and lack of clarity in wireless access.

In wifi networks multiple channels may be active simultaneously. while monitoring the wifi networks in specific location ,there are two choices 1.Fixing multiple radio in one monitoring device, 2.multiple single radio device in one location. But these methods are not feasible ,because huge amount of hardware required and also costly. our approach monitors multiple channels using single radio but periodically changing the channel on which the radio device is capturing the traffic traces. The monitored traffic traces are merged in centralized sniffer based on time intervals. The merged traffic traces are analyzed by Hidden markov model to predict the selfish node based on probability of deferral behavior in sender side.

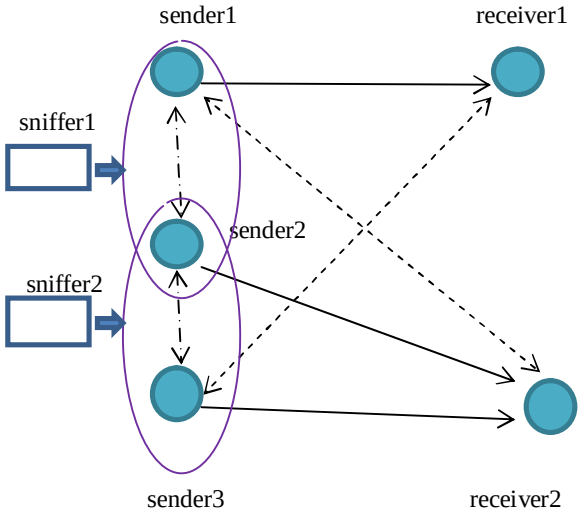

Fig 1. Overview of the approach.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

A. Approach

A set of "sniffers" are deployed to collect traffic traces from large network. Each sniffer contains only one radio device. The radio device shifts the channels periodically in predetermined order which is given by centralized sniffer, using coordinated sampling algorithm. Monitored traffic traces are merged ,analyzed by Hidden Markov Model to predict the selfish node. Our approach achieve following three goals, it doesn't require multiple radio device, it maximizes the capturing of unique frames and reduce the overlap between sniffers. The most important challenging is entire traffic traces are not monitored.

We discuss related work in section 2 and the broad approach in section 3.The details of the HMM in section 4.section 5 presents the experimental evaluations for selfish carrier sensing detection. we will conclude in section 6.

II. RELATED WORK

A. Detecting MAC-Layer Misbehavior in 802.11

Most of the existing MAC layer misbehavior detection techniques only attempt to detect one type of selfish behavior: backoff manipulation in 802.11.They use different methods , such as game theoretic approach[12].sequential Probability[13],nonparametric cumulative sum(CUSUM) test[14],coordination from the receiver[15] to identify backoff manipulation or to restrict the sender from being selfish DOMINO[2] can detect other misbehaviors in addition to backoff manipulation ,e.g., sending scrambled frames, "using smaller DIFS and using oversized NAV.None of these techniques can detect selfish carrier-sense behavior and thus can be complementary to the approach described in this paper. Manipulation of the carrier sense behavior is harder to detect. This is, because normal fluctuations of wireless channel must be distinguished from carrier sensing. In our knowledge [2],[7] has addressed this issue, but [7] uses active measurement,[2] uses the monitoring mechanism for single channel only.

B. Use of Distributed Sniffers

Distributed sniffer traces will be used for multiple reasons such as congestion [1].The DAIR system also uses such an approach for troubleshooting [3] and security [4].The system which is used to trace as well as merge wireless frames from sniffers [09].The sniffers in this system are all configured to capture packets on the same channel, which leads to a large percentage of frames being heard at multiple sniffers.

III. OVERALL APPROACH

A. Problem Statement

Our general goal is detection of selfish node by sniffer. But in existing approach the sniffer monitor the single channel traces and/or to monitor multiple channel it requires multiple radio device, it requires bulk amount of hardware. our approach uses one radio device to monitor the multiple channels periodically.

We wish to capture as much traffic as possible. our approach collects only a sample of frames passing through all the channels, We call this technique channel sampling. channel sampling shifts the radio sequentially through each channel in the wireless network, in a predetermined order, and spends equal amounts of time on each.

