Authentication in 802.11 LANs using a Covert Side Channel

Telvis E. Calhoun Jr., Reed Newman, and Raheem Beyah, *Members, IEEE*
Communications Assurance and Performance Group
Department of Computer Science
Georgia State University
Atlanta, GA, USA
{tcalhoun1@student, rnewman@student, rbeyah@cs}.gsu.edu

***Abstract*— We present a covert side channel technique that uses the 802.11 MAC rate switching protocol as cover for covert authentication messages. Covert authentication prevents an attacker from knowing when a user is authenticating and protects user credentials from malicious software attacks. Similar to port knocking, a remote client sends authentication messages to an access point in order to access a protected service. The technique uses a one-time password algorithm to protect against replay attacks. We investigate how the covert side channel affects node throughput in mobile and non-mobile scenarios. We also investigate the covertness of the covert side channel using standardized entropy. The results show that the performance impact is minimal and increases slightly as the authentication frequency increases. We further show that we can authenticate with 100% accuracy with minimal impact on rate switching entropy.**

***Index Terms*—steganography, covert channels, wireless networks, authentication, 802.11, rate switching**

I. Introduction

Covert channels encode information within a system where one or more of the system components act randomly. Such a system appears random to an observer, but a covert receiver can decode information from system behavior. A covert channel can use information hiding methods to hide data within an existing communication channel. Using the salt in a digital signature algorithm to leak private key information is an example of information hiding [1]. A covert channel can use a side channel by exploiting some system component that is not intended for communication. Using a wireless channel collision avoidance algorithm to transmit covert data is an example side channel technique. For either method, the exploited system must be non-deterministic, since deterministic protocols are certifiably free of covert channels [2]. All non-deterministic systems can be modeled as a set of states and state transitions that have a given probability. Therefore, any system that can be modeled as such is vulnerable to covert channels. Researchers have proposed different techniques to remove randomness from protocols in order to verify that a protocol is covert channel free [1-3].

Wireless networking protocols are vulnerable to covert channels due to randomness caused by the wireless environment. Factors such as mobility, RF interference or collision avoidance algorithms can contribute to non-determinism. In [3], Choi showed how the interaction between multiple protocols can produce non-deterministic behavior.

Rate switching protocols can be used as a covert channel. These protocols are designed to select a data rate that will achieve optimum performance for the current channel state. Rate switching algorithms can be modeled as a non-deterministic system where each data rate represents a state and the trigger events represent the probabilistic state transitions. Trigger events include: channel quality, frame loss, throughput or any other metric the protocol uses to detect channel state. Additionally, issues within the rate switching protocols can make them vulnerable to covert channels. Loiacono et al. [4] observed temporal differences in system performance caused by the so-called Snowball Effect. The Snowball Effect occurs when the rate switching algorithm selects a sub-optimal data rate for a given channel state. This starts a chain-reaction that leads to a period of unstable rate switching that degrades system performance. These unstable periods are triggered by the number of contending stations and the application traffic generated by the stations.

We present a technique that uses the 802.11 MAC rate switching algorithm as a covert channel for authentication messages between a station and access point. This scheme is used to access a protected service, such as a protected network port [5], that does not require authentication at start-up. Covert authentication prevents an attacker from knowing when a user is authenticating. The authentication algorithm generates one-time passwords [6] based on a shared secret and pseudo-random input. This prevents an adversary from breaking the security by simply stealing user credentials since both the pseudo-random input and private key are required to generate the one-time password.

A wireless station periodically injects a data rate sequence into the normal rate switching algorithm. The injected rate sequence, called a watermark, is derived from a one-time password and pseudo-random input. The pseudo-random input introduces non-determinism, making the watermarked rate switches appear as random as unstable rate switches initiated by the Snowball effect. The one-time passwords prevent replay attacks where an adversary could simply repeat a rate sequence to gain access to the protected service. We perform modeling and simulation to examine the overhead incurred by the covert channel in terms of node throughput (TCP and

UDP). We also examine how the covert channel affects rate switching entropy and the reliability of the covert channel.

The rest of the paper is organized as follows. In Section II we discuss related covert channel schemes. In Section III we examine the causes of non-determinism for various rate switching protocols. In Section IV we present the covert channel technique using rate switching. In Section V we discuss the simulations and results. Section VI discusses the conclusions and future work.

