Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2010

A Novel Design and Implementation of Dos-Resistant Authentication and Seamless Handoff Scheme for Enterprise WLANs

Isaac Lee
University of Canterbury,

Ray Hunt
University of Canterbury,

Originally published in the Proceedings of the 8th Australian Information Security Mangement Conference, Edith Cowan University, Perth Western Australia, 30th November 2010
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/91

A Novel Design and Implementation of Dos-Resistant Authentication and Seamless Handoff Scheme for Enterprise WLANs

Isaac Lee and Ray Hunt
Computer Security and Forensics Group
Department of Computer Science and Software Engineering,
University of Canterbury, Christchurch, New Zealand
isaac.lee@canterbury.ac.nz
ray.hunt@canterbury.ac.nz

Abstract

With the advance of wireless access technologies, the IEEE 802.11 wireless local area network (WLAN) has gained significant increase in popularity and deployment due to the substantially improved transmission rate and decreased deployment costs. However, this same widespread deployment makes WLANs an attractive target for network attacks. Several vulnerabilities have been identified and reported regarding the security of the current 802.11 standards. To address those security weaknesses, IEEE standard committees proposed the 802.11i amendment to enhance WLAN security. The 802.11i standard has demonstrated the capability of providing satisfactory mutual authentication, better data confidentiality, and key management support, however, the design of 802.11i does not consider network availability. Thus 802.11i is highly susceptible to malicious denial-of-service (DoS) attacks, which exploit the vulnerability of unprotected management frames. This paper proposes, tests and evaluates a combination of three novel methods by which the exploitation of 802.11i by DoS attacks can be improved. These three methods include an access point nonce dialogue scheme, a fast access point transition protocol handoff scheme and a location management based selective scanning scheme. This combination is of particular value to real-time users running time-dependant applications such as VoIP. In order to acquire practical data to evaluate the proposed schemes, a prototype network has been implemented as an experimental testbed using open source tools and drivers. This testbed allows practical data to be collected and analysed. The result demonstrates that not only the proposed authentication scheme eradicates most of the DoS vulnerabilities, but also substantially improved the handoff performance to a level suitable for supporting real-time services.

Keywords and phrases

IEEE 802.11i, 802.11r, 802.11w, Denial of Service attacks, Fast Access Point Transition Protocol, Access Point Nonce authentication, client puzzle, Quality of Service, Location Management Selective Scanning (LM-SS), handoff performance,

INTRODUCTION AND BACKGROUND

The IEEE 802.11i security standard [IEEE802.11i, 2004] provides an enhanced user authentication and strong data confidentiality to WLANs. However, the standard only concerns the protection of higher-layer data, i.e., IEEE 802.11 data frames, and the management frames used for connection administration are left unprotected. Hence, there is a wide spectrum of known attacks that are threatening to the WLAN security, particularly DoS attacks. Mitigation solutions for wired networks have been widely researched and studied. For example [Lee and Hunt, 2008] proposes an effective DoS mitigation solution for SIP systems. However, link-layer DoS attacks in WLANs have not been fully mitigated to a satisfactory level. Although the IEEE 802.11w amendment [Huang and Li, 2008] was subsequently introduced to further extend the data protection to the management frames, the experimental results in this current research show that the 802.11w protection is incapable of providing protection without causing severe performance degradation to the network under high rate flooding, and not all of the management frames can be protected with the 802.11w standard.

This research first examines the security of the IEEE 802.11i amendment and identifies some of the common link-layer DoS vulnerabilities. Experimental evaluations are performed to quantitatively measure the performance impact by DoS attacks that exploit those vulnerabilities. Mitigation requirements are analysed and some potential techniques to prevent spoofing and flooding activities are also discussed. Based on the results of this analysis, the paper first proposed a lightweight, stateless frame authentication scheme, called APN (Access Point Nonce) authentication, to address such DoS vulnerabilities.

The research further focuses on improving the existing handoff performance in order to achieve secure and seamless link-layer handoffs that can meet the QoS requirements of real-time multimedia applications. The handoff performance is improved by shortening both the re-authentication latency and the channel scanning delays in the discovery phase.

To achieve a faster scanning than the existing 802.11 active scan and secure roaming between APs with reduced re-authentication latency, a handoff scheme called Fast AP Transition Protocol (FATP) is proposed. Further, a location management based selective scanning (LM-SS) scheme is proposed.

Section 2 provides an analysis of the link-layer vulnerabilities in IEEE 802.11i while Section 3 proposed three mechanisms to improve protection against such DoS attacks. Section 4 describes the experimental testbed. Section 5 describes the experimental results which demonstrates that the combination of the LM-SS and FATP schemes provides a complete suite of handoff solutions that can offer promising results - particularly for real-time applications such as VoIP. Section 6 concludes the paper.

LINK-LAYER DOS VULNERABILITIES IN IEEE 802.11i

IEEE 802.1X/EAP and RADIUS allow the networks to authenticate clients based on credentials (e.g., username and password) rather than MAC addresses, which can be easily spoofed. Although this provides the flexibility of allowing authentication and key management functionality to be implemented without modifications to the existing IEEE 802.11 MAC sub-layer, this, however, opens up vulnerabilities for flooding attacks because there is no link-layer authentication and filtering capabilities. Moreover, the upper layer authentication exchange is stateful, so unprotected EAP frames are also vulnerable to flooding attacks.

This suggests that the lack of per-packet authenticity and integrity in IEEE 802.11 management frames is a key factor in many of the security problems as flooding-based DoS attacks primarily exploit the lack of authenticity in management frames. Therefore, authenticity and integrity of management frames needs to be protected and assured in order to mitigate those DoS vulnerabilities.

Accordingly the IEEE 802.11w working group is proposing cryptographic-based protection mechanisms to secure management frames. Those mechanisms are very similar to the protection of data frames using the keys derived for TKIP (Temporal Key Integrity Protocol) or CCMP (Counter Mode CBC-MAC Protocol). However, there are some limitations in the current version of 802.11w. First, all management frames sent or received by a station before keys are derived are unprotected. Secondly, 802.11w does not explain how to protect authentication and association request frames. Neither does it address how to prevent flooding attacks. Further, research work such as [4] has demonstrated that the 802.11w standard is effective only for low rate deauthentication and disassociation DoS attacks. Large-volume flooding with management frames against an AP can still lead to a DoS condition due to the heavy workload and overhead for computing the cryptographic key processes required to authenticate the spoofed frames.