Consider a multiple sniffer in large area, some areas covered by more than one sniffer. we say that two sniffers are neighbors if they have recently captured a redundant frame. Neighboring sniffers will observe the same channel to be busy and therefore choose to spend more time on same channels. We define overlap as the total amount of time that neighboring sniffer spend on the same channels. This overlap results in redundant frame capture by neighboring sniffers. Therefore ,to better address the goal of maximizing unique frame capture we need to reduce the amount of overlap.

In order to detect the probability of deferral among two senders on dynamically changing channels we used the "coordinated sampling" for network monitoring[10]to avoid the redundancy.

In this paper we describe a "coordinated sampling "strategy to capture the unique frames by reducing the overlap time.

B. Capture Unique Frame

Our hypothesis is that scheduling the channels on Sniffers, as shown in Fig. 2. and 3, such that the coverage includes minimal overlap, should result in even greater unique frame capture.

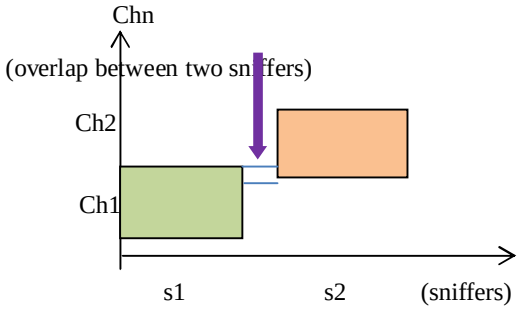

Fig. 2. Overlap between two sniffers at time t1.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

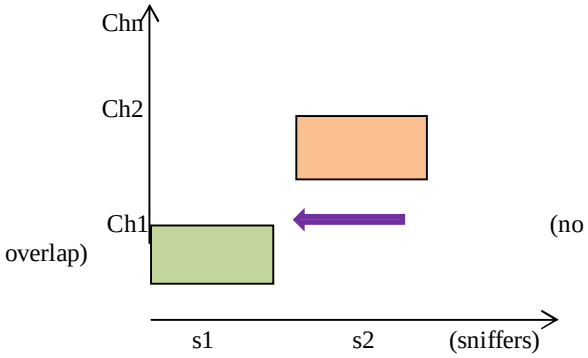

Fig. 3. No overlap between two sniffers at time t2.

Our approach has three goals

- maximize unique traffic capture through proportional sampling,
- capture representative traffic by ensuring that all channels are sampled and that there is coverage over space and time, and
- minimize redundant frame capture by coordinating neighbor's schedules.

Our approach recognizes three constraints

- a single radio can capture traffic only on one channel at one time,
- deploying a sniffer costs money and space, hence limits deployment,
- no frames are captured during channel changes, which take time.

C. The Coordination sampling Algorithm

The coordinated sampling schedule reduce the overlap among neighboring sniffer. The central controller determines a sampling schedule for all sniffers, based on statistics of recently captured traffic.

The output of the coordinated sampling strategy is a channel sampling schedule for each sniffer, identifying the order and duration of visited to each channel. we use simulated annealing approach to minimize the overlap time. The coordinated sampling generates a series of schedules by altering each schedule a little. If new schedule has lower overlap we keep it otherwise we keep it anyway with probability. Our algorithm works as follows.

1) Identify the neighbor relationships among all sniffers.
2) Create a new schedule S for each sniffer for assigning
the multiple channels dynamically.
3) for each sniffer i……..N
4) for each neighbors j…….M
5) calculate overlap between i&j,(i.e $overlap_{ij}$)
6) if($overlap_{ij}$ >overlap limit)
7) reschedule the channel assignment based
on next priority channels
8) end loop
9) end loop.

The above coordinated algorithm will increase the unique frame capturing by reducing the total overlap time.

D. A Coordinated Sniffer

Based on the channel sampling schedule, on each sniffer, channel instances are invoked for the specific duration. The channel sampling schedule will be given by sniffer controller dynamically.channel schedule will be changed on consideration of neighboring sniffer channel. Another important component is merger, Which is used to receive the streams of frames captured by the sniffers and to merge these into a chronologically consistent order, duplicate frames are removed , to enable analysis of the traffic. Fig. 4. shows coordinated sniffer architecture.