II. Related Work

A covert channel can allow a process to transmit data without any indication that the system has been compromised. Lampson [7] originally discussed covert channels as a potential vector to leak sensitive information. Covert channels have received considerable attention in the network security domain. Borders et al. [8] discuss how attackers use HTTP traffic as a covert channel to bypass security measures. Covert timing channels have been used to identify the source of interactive attacks that use intermediate hosts to mask the malicious source [9, 10].

Wang et al. [11] use a MAC splitting tree algorithm as a covert channel. The tree-splitting algorithm resolves collisions among active channel contenders. Colliding nodes are split into two subsets by randomly joining either the left or right subset. A splitting tree is created where the tree nodes are the collision resolution periods and the tree edges are the left or right subset selections. The station encodes a covert message as a sequence of subset selections. A covert receiver decodes the subset selections for a particular host to derive its covert message. They propose a secure algorithm that utilizes a 1-way hash to generate a temporal client key that is used to encode the message. The receiver generates the same key to decode the covert message. Though the overall technique is novel, tree splitting MAC protocols are not common in commercial wireless networks so the technique has limited practical use. Another disadvantage of this scheme is the need to transmit the nonce via a control packet, thus adding to the overhead of the scheme.

Kratzer et al. [12] use the 802.11 MAC header as a covert channel to communicate between two random WLAN hosts. The scheme modifies a MAC header field to send one or more covert bits per packet. The scheme modifies an erroneous bit which causes non-covert receivers to drop a packet while the covert receiver decodes the message. An alternate method is to modify the retry bit by duplicating a packet with retry bit set. A disadvantage of this scheme is that it requires two cover hosts to hide the covert communication channel. Additionally, the receiver must know the cover host identities and covert sender identities.

Our technique differs from previous work in several ways. First, our covert channel uses the MAC layer rate switching as a covert channel. This avoids the potential side effects of embedding information in MAC layer frames. Second, the technique uses the covert channel for authentication. The covert channel protects the authentication messages from detection by an adversary. Finally, our technique is designed to operate with currently deployed 802.11 devices.

III. Rate Switching Protocols

The objective of a rate switching protocol is to select a data rate value that will achieve optimum performance for the current channel state. The two basic metrics for determining channel state are signal quality and trigger statistics based on network performance. These trigger statistics include packet loss, delay or throughput. Algorithms that use packet loss, such as Autorate Fallback (ARF) [13] or Adaptive ARF (AARF) [14], adjust the date rate based on dropped frames, delay or decreased throughput. Loiacono demonstrated how wireless instability occurs regardless of the trigger statistic chosen [4]. Signal quality algorithms such as SGRA [15] and RBAR [16] measure the signal-to-noise ratio (SNR) or receiver-side signal strength (RSSI) to determine the optimum data rate. Zhang et al. [15] use an online calibration technique to correlate the frame delivery ratio to an SNR. Rate switches are performed on SNR thresholds rather than frame loss thresholds.

Commercial WLAN products implement various rate switching schemes that are based on the ARF algorithm. The implementations vary because the 802.11 specification does not define a rate switching algorithm. These commercial devices are vulnerable to the Snowball Effect caused by a failure to differentiate network congestion and channel degradation. As a consequence, rate switching algorithms can periodically decrease system performance through unstable rate switching as it attempts to respond to the channel state [4]. In our previous work [17], we observed this phenomenon in real-world networks and used the frequent rate switching as a means to identify 802.11 hardware. In response to unneeded rate switching caused by this issue, several alternatives have been proposed that can distinguish between congestion and channel degradation. However, detecting signal quality is difficult to do in practice due to calibration differences in wireless receivers [4, 15]. The difficulty in assessing the channel state increases the amount of rate switching that occurs in a typical wireless network and provides sufficient cover for a covert channel.

IV. Covert Channel using Rate Switching

This covert channel scheme uses the 802.11b rate switching algorithm as cover for authentication messages between a mobile station and an access point. Each station periodically computes a one-time password and encodes the password into a data rate sequence. The access point decodes the received rate sequence and authenticates the station.