PROPOSED LINK-LAYER DOS PROTECTION MECHANISMS

A lightweight, stateless frame authentication scheme

A lightweight, stateless frame authentication scheme, called APN (Access Point Nonce) authentication is proposed to address such DoS vulnerabilities. A RSN (Robust Secure Network) association can be established using this APN authentication instead of the existing Open System authentication - which actually provides minimal security. This has the advantages of simplicity, compatibility with the standard involving few modifications, as well as low computation overhead and bandwidth utilisation.

Experimental results demonstrate that with a small increase in the initial connection delay, the APN authentication scheme is able to effectively identify between legitimate and spoofed traffic, with minimal computation cost due to the efficient “client puzzle” verification mechanism proposed [Rui, 2009]. This frame verification process allows the AP to drop the spoofed frames under flooding conditions without affecting legitimate users’ application traffic.

In this proposed APN authentication scheme, the AP issues each client requesting network access a unique client puzzle. A client puzzle, formulated using a secret only known to the AP, timestamp, and an AP generated predictive nonce (i.e., APN) computed using some client specific information, is a solvable cryptographic problem a client must resolve in order to have the AP or network server resource allocated for its connection. A legitimate client who knows the pre-shared secret is able to determine the puzzle solution without spending extra resources solving it, whereas an attacker would have to spend a significant amount of time solving a puzzle for each request frame transmitted in order to launch a flooding attack. The APN authentication also provides a means to allow the client and the AP to authenticate subsequent layer 2 frames, including management frames and EAP messages, with a technique that uses the hard factorisation principle [RSA, 2002].

The proposed APN authentication procedure is shown in Figure 11 and is based upon a dialogue involving prime numbers (P_s and Q_s), client's MAC address together with its cryptographic hash function, an identity tokens (Ns and N_A) which are the product of the two prime numbers, a secret that is only known to the AP, and the current timestamp (t). The APN hash function generation is shown below:

APN = h (MACs, Ns, SECRET, t)

The APN provides a binding between the client's MAC address and its identity token. However, MAC addresses cannot be trusted in WLANs, so this binding needs another layer of protection to ensure the identity token is mapped to a legitimate identity. This is achieved by embedding the APN in a client puzzle so that it is bound to the trusted shared key of the client which can solve the puzzle.

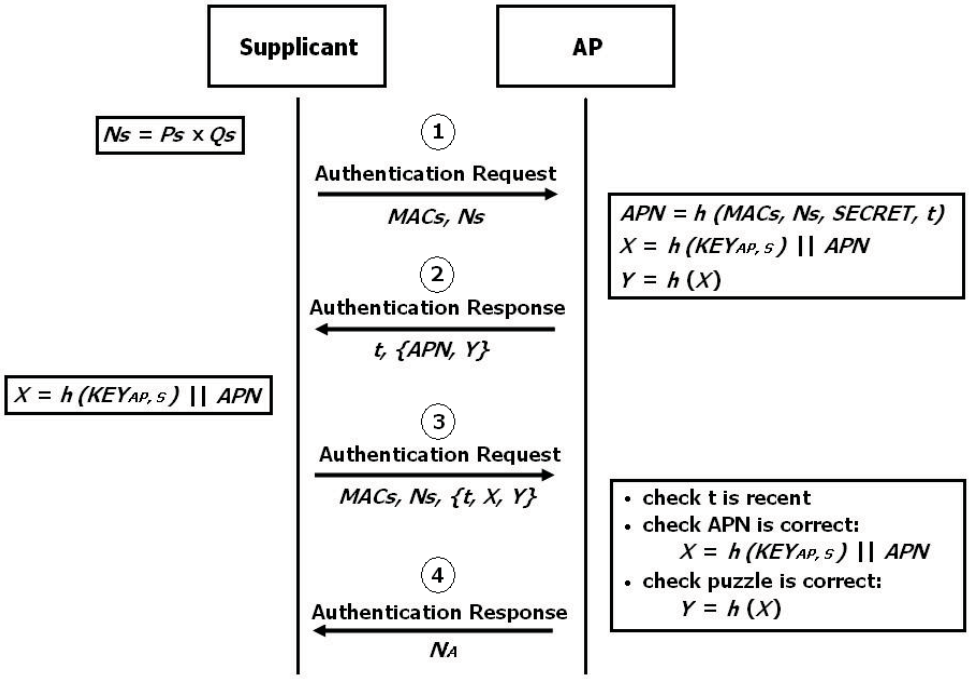


Figure 11: The proposed APN authentication procedure

To provide a binding between the APN and the identity of the client without trusting its MAC address, which can easily be spoofed, the AP validates the client by challenging it with a puzzle constructed in a way that a legitimate client who knows the key shared by the AP and client or supplicant (s) (denoted as KEYAP,S) can easily solve it. To do this, the AP first generates a pre-image by hashing the client's shared key and concatenating the output with the APN, then a puzzle image Y is computed by hashing the pre-image:

Pre-image: X = h (KEYAP,S) || APN

Image: Y = h (X)

To set the puzzle difficulty, the first 128 bits (i.e., the key digest part) of X is removed, which effectively means that the APN itself is used as the partial pre-image (x) that forms the puzzle together with Y. This client puzzle construction process is shown in Figure 2, where the shaded bitstrings represent the puzzle.

After constructing the puzzle, the AP attaches the timestamp and the puzzle in an authentication response frame and sends it to the client as demonstrated as message 2 in Figure 1. The client then obtains the puzzle from the received response frame and computes the puzzle solution by hashing the shared key. Because only the legitimate client knows the shared key, solving the puzzle involves nothing more than generating the key digest, meaning that only one hash operation is needed. After solving the puzzle, the client transmits another authentication request, shown as message 3, which contains the same identity token and timestamp, together with the puzzle solution (X and Y). The AP will check that the timestamp is recent and the puzzle solution is valid (i.e., the APN matches the last 128 bits of X). If all the checks are successful, the client is considered legitimate and will be allowed to proceed with stateful operations such as association and upper layer authentication.