IV. HIDDEN MARKOV MODEL

The coordinated sampling approach is used to trace the traffic among multiple channels. These traces will be analyzed
by hidden markov model to infer the degree of selfishness of node in WLAN[2],asymmetry property on probability of deferral behavior among sender side nodes.

V. SAMPLING EXPERIMENTS

In this section, we are going monitor the traffic traces among multiple channels by using scheduling mechanisms.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

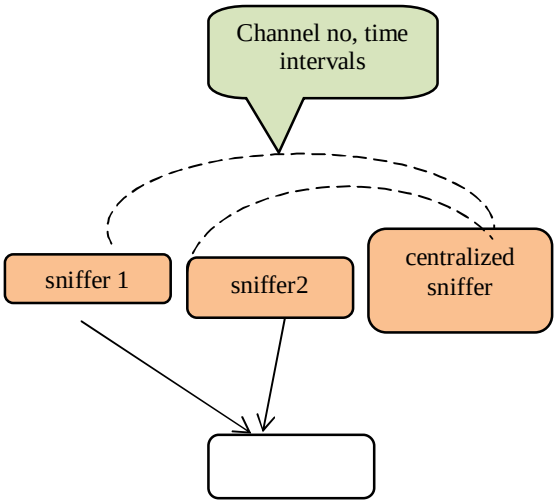

Fig. 4. Coordinated sniffer architecture.

A. Wireless Lan

The wireless LAN consists 5 to 6 access points as well as 20 to 30 client system. There are 5 sniffers placed among the wireless LAN. The access points will switch to the following channels 1,6,11. Based on schedule by centralized sniffer, sniffer1 will monitor the traffic traces on channel 6 for specific time period. During that time period sniffer 2 will monitor the traffic traces on channel 1. we can easily reduce the redundant frames over multiple sniffers using coordinated scheduling algorithm.

B. Results

The number of unique frames captured by both the Single channel and multi-channel collected and compared in 20 second intervals in Fig. 5.

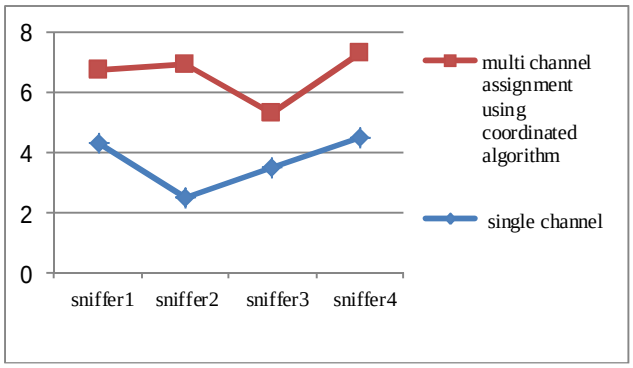

Fig. 5. Comparison between single and multi-channel Monitoring for unique frames at time t.

In multi-channel monitoring the no of unique frames is high compared to single channel monitoring. The no of redundant frames are reduced when the overlap time is minimized.co-ordinated scheduling algorithm will assign the channels dynamically to each sniffer with consideration neighborhood sniffer channel assignment which is used to reduce the overlap time between sniffers.

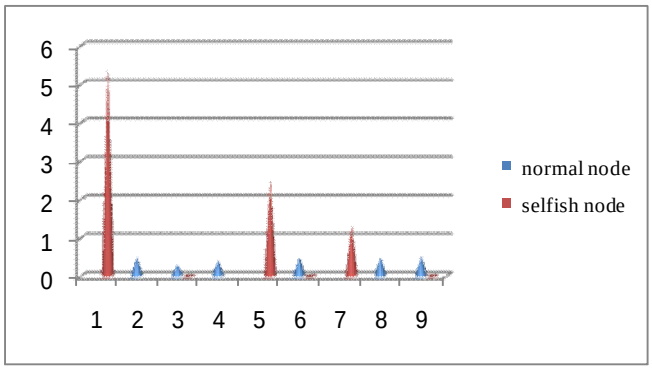

Fig. 6. Determination of selfish node with degree of selfishness

The unique frames are collected with the help of merger, collected traffic traces are analyzed by hidden markov model to predict the misbehavior node. selfish node identified with degree of selfishness among WLAN or wifi network. The selfish nodes 1,5,7 are identified over degree of selfishness among 9 nodes in Fig 6.

