東海大學電機工程學系

碩士論文

可抵禦攻擊之無線感測網路能耗管理機制

Secure Power Management Scheme for WSN

研究生:王昱元

指導教授:蔡坤霖 博士

中華民國一零五年六月

東海大學電機工程學系碩士學位

考試委員審定書

電機工程學系研究所 王昱元 君所提之論文

可抵禦攻擊之無線感測網路能耗管理機制

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：張延任 (簽章)

委 員：蔡坤霖

陳坤志

陳立偉

鍾玉梅

中 華 民 國 105 年 06 月 03 日

致謝

在進行研究以及寫作論文的過程中，歷經了許多人的幫助，要感謝的人非常多。首先要感謝我的指導教授蔡坤霖老師，在研究的過程中指引我方向，並傳授寶貴的研究經驗，讓我解決實驗中的難題，順利完成研究。除此之外，老師平常培養我解決問題的能力，並給予我關心與鼓勵，使我在研究所期間獲得成長，在此致上最深的感謝與敬意。

感謝我的同學益豪與鉦新，和我一起學習與研究，並在實驗時給予我幫助。感謝我的學長又禎和柏翰，教我待人處事的圓融。感謝實驗室的學弟景成、冠圻、修華、宇辰，時常陪我討論並提供意見。還有實驗室的承瀚、郁淩，感謝你們平常的陪伴與幫助。有這麼多人的幫忙才能讓我的論文能夠順利完成。

最後要感謝我的家人，在研究所期間給予我支持與鼓勵，讓我無後顧之憂的進行學習，並在我遭遇瓶頸時給予關心，使我重拾繼續前進的勇氣，我才能夠順利度過難關，完成學業。謹以此篇論文獻給所有關心並幫助我的人，祝福你們快樂與安康。

摘要

近年來，無線感測網路（WSN）已被廣泛應用於軍事、醫療和科學環境上，而其感測器通常都是由電池作為供應電源。因此，要如何延長無線感測網路的生命週期是一項重要的挑戰。但要實現這一點，我們必須考慮到無線感測網路的所有設計和通訊。其中，電源管理是能減少感測器能耗有效的方法之一。此外，電源管理可能在無線感測網路被駭客攻擊時失控。因此，我們提出了一個安全能耗管理方案，命名為可抵禦攻擊之無線感測網路能耗管理機制來處理無線感測網路的能源問題，並延長以及協調其感測節點的運行時間。最重要的是，在被攻擊的期間，此機制仍然能持續運作，而且，在無線感測網路節點處於空閒狀態時，我們提的方法能有效地使節點進入休眠狀態，然後在必要的時候喚醒他們，因此能使得節點消耗的能量更少。實驗模擬結果顯示，當被惡意攻擊時，與典型的電源管理方案相比，我們的方法仍能有效降低功耗。

關鍵字：功率管理、無線感測網路、安全性、惡意攻擊、收支相抵點、低功耗

Abstract

Recently, wireless sensor networks (WSN) have been widely used in military, healthcare, and scientific environments and their sensors are often powered by batteries. So how to lengthen WSN's lifetime is an important challenge. One of the solutions is reducing sensors' energy consumption. Power management in turn is one of effective methods for lowering their consumed energy. But to achieve this, we must take into account all design and communication stages of a WSN. Also, the power management may be out of control when the WSN is now being attacked by hackers. Therefore, in this paper, we proposed a secure energy consumption management scheme, named Secure Power Management (SPM for short) to deal with the energy problem of a WSN and prolong operating time of its sensor nodes as well as coordinators. Most importantly, the SPM is still effective during being attacks. It then efficiently turns WSN nodes into sleeping mode when they are idle and wakes them up when necessary. In this mode, nodes consume less energy. A token based control policy is also developed to manage the power consumption of WSN nodes. Our simulation results show that during malicious attacks, the SPM still effectively reduces power consumption compared with that of the typical power management scheme.

Keyword：Power management; wireless sensor network; Security; malicious attack; break-even point; low power

目錄

圖目錄

表目錄

第一章 緒論

1.1 前言

在過去的十年中，由於需要較高的性能、功能和可攜性，低功率設計在設計電子設備中一直是關鍵的問題之一[1]。對於以電池供電的各種設備，低功耗是一個用以延長設備工作時間的重要設計準則。在各種低功率的設計方法中，其中一種有效的方法為電源管理，當系統處於空閒狀態時，他可以管理系統使其節省不必要的電力消耗，且已被廣泛應用到各種系統，如伺服器[2]，雲端計算[3]，智慧型手機[4]和無線感測網路(Wireless Senor Network;WSN)[5-7]等。

然而，許多先前的研究都是著重於對電源管理的效率和性能[8-10]，只有少數研究著重於安全性上[11-12]。當目標系統遭受惡意攻擊，甚至是這些惡意攻擊想破壞電源管理機制時，這時如何保持電源管理控制策略是一個非常重要的問題。事實上，可能會發生且導致整個系統的崩潰。例如，惡意攻擊可能造成耗電，並導致設備過熱或縮短其電池的工作時間[15]。在無線感測網路中，網路的壽命是感測環境數據和發送該數據到指定目標的一項關鍵因素[16]。基本上，惡意攻擊可能會藉由攻擊電源管理方案，去耗盡某些節點的能量。如果無線感測網路閘道節點中的一個被攻擊且停止工作，它將不能成功地將數據傳輸到協調器，導致嚴重的數據遺失。