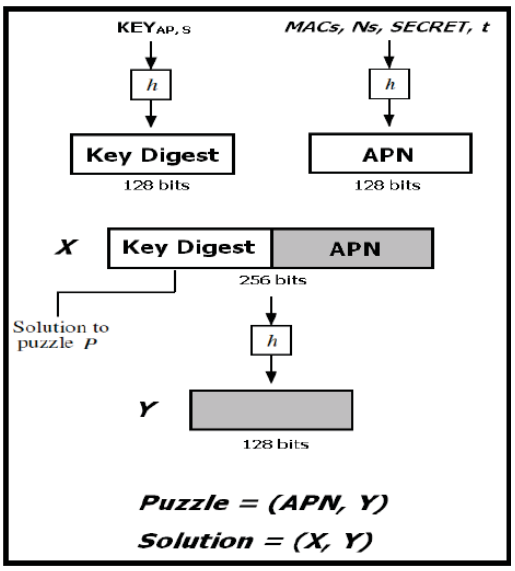


Figure 2: APN Client puzzle construction process

For a subsequent frame to be authenticated after a successful APN authentication exchange, the sender encrypts one of its validating key (either *P* or *Q*) using the shared key and attaches the encrypted validating key in the frame. Before accepting the frame, the recipient decrypts the validating key using the same shared key, looks up the sender's identity token (*N*), and validates it with the decrypted validating key. If the validation fails (i.e., the validating key does not divide N), the recipient drops the frame. Similarly, an AP can also provide authenticity in its broadcast frames by including its validating key in the frame which is encrypted with the group key. This group key is the result of a successful group-key handshake, which happens immediately after the 4-way handshake. Thus all clients that are authenticated to the AP though 802.1X will share this group key with the AP. This provides an effective protection against DoS attacks such as deauthentication or disassociation flooding that can spoof a legitimate AP's MAC address.

A fast handoff transition protocol scheme

The existing link-layer handoff schemes in WLANs are classified into five categories: and shown in Figure 3, viz (1) full authentication, (2) full authentication with lightweight EAP method, (3) proactive key distribution (PKD), (4) pre-authentication, and (5) IEEE 802.11r Roaming [IEEE802.11r, 2008]. Most are designed to shorten the 802.11i re-authentication delay by the means of pre-distributed keys or predicting client movement but the challenge is how to achieve fast re-authentication at a low cost without compromising the 802.11i level of security.

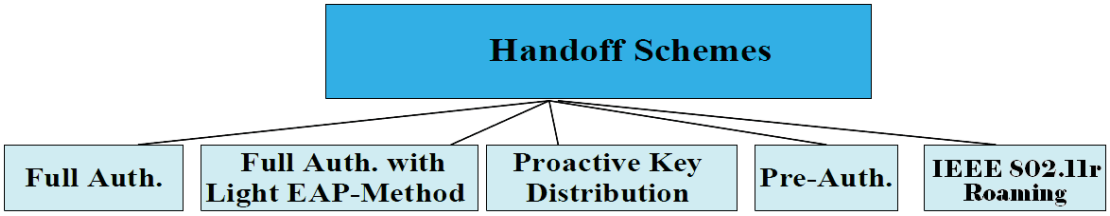


Figure 3: Classification of existing handoff schemes

To achieve a secure roaming between APs with reduced re-authentication latency, a handoff scheme called Fast AP Transition Protocol (FATP) is proposed. The FATP is a proactive key distribution-based handoff scheme which delivers new session keys from the client's current associated AP to the target AP prior to handoff. In order to achieve the same level of security as the 802.11i standard, the three-tier key hierarchy used in the IEEE 802.11r is adopted in the FATP scheme for managing and associating new security keys for handoff sessions.

The FATP implements the 802.11i protocol paradigm: authentication (i.e., to establish a trust relationship) first, and then re-association (i.e., to change AP attachment). Based on this paradigm, the FATP scheme comprises two stages: trust transfer prior to handoff and fast re-association after moving to the new AP. 4 shows a high level concept of the FATP scheme.

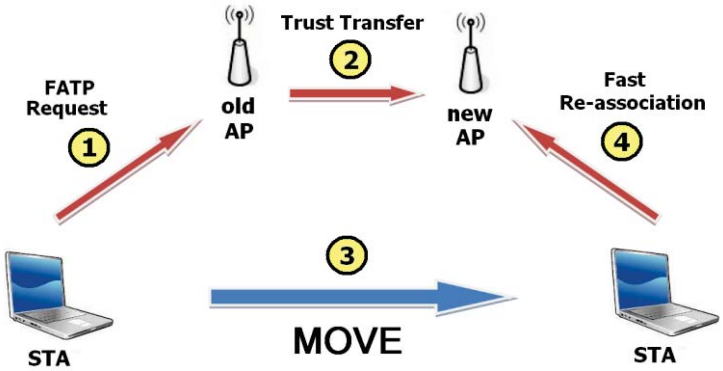


Figure 4: Top level concept of the proposed FATP handoff scheme

One of the major differences between the proposed FATP solution and the IEEE 802.11r roaming standard lies in the proposal of an early execution of the four-way handshake prior to handoff with the FATP [Lee, 2010]. This allows the FATP to achieve a faster re-association with the new AP, and thus, the handoff latency and packet loss can be further reduced compared to the performance of the 802.11r roaming. More importantly, the FATP supports the re-generation of the security parameters used by the APN authentication so that the subsequent link-layer frames can still be authenticated using the refreshed keying material in new handoff sessions. The experimental results in Section 4 show that the FATP scheme can achieve considerable reduction in handoff latency whilst providing the same security level as a full 802.1X authentication.

A location management-based selective scanning scheme

The scanning phase poses the most significant challenge for seamless handoffs in WLANs. Most of the existing 802.11 implementations only attempt to scan when a client's link quality degrades to a point where connectivity is threatened. Further, with the considerable delay and overhead associated with the 802.11 active scanning, the total handoff latency, during which incoming packets are dropped, is typically well over 500ms to a second, where 90% of the delay comes from the scanning phase. The result is far beyond what can be tolerated by real-time multimedia applications such as VoIP.

To achieve a faster scanning than the existing 802.11 active scan, a location management based selective scanning (LM-SS) scheme is proposed. In this LM-SS scheme, a location server is introduced to maintain the AP topology information, and a roaming client can be informed of the presence of nearby APs, and therefore determine the number of channels required to scan from the AP topology information provided by the location server. Figure 5 illustrates the proposed location management mechanism. Although the focus of this research is on intra-domain handoffs, this scheme can also be applied to manage inter-domain (i.e., across different subnets) handoffs.

