



二．項目簡介

(項目所屬科學技術領域、主要技術內容、授權專利情況、技術經濟指標及應用推廣情況)

本項目為產學研合作項目，屬於計算機學科中的網絡安全、計算機網絡以及模式識別領域。

資訊與網絡已成為社會的關鍵基礎設施，如同交通、金融以及能源一樣。我們的工作生活與網絡資訊越來越密，隨之而來的網上犯罪行為也越來越多，尤以網絡入侵危害最甚也最為廣泛。根據《卡巴斯基公司 2010 年度安全統計報告》顯示，在 2010 年整年，全世界的攻擊偵測系統（IDS）錄得 1,311 億次網絡攻擊，這一數字在 2009 年為 220 億，增長迅速。中國互聯網絡信息中心與國家互聯網應急中心發布的《2009 年中國網民網絡信息安全狀況調查系列報告》顯示，2009 年，52% 的網民曾遭遇過網絡安全事件，其中 21.2% 的網民帶來直接經濟損失，按國內 3.84 億網民計算，人均處理網絡安全事故費用約為 40 元，共損失 153.6 億人民幣。可見網絡安全問題對社會造成的危害之廣泛。

IDS（入侵檢測系統）是保證網絡安全的有效方法，目前 IDS 大多數是企業級和主機級，企業級 IDS 是一個獨立硬件系統，相對比較昂貴，維護成本高，可防護的網段有限。主機級 IDS 為入侵偵測軟件，安裝在個人電腦上，存在軟件 IDS 的“功能悖論”^[1]，即病毒、蠕蟲、惡意軟件或木馬透過電郵、網上文件下載、移動存儲設備（例如 U 盤）入侵個人電腦，加上有一些電腦沒有及時更新特徵數據庫或對系統進行補丁（patch），導致主機受到病毒感染或蠕蟲入侵（Local Infection），從而引起 IDS 軟件運作失效，進而導致網絡漏洞暴露。還有個別情況下，安裝在個人電腦上的防毒軟件或防攻擊軟件容易與個人電腦上的其它軟件不兼容，導致失效。因此主機類 IDS 軟件存在不穩定性及脆弱性。

可見，目前硬件 IDS 價格昂貴不適合廣泛推廣，軟件 IDS 又存在著功能悖論。因此，開發一種價格低廉，獨立運作的硬件 IDS，顯然有很大市場價值。嵌入式防火牆或 IDS 一直受到工業界學術界的重視，許多研究^[2-5]提出不同的方法來解決主機型 IDS 所面對的問題。但是一直沒有提出一個產品。

本發明針對上述問題進行了技術突破，利用體積較小成本較低的嵌入式開發平臺，基于模式識別技術 SVM 分類器算法，研發出一種小型化的、獨立用於個人電腦使用的網絡攻擊偵測器。目前項目從專利設計到產品功能設計實現方面，完成了以下一些技術創新點。

1、**國內目前體積最小的硬件 IDS。**根據《廣州市科技查新諮詢中心出具的國內查新報告編號：12KJCX0399》，（見附件），本項目產品為國內報導的最小型的入侵檢測系統（IDS），適合個人電腦使用。本產品原型體積為 32mm(H) x 32mm(W) x 62mm(L)，約三分之二個名片盒般大小。

2、**POE 供電，可以迅速佈防。**專利中提出採用 POE 技術，項目組設計了一個可供研發樣品使用的，支持以太網供電的 POE 接口，利用 POE（Power on Ethernet，網綫供電）技術供電，不需外接電源，系統可通過網綫獲得電力。這一功能大大提高產品的便攜性，在偵測黑客的過程中，可以在缺乏電源插座的區域，迅速布下攻擊偵測器。本項設計目前已納入專利保護，以及在實驗室中實現了，由於研發經費有限，在測試樣品中尚未實施，

3、**基於 SVM 分類算法並降低特徵變量維度。**《卡巴斯基公司 2010 年度安全統計報告》指出，當中最常見的前五種攻擊行為是 Intrusion.Win.NETAPI.buffer-overflow.exploit（42.49%）、

DoS.Generic.SYNFlood (30.54%)、Intrusion.Win.MSSQL.worm.Helkern (20.02%)、Scan.Generic.UDP (3.46%) 以及 Intrusion.Win.DCOM.exploit (1.08%)。上述四種攻擊行為佔所有攻擊行為總數的 97% 屬於帶漏洞掃描式攻擊及 DoS (Denial of Service, 拒絕服務) 類攻擊。針對這些常見攻擊行為，可以在現有的模式識別方法的基礎上，進行 SVM 分類器的特徵維度降低工作，從 41 維降低到 11 維，以降低算法計算量，提高偵測速度及準確度。

經過兩年半的研發，本項目已研製出有關硬件及算法軟件，獲得兩項實用新型專利，一項澳門科學技術發展基金資助項目，一項企業研究資助，建立了一個網絡安全測試環境的嵌入式系統的開發平臺，產品原型目前正在邀請用戶對產品進行測評，已獲得一定數量的測評意見 (見附件)。兩項專利中，《一種便攜式網絡入侵檢測裝置》是有關產品硬件設計的專利，《一種級聯融合式網絡入侵檢測系統》是有關產品軟件設計的專利。



產品外觀

(字數不超過 1200 字)