VI. CONCLUSION AND FUTURE WORK

The misbehavior node in WiFi networks detected by monitoring mechanism. In order to improve the

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization, Volume 3, Special Issue 1, February 2014

International Conference on Engineering Technology and Science-(ICETS'14)

On 10th & 11th February Organized by

Department of CIVIL, CSE, ECE, EEE, MECHNICAL Engg. and S&H of Muthayammal College of Engineering, Rasipuram, Tamilnadu, India

efficiency of wireless monitoring, multiple channels are monitored periodically to avoid the redundant frames. The monitored frames are merged, and then these traces are analyzed by machine learning approach[2].The degree of selfishness among misbehavior node identified. compared to existing method our approach reduces redundancy,increases the unique traffic traces.But complete traffic traces are not monitored only sample of traffic traces are gathered for each channel,we are focused to monitor the complete traffic traces with accuracy.

Our future work focuses on providing flexibility to applications so that the most relevant data can be made available by tuning the monitoring system to better meet the needs of the applications. Traffic trace analysis has been exploited by attackers to threaten user privacy in wireless networks.

REFERENCES

[1] A.P. Jardosh, K.N. Ramachandran, K.C. Almeroth, and E.M.Belding- Royer, "Understanding Congestion in IEEE 802.11b Wireless Networks," Proc. ACM SIGCOMM, 2005.

[2] U.Paul , AnandKashyap, S.R.Das, and R. Maheshwari, "Passive Measurement of Interference in WiFi Networks with Application in Misbehavior Detection" ,IEEE Transcations on mobile computing Vol 12,No 3.March 2013.

[3] P. Bahl et al., "DAIR: A Framework for Troubleshooting Enterprise Wireless Networks Using Desktop Infrastructure," Proc. ACM HotNets- IV, 2005.

[4] P. Bahl et al., "Enhancing the Security of Corporate Wi-Fi Networks Using DAIR," Proc. ACM/USENIX Mobile Systems, Applications, and Services (MobiSys), 2006.

[5] R. Mahajan, M. Rodrig, D. Wetherall, and J. Zahorjan, "Analyzing the MAC-Level Behavior of Wireless Networks in the Wild," Proc. ACM SIGCOMM, 2006.

[6] K.Pelechrinis,G.Yan,S.Eidenbenz,and S.V. Krishnamurthy,"Detecting Selfish Exploitation of Carrier Sensing in 802.11 Networks," Proc. IEEE INFOCOM, 2009.

[7] J. Yeo, M. Youssef, and A. Agrawala, "A Framework for Wireless Lan Monitoring and its Applications," Proc. Third ACM Workshop Wireless Security (WiSe), 2004.

[8] Jihwang Yeo, Moustafa Youssef, Tristan Henderson,and Ashok Agrawala. An accurate technique for measuring the wireless side of wireless networks. In Proceedings of the International Workshop on wireless Traffic Measurements and Modeling, pages 13–18, Seattle, WA, USA, June 2005.

[9] UdayanDeshpande,DavidKotz,Chris cDonal,"Coordinated sampling to improve the efficiency of wireless network monitoring",ICON 2007.

[10] Udayan Deshpande,Tristan Henderson,and David Kotz.Channel sampling strategies for monitoring wireless networks.InProceedings of the second workshop on wireless network measurements, Boston, MA,USA,April 2006,IEEE Computer Society Press.

[11] M. Cagalj, S. Ganeriwal, I. Aad, and J.-P. Hubaux, "On Selfish Behavior in CSMA/CA Networks," Proc. IEEE INFOCOM, 2005.

[12] S. Radosavac, J.S. Baras, and I. Koutsopoulos, "A Framework for Mac Protocol Misbehavior Detection in Wireless," Proc. ACM Workshop Wireless Security, 2005.

[13] J. Tang, Y. Cheng, Y. Hao, and C. Zhou, "Real-Time Detection of Selfish Behavior in IEEE 802.11 Wireless Networks," Proc. IEEE 72nd Vehicular Technology Conf. Fall (VTC-Fall), 2010.

[14] P. Kyasanur and N. Vaidya, "Detection and Handling of Mac Layer Misbehavior in Wireless Networks," Proc. IEEE Int'l Conf .Dependable Systems and Networks(DSN), 2003.