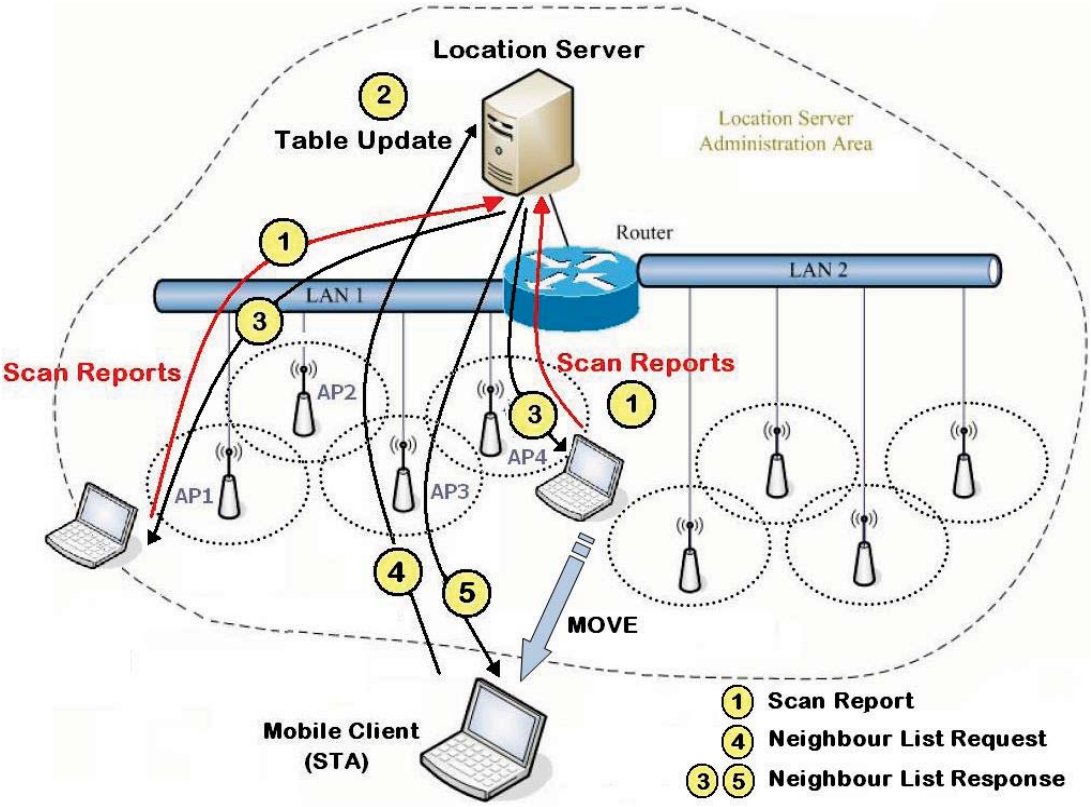


Figure 5: Proposed Location Management Scheme and Network Structure

To eliminate the waiting time spent in each channel scanned, a cross-layer probing technique utilising unicast probe requests and IP-based probe responses is proposed. The packet buffering mechanism provided by the existing 802.11 power saving mode is used as a signaling mechanism for buffering packets while the client is performing probing activities on other channels. This prevents packet loss during the scanning process. The scanning delay of the proposed LM-SS scheme can be determined by the following equation:

$$\textbf{Scanning delay} = CS \times (n + 1) + tprobe \times n$$

where *CS* is the channel switching delay, *n* is the number of channels to scan, and *tprobe* is the time required to send a probe request on a channel.

From the experimental measurements, the average tprobe was found to be close to 1.3ms. Hence, the expected scanning delay for scanning a certain number of channels can be calculated with the above equation, and the scanning delays are plotted in Figure 6. The scanning delay is linearly dependant on the number of channels to scan, so there will not be time wasted on probing channels that are empty. The specific channels that are required to be probed are reliably provided by the location server after the client associates to an AP.

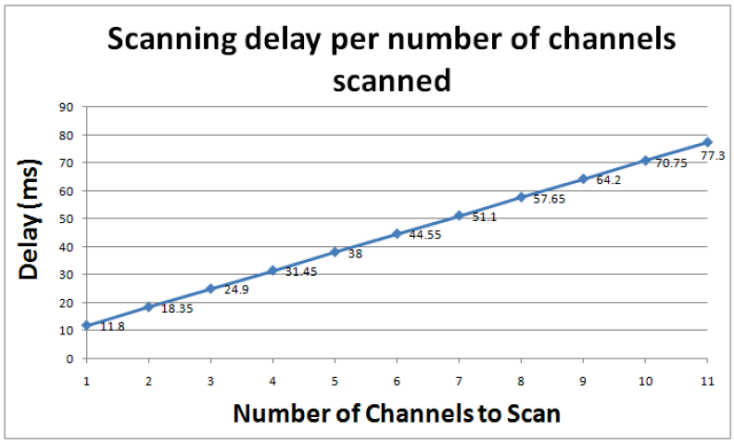


Figure 6: LM-SS scanning delay per number of channels scanned

With the frame protection provided by the APN authentication scheme, together with the fast handoff transition protocol and location management-based selective scanning schemes most of the DoS attacks can be mitigated while at the same time providing a greatly enhanced handoff performance.

DESIGN OF THE TESTBED

To quantify the impact of DoS attacks on the throughput of wireless networks, a WLAN testbed is constructed to provide an experimental framework for measuring the effects of DoS attacks. As the Linux open source community is growing rapidly, the fully functional 802.11i testbed built for this research use the Linux operating system and open source wireless device drivers and tools. The testbed is configured to use EAP-TLS as the upper layer authentication method and CCMP mode of AES for data encryption.

The experimental setup consists of multiple APs connecting to the same subnet with the same ESSID, two wireless clients (supplicant), a wired traffic generator station (for generating network traffic), a RADIUS authentication server, and a wireless monitor station that captures the wireless frames transmitted in the network. The testbed represents a simplified version of an enterprise WLAN infrastructure and has the following properties that the proposed schemes rely on: the architecture of the WLAN network consists of multiple APs interconnected via a high-speed switched network so that efficient broadcast/multicast communications is available at layer two. In addition, APs are deployed within overlapping radio ranges of each other so continuous wireless coverage is available over the testing areas. A dedicated switch is installed for efficient communications between APs. Figure 7 shows the basic structure of the testbed.

All the stations are running on Pentium 4 (2.26 GHz CPU) machines with 512 MB RAM. Linux kernel 2.6.25 is installed on those machines. NTP (Network Time Protocol) is run on all stations to synchronize their clocks in order to allow accurate measuring and analysis of traffic latency and delay.