A. Initialization

In the initialization phase, a trusted authority creates an initialization vector (IV) for each station. The IV serves several purposes. First, the IV synchronizes the password sequence generated by a station and the access point. Second, it assures that the each station generates a unique password sequence. Finally, the IV allows the access point to expire password sequences.

A trusted authority (TA) generates a 1024-bit master key (MK) using a cryptographically secure random function. Next, a trusted authority generates a 160-bit initial key (IK) based on a hash function, the master key and a client identifier such as a MAC address or serial number. At startup, each station seeds a common pseudo-random number generator with the initial key. It is essential that the PRNG is cryptographically secure so that the watermarks are sufficiently random. The common PRNG ensures that the station and access point generate identical sequences of random numbers. Next, each station creates the IV by concatenating the initial key and nonce. Finally, each station calculates a *one-time password*, which is the digest of the IV generated using a one-way digest algorithm like SHA. The one-way property assures that the IV cannot be derived from the password. The TA can invalidate old keys by updating the master key and generating new initialization vectors.

B. One-Time Password Generation

Each station uses a password generation function similar to S/Key [6, 18] to generate a one-time password used for authentication. This operation avoids repeated transmission of the same password by a single node. During this operation, the station generates a nonce from a common PRNG. To generate the next password, the client uses the cryptographic hash function, f(x), on the previous key concatenated by the nonce. The access point also performs this operation to maintain synchronization with the station.

C. Watermark Encoding

The station encodes the one-time password as a sequence of available data rates. This rate sequence is referred to as a *watermark*. The encoding scheme is based on the number of data rates available to the wireless networking protocol. For this experiment, we use four data rates available in 802.11b. The rates – 1Mbps, 2Mbps, 5.5Mbps and 11Mbps represent the bit combinations – 00, 01, 10 and 11, respectively. Figure 1 shows how a small 16-bit one-time password (0xFA51) is encoded into an 8-bit watermark.

D. Authentication Frequency

Authentication frequency determines the level of security provided by the covert channel. The covert authentication channel is designed to be a general authentication method that can provide various levels of security. Networks that require higher levels of security, such as corporate networks, will use more frequent watermarks. Conversely, networks that require less security may require less frequent watermarks.

To address this requirement, the administrator can specify a *maximum cycle length* that determines the maximum number

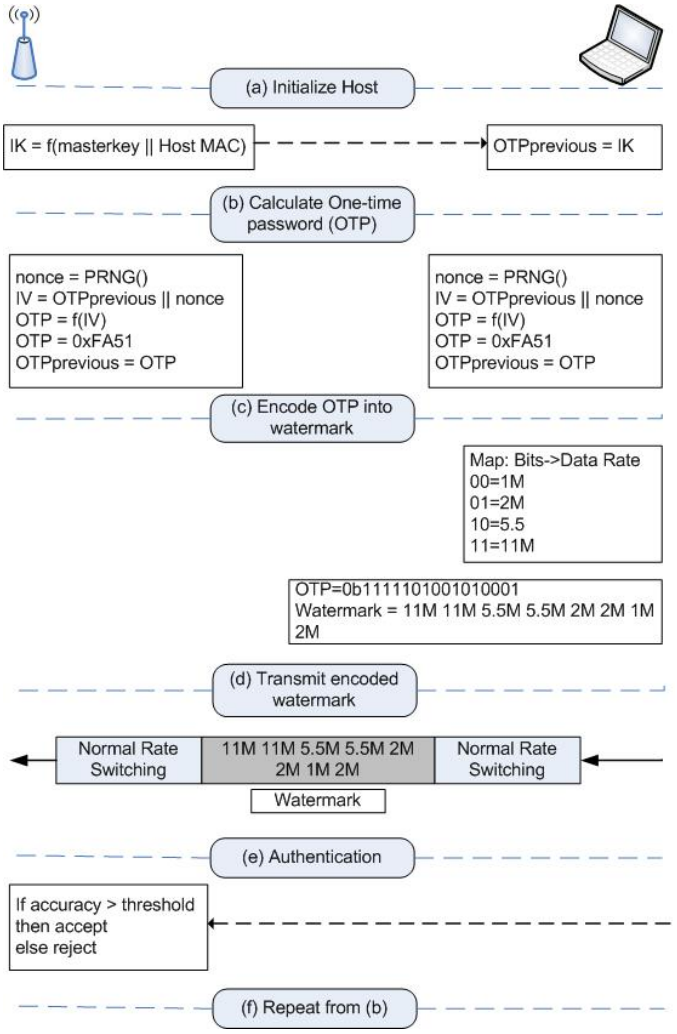

Figure 1. Watermark Encoding Process.

