A DCF-Based Covert Timing Channel for IEEE 802.11 With Off-The-Shelf Wireless Cards

Sakthi V. Radhakrishnan, A. Selcuk Uluagac, and Raheem A. Beyah
Communications Assurance & Performance Group, The School of ECE, Georgia Institute of Technology
sakthi03@gatech.edu, {selcuk,rbeyah}@ece.gatech.edu http://www.ece.gatech.edu/cap

ABSTRACT

By using covert communication channels, an individual can hide messages and other information within regular traffic and can thereby circumvent security protocols. A promising area for covert channels is wireless networks. Specifically, those that employ carrier sense multiple access with collision avoidance (CSMA/CA) (e.g., 802.11 networks). These schemes introduce randomness in the network that provides good cover for a covert timing channel. Hence, exploiting the random back-off in the distributed coordination function (DCF), used to avoid collisions, we realize a relatively high bandwidth covert timing channel for 802.11 networks (Covert DCF). In this poster, we share our initial results from the implementation of Covert DCF using off-the-shelf Atheros-based 802.11 a/b/g wireless card.

COVERT COMMUNICATIONS

- **Hiding information within regular network traffic.**
- **Possible to bypass a Wireless Intrusion Detection System (WIDS) [1]**

Timing Channels

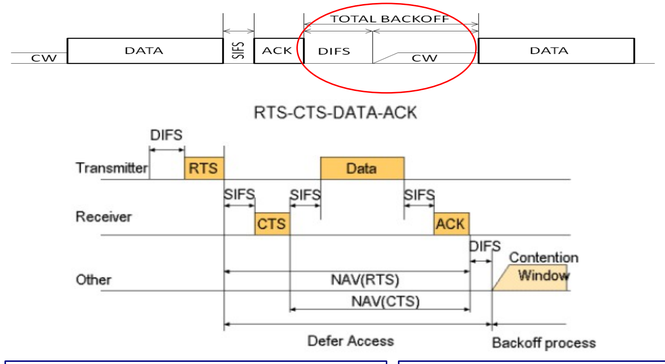
Use timing patterns to hide information

Storage Channels

Use storage medium to hide information

Our work → COVERT DCF

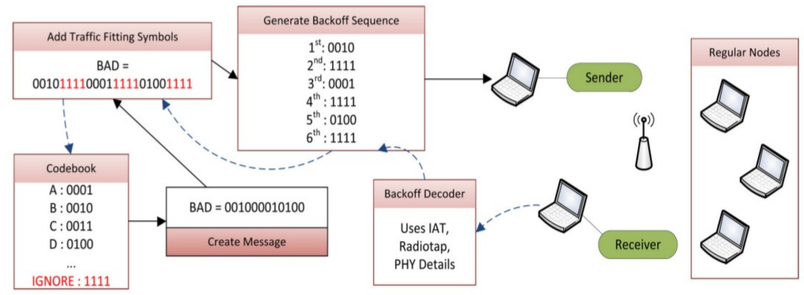
OVERVIEW OF 802.11 MAC



DCF:Distributed Coordination Function
CW: Contention Window
SIFS: Short Inter-frame Space
DIFS: DCF Inter-frame Space

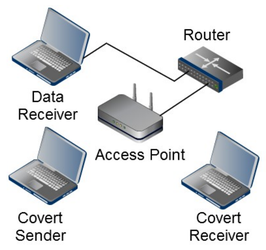
ACK: Acknowledgement
NAV: Network Allocation Vector
RTS: Request-to-Send
CTS: Clear-to-Send

COVERT DCF: CONCEPTUAL VIEW



- The sender and receiver agree on a pre-defined codebook mapping symbols from S = {} to a set of back-off values.
- For ex., let S = {0000; 0001; 0010; .. ; 1111} be associated with back-offs of {100µs,105µs,110µs,…,135µs}.

IMPLEMENTATION ON OFF-THE-SHELF WIRELESS CARDS

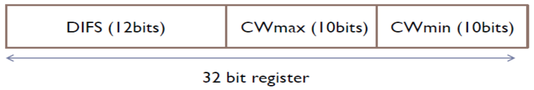


HARDWARE

Router: NetGear FVS338
Access Point: ZyXEL G-570S
Laptops: Lenovo C 100
WiFi Cards: Cisco Aironet
PCMCIA Cards: (Qualcomm Atheros AR-5212 Chipset)

SOFTWARE

Driver: Madwifi Trunk
O/S: Ubuntu 11.04 (Kernel 2.6.38)
Capture tool: *Tcpdump.*
Languages: C, Python



Actual Setup

Directly write into this register for each packet:
- *OS_REG_WRITE(ath_hal, addr, val);*
- *OS_REG_READ(ath_hal, addr, val);*
- *writel(val, Register_addr)*

PROCEDURES AT THE RECEIVER

STEP-I

Monitor
Observing the covert channel.

STEP-II

Filter
Filtering the intervals of interest.

STEP-III

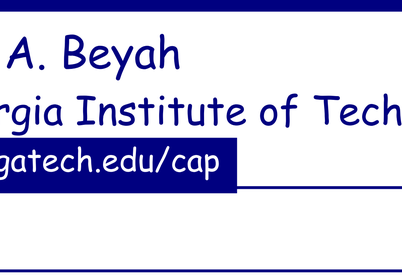
Process
Extracting the symbols from noisy back-offs.

STEP-IV

Translate
Converting the symbols into a bit stream.

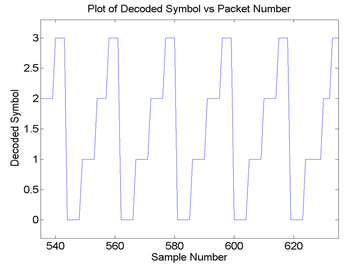
RESULTS

STEP-I



STEP-II

STEP-III



STEP-IV

...10 11 00 01 10 11 00 01 10 11 00 01 10 11 00 01 10 11 00 01 10 11...

- *17125 pkts in 15 seconds = 1142 pkts/sec*
- *2 bits per pkt → 2.28 Kbps throughput (no redundancy)*
- *Redundancy (50 pkts/symbol) added for errors. Hence, throughput: 46 bps (comparable schemes achieve 96bps 17 bps (only in simulations [2,3]!)*

ACKNOWLEDGEMENT

NSF DARPA

REFERENCES

[1] Russell Holloway and Raheem Beyah. "Covert DCF: A DCF-Based Covert Timing Channel in 802.11 Networks." The IEEE International Conference on Mobile Ad-hoc and Sensor Systems (MASS), October 2011
[2] T. Calhoun, R. Newman, and R. Beyah, "Authentication in 802.11 lans using a covert side channel," in IEEE International Conference on Communications (ICC)., jun. 2009, pp. 1 –6.
[3] S. Cabuk, C. E. Brodley, and C. Shields, "Ip covert timing channels: design and detection," in CCS '04: Proceedings of the 11th ACM conference on Computer and communications security. 2004, pp. 178–187.