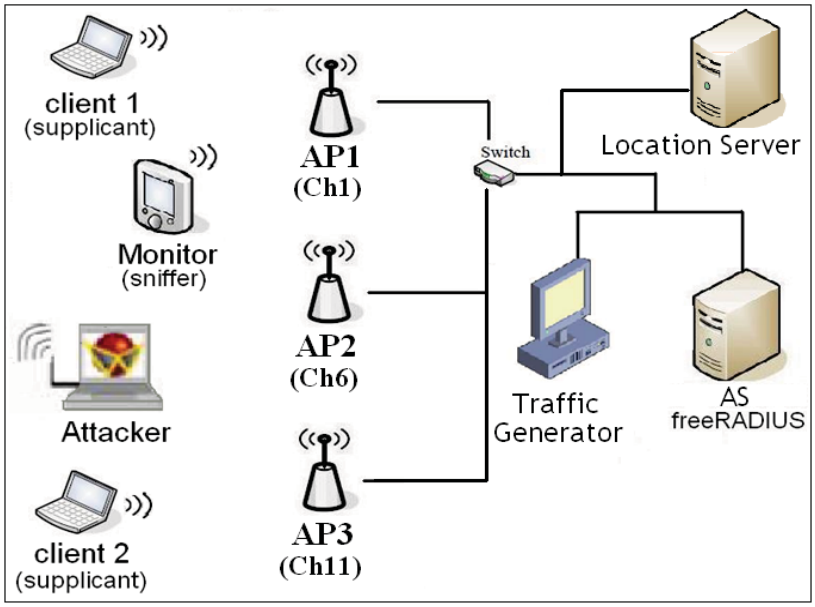


Figure 7: Testbed environment for the evaluation of the proposed schemes

The RADIUS server, which provides authentication and authorisation, is implemented using the open source tool - freeRADIUS[3]. Wireshark, is installed on the monitor station to analyse the captured frames. All the wireless stations, including the monitor, location server, attacker and the two APs, are equipped with a D-Link DWL-G520 PCI wireless adapter card, which utilises Atheros AR5002G chipsets to provide IEEE 802.11g (2.4GHz) wireless access and hardware encryption functions (e.g., AES) for IEEE 802.11i security. The Madwifi driver (v0.9.4), which is a Linux kernel device driver for Atheros chipsets, is installed on those machines. Figure 8 shows the software architecture of the overall implementation.

[3] http://freeradius.org/

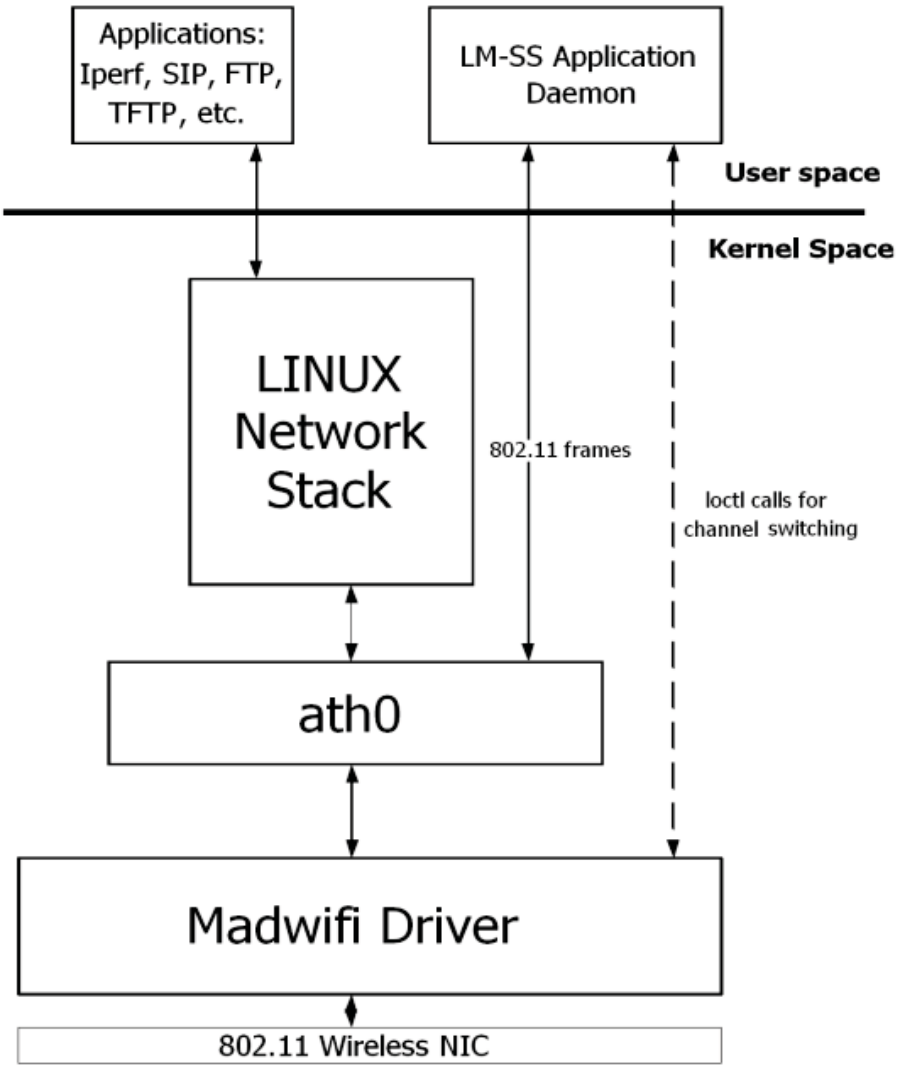


Figure 8: Software architecture of the implementation

RESULTS

This section provides the results obtained from analysis of the testbed studies for APN (Access Point Nonce) authentication as well as the scanning delays associated with the new handoff schemes LM-SS (Location Management-based Selective Scanning) and FATP (Fast AP Transition Protocol).

APN (Access Point Nonce) authentication scheme

Instead of using Open System authentication, APN authentication is used during the initial stage of a RSN association establishment. The complete APN authentication involves a four-message exchange (Figure 11). The authentication process comprises four main tasks that will incur delays: client preparation (i.e., generating P, Q and N), puzzle construction at the AP, puzzle solving at the client, and puzzle verification at the AP. Depending on the length of the identity tokens used in the exchange, the overall authentication latency can vary significantly. Generating primes requires computation time in the order of seconds, and hence, as a proof of concept implementation pseudo-primes are used to allow faster computation.

For the testbed implementation, 256-bit identity tokens are used because they provide enough key space to prevent cracking of validating keys within the required timeframe while the overall authentication latency is relatively short. Table 6 shows the delay components of a 256-bit APN authentication. The results are the average of 20 authentications.

Complete APN Authentication Overhead (Based on 256-bit Identity Token)	
Task	**Time (ms)**
Client: Preparation	12.5736
AP: Puzzle Construction	0.0452
Client: Puzzle Solving	0.0129
AP: Puzzle Verification	0.0247
Transmission and RTT	3.1916
Total:	**15.848**

Table 6: Break down of 256-bit N authentication latency

From this table it is clear that the major source of delay comes from the computation of validating keys in the client preparation phase, while the second comes from the frame transmissions and the Round Trip Time (RTT). Because of the lightweight nature of APN authentication, the puzzle construction, solving, and verification can be done very quickly with trivial delays. With the 256-bit identity token based APN authentication, the average overall latency is about 15.85ms. Comparing this delay to the existing initial network connection time (i.e., performing full scanning plus 802.11/EAP-TLS) of almost 1.5 seconds, the APN authentication introduced only about 1% increase to the network connection time.