of successfully transmitted data frames between successive watermarks. The algorithm calculates a pseudo-random cycle length whose minimum value equals half the maximum cycle length. The random lengths prevent an adversary from knowing when a watermark begins and ends. The client and access point use a common PRNG to calculate the random cycle length in order to ensure synchronization.

E. Synchronization

The covert authentication channel uses 802.11 MAC sequence identifiers to synchronize the client and the access point. The MAC ID increments after each successfully acknowledged data frame. This allows the covert channel to calculate the beginning and end of watermarking intervals and detect MAC layer retries. This synchronization assures that no error occurs over the covert channel.

F. Decoding the Watermark

The access point stores data rates from each client in a watermark buffer by shifting in the most recently received rate and shifting out the oldest rate. The access point calculates the final MAC sequence ID for the watermark and then performs authentication when this sequence ID is detected. Successful authentication occurs when the decoded watermark matches

the one-time password for the watermark interval.

G. Covert Channel Overhead

Covert authentication overhead occurs when the covert channel chooses a data rate that is less than the optimal data rate for a given channel state. This results in decreased node throughput during the brief authentication cycle. Conversely, the covert channel may force a client to choose a higher data than it would choose otherwise. In mobile scenarios, this can potentially lead to packet loss when the radio range decreases at the higher rate. The amount of overhead can be mitigated by adjusting the authentication frequency.

H. Adversary Model

The adversary in our network is an unauthorized station that can passively monitor rate switching traffic and inject packets at will. The station identification data such as MAC addresses and serial numbers are assumed to be public. The adversary can only know the watermark length. The adversary cannot know when a watermark begins because the client randomly selects the cycle length for each watermark.

Rate switching entropy provides cover for watermarks and provides protection against passive attacks. The scheme is covert if the watermark has minimal impact on rate switching entropy over a given period. The one-time password algorithm ensures watermark entropy and prevents an adversary from guessing the watermark using some brute force technique.

V. Simulation and Analysis

A. Simulation Environment

We analyze how the covert authentication channel impacts node throughput and rate switching entropy. We also investigate how client mobility impacts the covert channel. The simulations were performed using the 802.11b model Qualnet Simulator 4.5. The 802.11 model uses a standard ARF algorithm that increases the rate after 10 successfully received ACK frames and decreases the rate after 2 missed ACK frames.

The wireless network consists of 14 wireless clients and 1 access point. The wireless clients generate continuous HTTP, FTP and constant bit-rate UDP traffic. The mean UDP throughput is approximately 4096 bps for 256-byte CBR packets generated every 500 ms on average. The mean TCP throughput is determined by the FTP and HTTP application models.

The maximum cycle lengths were varied to investigate how the authentication frequency impacts UDP and TCP throughput. The correlation between cycle length (measured in frames) and authentication frequency (measured in authentications/hour) was determined empirically. Only one client uses the covert channel technique during the experiments. This is done to isolate the impact of the covert channel. Future work will examine the performance impact of multiple covert channels. Figure 2 provides all of the simulation parameters.

Watermarking	
Maximum Cycle Lengths	10000 frames (~50 authentications/hr)
	20000 frames (~25 authentications/hr)
	40000 frames (~12 authentications/hr)
	80000 frames (~6 authentications/hr)
One-Time Password Length	160 bits
Wireless Network	
Number of Wireless Clients	14
Number of Access Points	1
Terrain Dimensions	400 x 400 meters
Simulation Time	1 hour
Wireless Clients Mobility	Stationary, 0.6 m/s
Mobility Model	Random Waypoint
MAC	
MAC Protocol	802.11b
1 Mbps Radio Range	442 meters
2 Mbps Radio Range	339 meters
5.5 Mbps Radio Range	328 meters
11 Mbps Radio Range	271 meters
HTTP Traffic	
Mean time between HTTP requests	25 seconds
Standard Deviation	5 seconds
FTP	
FTP File Size	10 MB
Constant Bit Rate (CBR) UDP Traffic	
CBR Packet Size	256 bytes
Mean Inter-packet delay	500 milliseconds
Standard Deviation	100 milliseconds

Figure 2. Simulation Parameters.

