

# WiMAX環境下分散式阻斷服務攻擊偵防之研究

白宗祐、林清同

E-mail: 9708158@mail.dyu.edu.tw

## 摘要

西元2001年IEEE公佈802.16標準，然而WiMAX安全規範的核心是基於MAC層通訊協定的安全子層，不過駭客依然可以透過建立惡意的基地台端來強行與用戶終端進行連接，這是在WiMAX環境下必須進一步解決的問題。分散式阻斷服務攻擊將攻擊方式延伸為分散式的攻擊方式，入侵者可以同時控制若干台殭屍電腦對目標伺服器發動攻擊。本研究將採用VI作為認證標記，以防止Mobile WiMAX網路可能受到的DDoS攻擊。我們將透過有採取VI機制和沒採取VI機制的系統的比較的例子觀察在DDoS攻擊下採用VI能減低DDoS所造成的系統負擔。

關鍵詞：全球互通微波存取；分散式阻斷攻擊 分散式阻斷攻擊；殭屍電腦

## 目錄

中文摘要	iii	英文摘要	iii
iv 誌謝辭		v 內容目錄	
vi 表目錄		viii 圖目錄	
ix 第一章 緒論	1	第一節 研究背景	1
1 第二節 研究動機	4	第三節 研究目的	4
7 第二章 文獻探討	8	第一節 WiMAX的安全性	8
8 第二節 802.16 D3版本的安全機制	11	第三節 DDoS攻擊概述	11
16 第四節 D DDoS攻擊體系結構	18	第五節 DDoS攻擊工作原理分析	21
21 第六節 攻擊步驟	21	第七節 DDoS攻擊類型與分析	23
23 第八節 DDoS攻擊工具分析	24	第九節 常見DDoS攻擊	27
27 第十節 DDoS的發展	27	第十一節 Idle模式和Location Update	29
29 第十二節 BS和ASN GW上的DDoS攻擊	29	第十三節 NS-2模擬WiMAX環境	31
31 第十四節 設計NIST WiMAX模組架構	33	第十五節 WiMAX模擬設計	37
37 第三章 WiMAX環境下防禦DDoS攻擊	42	第一節 引言	42
42 第二節 VERIFY INFORMATION	42	第四章 模擬和分析	45
45 第一節 模擬概述	45	第二節 NS2模擬DDoS攻擊	49
49 第三節 VERIFY INFORMATION過程	51	第五章 結論與研究建議	53
53 第一節 結論	53	第二節 後續研究建議	53
53 參考文獻	53	表目錄	54
54 表目錄 表 1- 1 無線網路技術比較表	2	表 2- 1 無線網路比較表	13
13 表 2- 2 DDoS攻擊所採用的協定類型分散圖	17	表 2- 3 常見DDoS攻擊	27
27 表 2- 4 國內外WiMAX MAC模擬模組功能比較表	32	表 2- 5 NIST WiMAX模組功能表整理	33
33 圖目錄 圖 2- 1 直接攻擊	19	圖 2- 2 反射攻擊	20
20 圖 2- 3 Trin00運作原理圖	26	圖 2- 4 NIST 802.16 MAC NS-2物件類別圖	34
34 圖 2- 5 NIST 802.16 MAC NS-2訊框結構關係圖	35	圖 2- 6 NIST WiMAX NS-2各封包流入流出處理流程	37
37 圖 2- 7 CGU-III WiMAX模組系統架構圖	38	圖 2- 8 CGU-III WiMAX模組關係圖	40
40 圖 3- 1 驗證資訊的過程	43	圖 4- 1 模擬流程示意圖	48
48 圖 4- 2 系統遭受DDoS攻擊流量示意圖	50	圖 4- 3 遭受疑似攻擊啟動防禦機制	51

## 參考文獻

Beomjoon, K., Jaesung, P., & Yong-Hoon, C. (2006). Power saving mechanisms of IEEE 802.16e: Sleep mode v.s. idle mode. Computer Science, 4331, 142-149. Burness, A. L. (2005). Mobility, wireless and QoS. BT Technology Journal, 23(2), 12-23. Bellardo, J., & Savage, S. (2003). 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In P. Usenix (Ed.), Security Symposium. Washington, U.S.A.: D.C. CERT

Coordination Center. (2001). Distributed denial of service tools [Online]. Available: [http://www.cert.org/incident\\_notes/IN-99-07.html](http://www.cert.org/incident_notes/IN-99-07.html) [2001, January 15]. Daniel, S. (2006). WiMax operator ' s manual. Apress, 9, 187-194. Dittrich, D. (2007). The tribe flood network distributed denial of service attack tool [Online]. Available: <http://staff.washington.edu/dittrich/misc/tfn.analysis.txt> [2007, July 10]. Gupta, V., Krishnamurthy, S., & Faloutsos, M. (2002). Denial-of- service attacks at the MAC layers in wireless. Ad Hoc Networks, Anaheim, U.S.A.: California. Jeffrey, G. A., Arunabha G., & Rias M. (2007). Fundamentals of WiMAX. New York: Prentice Hall, 26-30. Lee, P. C., Bu, T., & Woo, T. (2007). On the detection of signaling DoS attacks on 3G wireless networks. Anchorage: Alaska. Liang, W., & Wang, W. (2005). Quantitative study of authentication and QoS in wireless IP networks. U.S.A.: Miami. Ng, H. S., Sim, M. L., & Tan, C. M. (2006). Security issues of wireless sensor networks in healthcare applications. BT Technology Journal, 24(2), 184. Power, R. (2002). Computer security issues & trends. 2002 CSI/FBI Computer Crime and Security Survey, 8(1), 1-12. Syed, A. A., & Mohammad, I. (2007). WiMAX: Standards and security. CRC: Press, 78-80. Song, J. H., Vincent, W., S. W., & Victor, C. M. L. (2007). Secure position-based routing protocol for mobile ad hoc networks. Ad Hoc Networks, 5(1), 76-86. Song, J. H., Poovendran, R., Lee, J., & Iwata, T. (2006). The AES-CMAC algorithm. IETF RFC, 4493, 176-287. Thomas, H., & Lakshminath, R. D. (2005). Security in Wireless LANS and MANS. Artech House Publishers, 30, 132-137. Zhang, M., & Fang, Y. (2005). Security analysis and enhancements of 3GPP authentication and key agreement protocol. IEEE Trans on WIRELESS COMMUNICATIONS, 4(2), 734-742.