Figure 9 shows the AP's CPU utilisation under the flooding condition. Without the APN authentication scheme, the CPU load is almost 80% under the flooding condition. This is because the AP was responding to the spoofed requests and allocating resources. On the other hand, with the APN authentication scheme enabled, the CPU utilisation is less than 40% under the same flooding condition. The significant reduction comes from the ability provided by the APN scheme to effectively identify spoofed frames and discard them without storing state information. A similar level of CPU load reduction was also found with other types of flooding attacks.

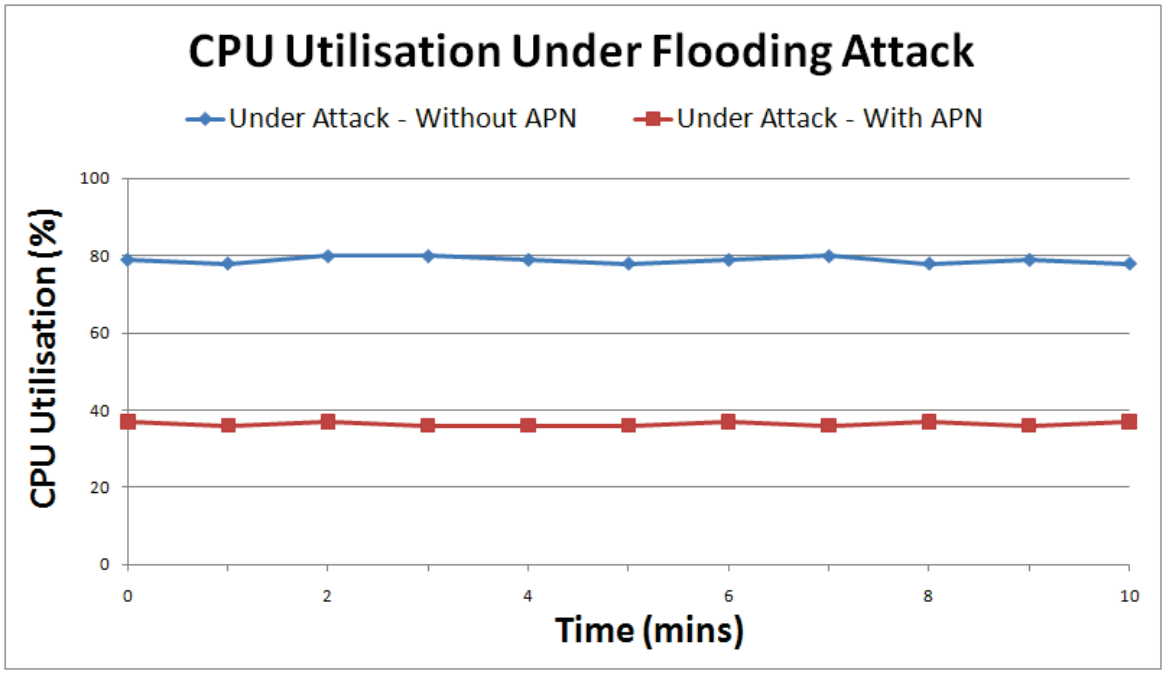


Figure 9: APs CPU utilisation under flooding condition

Because without the APN authentication scheme the AP was not able to identify spoofed requests and actually responded to them, the memory usage under the authentication flooding attack continued to increase, as shown in Figure 10. With the APN authentication scheme enabled, the AP's memory usage remained steady.

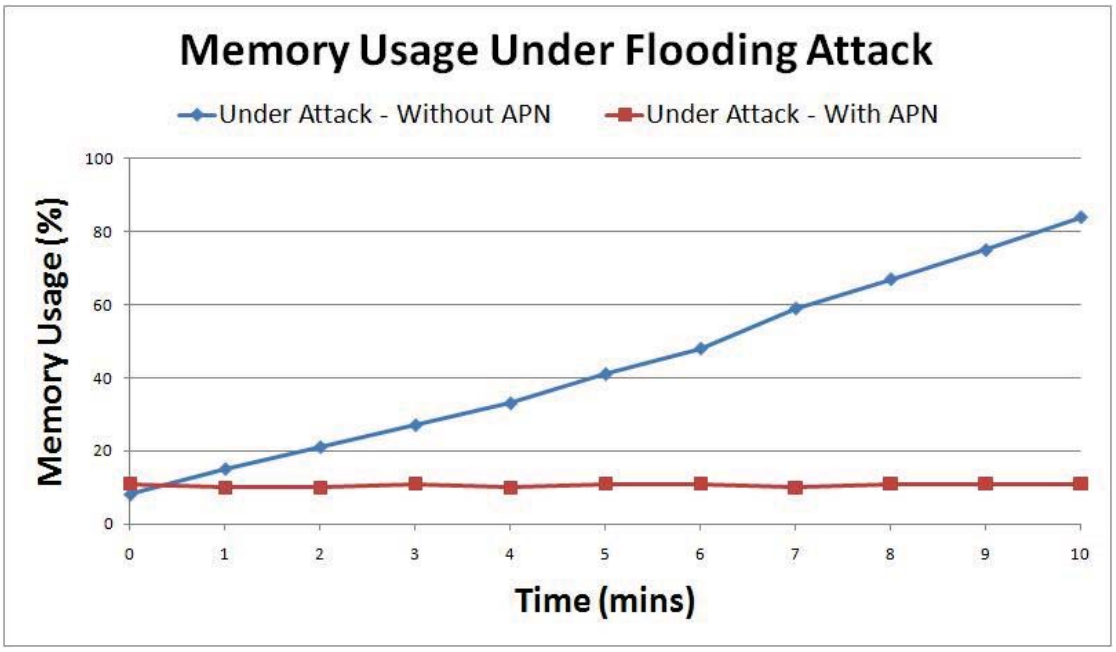


Figure 10: AP's memory utilisation under flooding condition

Handoff performance using (LM-SS and FATP) schemes

Experiments were conducted to compare the scanning delay with different AP densities versus different scanning methods. Three scan methods were tested: 802.11 active scan, selective scan, and LM-SS. The selective scan is the time required to perform active scan to probe only the channels used by neighbouring APs. The inclusion of the selective scan here allows the benefit of using IP-based probe responses to be evaluated, as the LM-SS scheme without utilising IP-based probe responses is equivalent to the selective scan.