B. Throughput

The throughput of the authenticating station is impacted by the number of contending nodes, amount of data traffic generated by contending nodes, station mobility, link quality and the frequency of the covert authentications. Figures 3 & 4 illustrate how the authentication frequency impacts node throughput (UDP and TCP). Overall, the figures show that there is a minimal decrease in throughput relative to the baseline throughput and in some instances the watermark cycles increased the node throughput (indicated by the positive values on the graphs). The decrease in node throughput is a result of authentication attempts that require

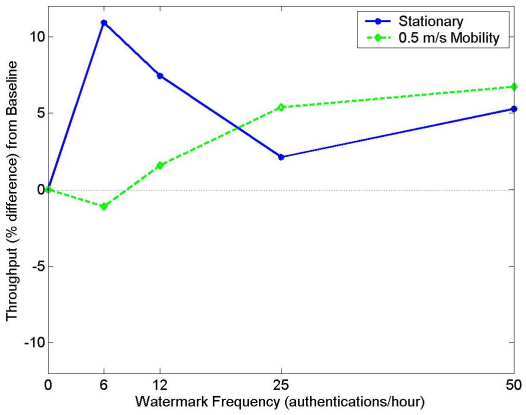

Figure 3. Percentage Difference in UDP Throughput vs. Watermark Frequency.

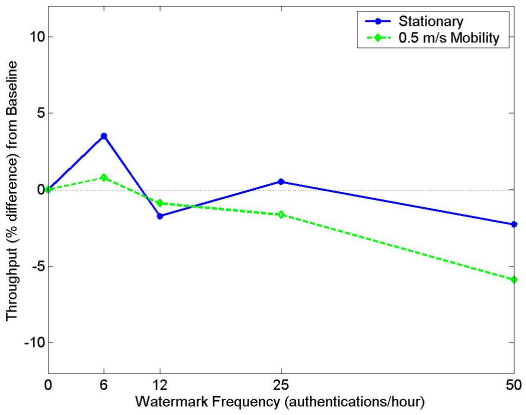

Figure 4. Percentage Difference in TCP Throughput vs. Watermark Frequency.

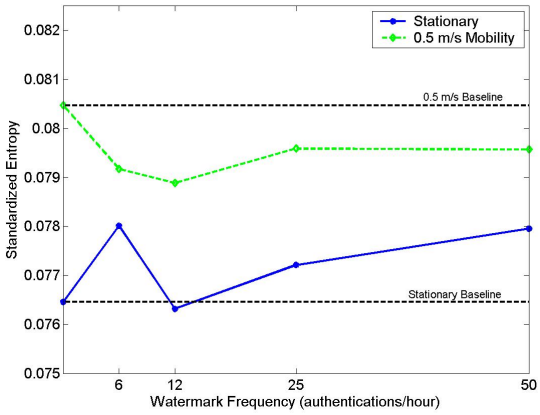

Figure 5. Overall Rate Switching Entropy vs. Watermark Frequency.

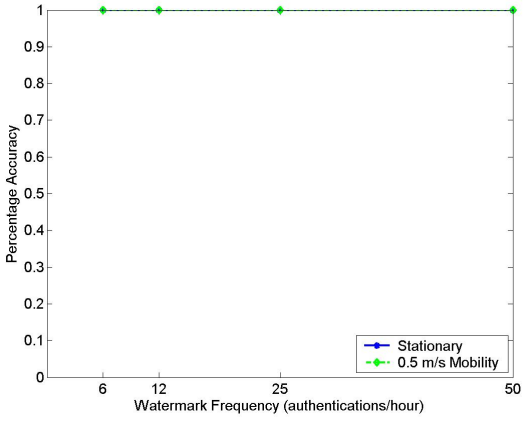

Figure 6. Authentication Accuracy vs. Watermark Frequency.

packets to be transmitted at specific rates when the rates were not available (e.g., when temporal RF interference would normally force the node to switch to 5.5 Mbps, 11Mbps is not available). This is temporary, and is shown to decrease the throughput by a maximum of 6% when authenticating at the highest frequency (50 authentications/hr). The increase in throughput is a testimony to ARF's sub-optimal performance (requiring unnecessary switches to lower rates) [4, 15, 16, 19]. During an authentication cycle, the covert side channel actually ignores ARF. Ignoring ARF during authentication negates its effect and increases the overall throughput.

Mobility also affects the amount of throughput degradation (or increase) seen by the authenticating node. Moving out of the range covered by the current rate normally triggers rate switching algorithms to select lower data rates (stronger encoding schemes) in order to continue communication. The covert channel degrades throughput by periodically selecting a data rate that is inconsistent with the current channel state (as mentioned above). Again, this temporarily leads to a minimal throughput degradation, or an increase in throughput as a result of ignoring ARF during authentication cycles.

The results also show that the covert channel impacts UDP more than TCP. The congestion control mechanism in TCP adapts to temporal differences in the wireless network state. This phenomenon is also observed by Choi [3]. UDP is an unreliable protocol and does not have a congestion control mechanism. Because of this, UDP cannot adjust to changes in wireless network state and incurs greater loss.

C. Entropy

In order to determine how covert our side channel is, we compare the entropy of normal flows with that of flows containing the watermarks. Rate switching entropy depends on the temporal characteristics of the network. Accordingly, this entropy level will fluctuate depending on the specific network. Thus, our goal is to have the entropy level of the watermarked flows closely follow that of the non-watermarked flows. Given that our technique thrives (becomes more covert) on rate switching for cover, we simulated the opposite scenario – one where rate switching is less frequent, making it harder for our scheme to be undetected. However, the simulation results show that the covert authentication channel has minimal impact on overall entropy, even for stable networks. The results in Figure 5 are a worse case, as the covert channel will become increasingly covert as the network has more frequent unstable periods.

As mentioned above, we apply an information theoretical

metric, standardized entropy [20], to measure the randomness of the rate switching and how the covert channel impacts this randomness. Let *rates* be the set of available data rates and F be the collection of rates selected for all data frames over a given interval. For each $rates_i$, $p_i := fi/f$, where fi is the number of frames transmitted at $rates_i$ and f is the number of frames in F.

$$SE(F) := \frac{-\sum_{i \in rates} p_i \log p_i}{\log f} \in [0,1], \quad (1)$$

According to (1), $-\sum_{i \in rates} p_i \log p_i$ is the entropy of the rate distribution and $\log f$ is its maximum entropy. Standardized entropy (SE) approaches 0 if a single data rate dominates the rate switching and approaches 1 as the rates become more evenly distributed. However, in this work the goal is to closely follow the entropy of the baseline, ensuring a robust scheme that can adapt to multiple network conditions.

Figure 5 compares the covert channel rate switching entropy to the baseline scenario where covert authentications are disabled. For stationary networks, the covert channel increases entropy up to 2%. Also, the entropy decreases as much as 2% for the 0.5 m/s mobility scenario. Both scenarios closely follow the standardized entropy of the non-watermarked flows, illustrating the covertness of the side channel.

D. Covert Channel Accuracy

As shown in Figure 6, the covert channel is 100% accurate for all authentication frequencies. This is expected since the client and access point use the MAC sequence identifiers to detect retries and for synchronization.

VI. CONCLUSION AND FUTURE WORK

We presented a covert authentication technique that uses 802.11 rate switching as a covert channel for authentication messages. We showed that commonly used rate switching algorithms are candidate covert channels due to randomness in the protocols. The simulation results show that the effects of the covert authentication channel on entropy and node throughput increase as the mobility increases and as the authentication frequency increases. The covert channel impacts UDP traffic more than TCP. The covert channel is 100% accurate due to synchronization using MAC sequence identifiers.

Future work will examine the effects of multiple covert channels and minimize the impact to rate switching entropy. We plan to apply this protocol to networks with a greater number of data rates, such as 802.11g, in order to increase covert channel throughput. We will also model the adversary to evaluate resiliency to active attacks.

ACKNOWLEDGMENT

We would like to acknowledge Scalable-Networks Inc. for supplying the university release of Qualnet 4.5 via the Qualnet University Program [21].