The results show that the active scan has the longest and fixed average delay. This is because all available channels were scanned without regard to the presence of neighbouring APs. Selective scan has a reduced average delay because the number of channels to scan is reduced to the number of neighbouring APs. LM-SS further reduced the delay by using IP based probe responses as the waiting time in each channel is eliminated. The results are the average of 10 runs and Figure 11 graphically compares the results obtained from the three scenarios.

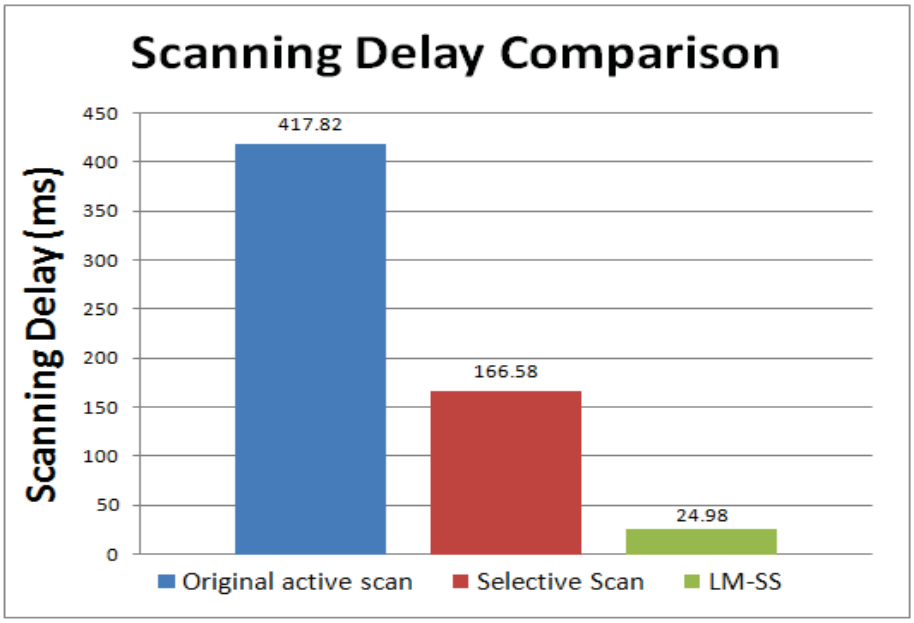
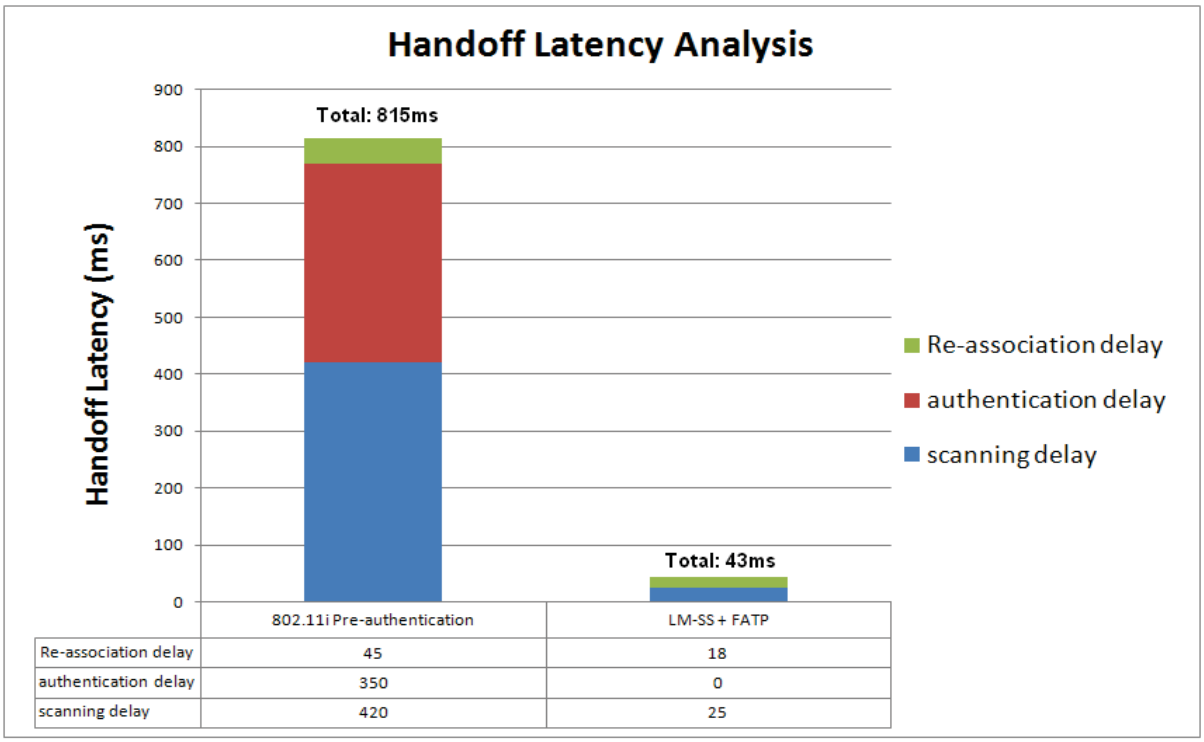


Figure 11: Three-channel scanning delay comparison

Because of the proactive nature of the FATP scheme, the handoff latency only comprises the scanning delay (as in Figure 6) and the FATP fast re-association delay. Based on 10 handoff experiments performed in the testbed, the average fast re-association delay was measured to be 18ms. Hence, the possible range of the actual handoff latency would be between 30ms to 95ms, depending on the number of channels to scan.

The performance of the FATP handoff scheme is compared with the existing 802.11i pre-authentication scheme (using EAP-TLS. Figure 12 shows the different components that constitute the actual handoff latency. The major portion of the delays comes from the scanning phase. With the LM-SS scheme, the result indicates that the scanning delay is significantly reduced. Because with FATP the pre-authentication and context transfer are done prior to handoff while the client is still connected to its current AP, the FATP authentication delay does not contribute to the actual handoff latency, whereas the 802.11i pre-authentication incurs an authentication delay of around 350ms. The FATP scheme also has a reduced re-association delay because the four-way handshake is not required.



	802.11i Pre-authentication	LM-SS + FATP
Re-association delay	45	18
authentication delay	350	0
scanning delay	420	25

Figure 12: Handoff latency components and comparison

For this comparison, the scanning delay is excluded and only the (re)authentication delay of those handoff solutions are considered. The result is shown in Figure 13. With the original 802.11 handoff, a complete 802.1X/EAP-TLS authentication was performed, which results in the longest authentication delay. With the 802.11i pre-authentication, the delay was reduced to 350ms. This is because most of the authentication work was done through the current AP prior to the disconnection of the client. With the 802.11r fast transition scheme, performance evaluations [Ahmed and Hassanein, 2008] have shown that a fast transition requires 40 to 50ms (excluding scanning delays). The proposed FATP scheme only took 18ms, which is the time required to execute the fast re-association with the new AP.