REFERENCES

[1] J. Y. Choi, G. Philippe, and J. Markus, "Tamper-Evident Digital Signature Protecting Certification Authorities Against Malware," in *Dependable, Autonomic and Secure Computing, 2nd IEEE International Symposium on*, 2006, pp. 37-44.

[2] D. V. Bailey, B. Dan, G. Eu-Jin, and J. Ari, "Covert channels in privacy-preserving identification systems," in *Proceedings of the 14th ACM conference on Computer and communications security* Alexandria, Virginia, USA: ACM, 2007.

[3] J. Choi, P. Kihong, and K. Chong-kwon, "Cross-Layer Analysis of Rate Adaptation, DCF and TCP in Multi-Rate WLANs," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, 2007, pp. 1055-1063.

[4] M. Loiacono, J. Rosca, and W. Trappe, "The Snowball Effect: Detailing Performance Anomalies of 802.11 Rate Adaptation," in *Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE*, 2007, pp. 5117-5122.

[5] R. deGraaf, J. Aycock, and M. Jacobson, Jr., "Improved port knocking with strong authentication," in *Computer Security Applications Conference, 21st Annual*, 2005, p. 10 pp.

[6] N. H. C. M. P. Nesser, "RFC-2289: A One-Time Password System," The Internet Society, 1998.

[7] B. W. Lampson, "A note on the confinement problem," *Commun. ACM,* vol. 16, pp. 613-615, 1973.

[8] K. Borders and P. Atul, "Web tap: detecting covert web traffic," in *Proceedings of the 11th ACM conference on Computer and communications security* Washington DC, USA: ACM, 2004.

[9] Y. J. Pyun, Y. H. Park, X. Wang, D. S. Reeves, and P. Ning, "Tracing Traffic through Intermediate Hosts that Repacketize Flows," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, 2007, pp. 634-642.

[10] X. Wang and D. S. Reeves, "Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays," in *Proceedings of the 10th ACM conference on Computer and communications security* Washington D.C., USA: ACM, 2003.

[11] Z. Wang, D. Jing, and R. B. Lee, "Mutual Anonymous Communications: A New Covert Channel Based on Splitting Tree MAC," in *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, 2007, pp. 2531-2535.

[12] C. Kratzer, D. Jana, L. Andreas, K. Tobias, and hne, "WLAN steganography: a first practical review," in *Proceedings of the 8th workshop on Multimedia and security* Geneva, Switzerland: ACM, 2006.

[13] A. Kamerman, Monteban, L., "WaveLAN-II: A High-perfromance wireless LAN for the unlicensed band," *Bell Labs Technical Journal,* vol. 10, p. 119, 1997.

[14] M. Lacage, M. H. Manshaei, and T. Turletti, "IEEE 802.11 rate adaptation: a practical approach," in *Proceedings of the 7th ACM international symposium on Modeling, analysis and simulation of wireless and mobile systems* Venice, Italy: ACM, 2004.

[15] J. Zhang, K. Tan, Z. Jun, W. Haitao, and Z. Yongguang, "A Practical SNR-Guided Rate Adaptation," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 2083-2091.

[16] G. Holland, N. Vaidya, and P. Bahl, "A rate-adaptive MAC protocol for multi-Hop wireless networks," in *Proceedings of the 7th annual international conference on Mobile computing and networking* Rome, Italy: ACM, 2001.

[17] C. Corbett, R. Beyah, and J. Copeland, "A Passive Approach to Wireless NIC Identification," in *Communications, 2006. ICC '06. IEEE International Conference on*, 2006, pp. 2329-2334.

[18] L. Lamport, "Password authentication with insecure communication," *Commun. ACM,* vol. 24, pp. 770-772, 1981.

[19] S. Lee and C. Kwangsue, "Channel Quality-based Rate Adaptation Scheme for Wireless Networks," in *Information Networking, 2008. ICOIN 2008. International Conference on*, 2008, pp. 1-5.

[20] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Profiling internet backbone traffic: behavior models and applications," in *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications* Philadelphia, Pennsylvania, USA: ACM, 2005.

[21] "Qualnet 4.5," Scalable Networks Inc., 2008.