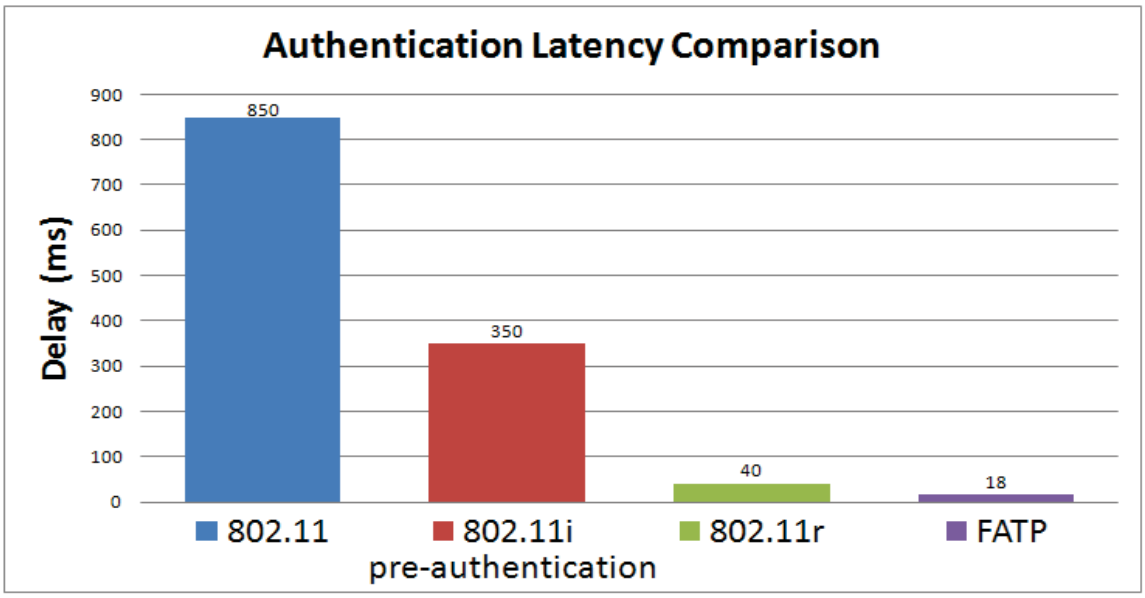


Figure 13: Handoff latency comparison between different handoff schemes

With the FATP, a roaming client's context information has already been transferred to the new AP prior to disconnection, so the client can directly re-associate with the new AP without needing to negotiate with the authentication server (RADIUS). This significantly reduces the authentication delay. Compared with the 802.11r, the further improved performance comes from the fact that with the FATP scheme the PTK security association between the new AP and client has already been established locally prior to handoff, so the fast re-association phase does not need to perform the four-way handshake, whereas the 802.11r sill requires a four-way handshake in order to complete the key setup.

CONCLUSION

IEEE 802.11i security standard provides an enhanced user authentication and strong data confidentiality to WLANs. However, the standard only concerns the protection of higher-layer data, i.e., IEEE 802.11 data frames, and the management frames used for connection administration are left unprotected leaving the way open for a variety of DoS attacks. Although the IEEE 802.11w amendment was later introduced to further extend the data protection to the management frames, the experimental results in this research showed that the 802.11w protection is incapable of providing protection without causing severe performance degradation to the network under high rate flooding, and not all of the management frames can be protected with the 802.11w standard.

Based on the results of analysis, the paper first proposed a lightweight, stateless frame authentication scheme, called APN authentication. The paper further focuses on improving the existing handoff performance in order to achieve secure and seamless link-layer handoffs that can meet the QoS requirements of real-time multimedia applications. The handoff performance is improved by shortening both the re-authentication latency and the channel scanning delays in the discovery phase. To achieve a secure roaming between APs with reduced re-authentication latency, a handoff scheme called Fast AP Transition Protocol (FATP) was proposed. Finally, to achieve a faster scanning than the existing 802.11 active scan, a location management based selective scanning (LM-SS) scheme was also proposed.

The experimental results demonstrated that the combination of the LM-SS and FATP schemes is a complete suite of handoff solutions that can provide promising results to real-time applications such as VoIP. Further, with the frame protection provided by the APN authentication scheme, the infrastructure can effectively mitigate most of the DoS attacks while at the same time achieving enhanced handoff performance.

Further research work will be required to fully extend the FATP scheme to support handoffs between multiple domains. The APN authentication and the FATP handoff scheme both require the client to generate prime numbers for the computation of identity tokens and validating keys. The computation time for generating large prime numbers can be significant and to the detriment of efficient handoff. Because of this, the implementation actually uses pseudo-primes instead, thus the optimisation of large prime computation will significantly improve the efficiency of these schemes. Other areas of future research include extension of the trust model beyond the authentication server, effects of speed of mobility during handoff and improving the flexibility that triggers scanning and operation of the FATP.

REFERENCES

IEEE 802.11i-2004, http://standards.ieee.org/getieee802/802.11.html.

Lee, I. and Hunt, R., A novel design of a VoIP firewall proxy to mitigate SIP-based flooding attacks, Int. J. Internet Protocol Technology, vol. 3, pp. 128-135, 2008.

IEEE 802.11w-2009 management frame amendment to IEEE 802.11, http://standards.ieee.org/getieee802/download/802.11w-2009.pdf, 2009.

Huang, C. and Li, J., A Context Transfer Mechanism for IEEE 802.11r in the Centralized Wireless LAN Architecture, presented at Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference, 2008.

Rui, Z. et al, A generic construction of useful client puzzles, in Proceedings of the 4th International Symposium on Information, Computer, and Communications Security. Sydney, Australia: ACM, 2009.

RSA Cryptography Standard, http://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf, 2002.

IEEE 802.11r-2008 (Fast Basic Subset Transition) secure roaming amendment to IEEE802.11 http://standards.ieee.org/getieee802/download/802.11r-2008.pdf, 2008.

Lee, I., A Novel Design and Implementation of DoS-Resistant Authentication and Seamless Handoff Scheme for Enterprise WLANs, Masters Thesis, www.cosc.canterbury.ac.nz/research/reports/MastTheses/#year2010, MAST 01/10, 2010.

Ahmed, H. and Hassanein, H., A performance study of roaming in wireless local area networks based on IEEE 802.11r, Communications, 2008 24th Biennial Symposium pp. 253-257, 2008.