由於大量使用了無線感測網路，如醫療保健監測[17]和工業監控[18]，以前的研究集中在防護數據的外洩和錯誤檢測[19-21]。Ren 等人[22]，提出了 location-aware end-to-end data security（LEDS)框架來克服 hop-by-hop 安全框架的漏洞。這種安全性的相關研究提出了對於常見的攻擊很好的防範；然而，對於電源管理方案的新類型攻擊防不勝防。

1.2 研究動機與目的

近年來，電源管理安全問題比以前獲得更多的關注。在伺服器系

統[11]和多核心處理器中[12]，已經提出了各種具有保護機制的電源管理策略的方法[13]。對於無線傳感器網絡的環境中，研究人員試圖解決彈幕攻擊(barrage attack)和睡眠剝奪攻擊(sleep deprivation attack)的問題。前者用正當的重複任務轟炸受害的節點，而後者發送請求給受害的節點，讓他們持續保持喚醒狀態。Pirretti 等[14]，提出了三個不同的防禦方法以緩解這些攻擊，即隨機表決機制(random vote scheme)，輪循機制(round robin scheme)，以及基於雜湊的機制(hash-based scheme)。這些方法表現出了優異的結果；然而，計算複雜高，使得目標系統的功率消耗在某些情況下顯著增加。

因此，在本研究中提出了一個安全的能源消耗方案，命名為可抵禦攻擊之無線感測網路能耗管理機制（Secure Power Management Scheme for WSN）的方法，通過採用電源管理概念，以控制無線感測網路節點的功耗，而且當他們遭受到惡意攻擊時，無線感測網路節點仍然可以節省電力。如果攻擊者對無線感測網路節點發送定期的垃圾訊息，對傳統的電源管理方案是有害的，例如：消耗更多的功率。SPM 是以標記計數策略為基礎所開發的，當在不適當的時間發生中斷信號時，睡眠模式將被延長，以防止負省電[24]。標記計數策略可以被用於各種硬體環境，有助於確定何時以及如何控制目標系統的操作模式。我們的模擬結果顯示，與不使用任何攻擊性機制的電源管理方案進行比較，SPM 可以有效地節省功耗。更重要的是，在我們所提出的方案協助下，可以有效地防止目標系統遭受到惡意攻擊所導致的負省電，並且只有極低的性能損失。

1.3 論文架構

本論文共分五章，第一章為緒論，此章節包括了前言、研究動機與目的以及論文架構。此章裡介紹惡意攻擊對無線感測網路的影響，並且說明研究動機與目的及論文整體架構。第二章為本論文相關的研究探討。第三章為 SPM 的實現方法，在 3.1 章節中，提出了系統架構且探討了惡意攻擊對能耗之影響，並且提出惡意攻擊的預測及防止，3.2 章節中提出了電源管理的模型，3.3 章節則是敘述 SPM 的方法。

第四章為模擬實驗結果，使用 NS2 模擬一般電源管理以及 SPM 對於惡意攻擊所造成的能耗影響，並分析模擬數據，驗證 SPM 的有效性。第五章為結論，對於本論文之研究成果做討論，最後是對於研究的未來工作。

第二章 相關研究

2.1 無線感測網路

隨著科技的日新月異，無線通訊已取代過去有線的溝通方式，成為生活中不可或缺的部分。無論何時，只要在可接收到訊號的地方，撥打手機便可和家人朋友通話；拿著配備無線網卡的電腦就可連上網路，隨時接收最新資訊。

早在 1993 年，日本 Hitachi 公司就提出把感測網路的概念應用於下水道監測系統的構想，但礙於線路配置和感測器設置的問題，感測網路只能使用在某些特定的高成本監測儀器上。直到 2000 年，加州大學柏克萊分校提出以無線傳輸為基礎的無線感測器網路（wireless sensor network, WSN），才解決了有線傳輸產生的問題。研究人員開發出一種體積很小，與普通阿斯匹靈藥片大小相似的感測器，稱之為「智慧灰塵」(Smart Dust)[23]，其採用微電子機械系統(MEMS)技術。由於這項計劃是由美國國防部研究計劃單位(DARPA)所支助，原先的構想是應用在軍事上，例如在戰場上，使用智慧灰塵的技術來監控與了解敵軍的行蹤，方法是使用無人駕駛的小飛機，帶著數以百萬計廉價且外型就像是灰塵一樣的無線感測器，灑在監控敵軍的區域，進行收集資料的任務，一段時間之後，同樣派遣無人駕駛的小飛機，將感測器收集到的資料透過無線網路傳回小飛機上，帶回基地加以分析，如此一來，就可以不需要冒著極大的危險派遣兵力深入敵方，完成收集敵軍情報的任務。後因為應用層面廣泛，學術和產業界都投入這研究領域，使無線感測網路迅速發展。

在無線感測網路中，感測器和無線網路是兩大核心，整個系統是由一到數個無線資料收集器以及為數眾多的感測器所構成的網路系統，而元件之間的通訊方式則是採用無線通訊的方式，我們可以任意擺放感測器或是無線資料收集器，不但省下可觀的佈線費用，而且極為方便。感測器不但能夠感測目標物 （溫度、光度、溼度、加速度、壓力等），感測節點也有自我組織網路的能力，每個都代表網路中的一個節點，可處理收集到的數據，並把處理後的資料以無線傳輸的方

式送到資料收集中心或基地台。圖 1 表示了 WSN 的基本組成，一般的 WSN 都是將感測節點散佈到一個區域，感測節點會收集資訊並匯集到基地台，再由基地台經由網際網路傳送給使用者。

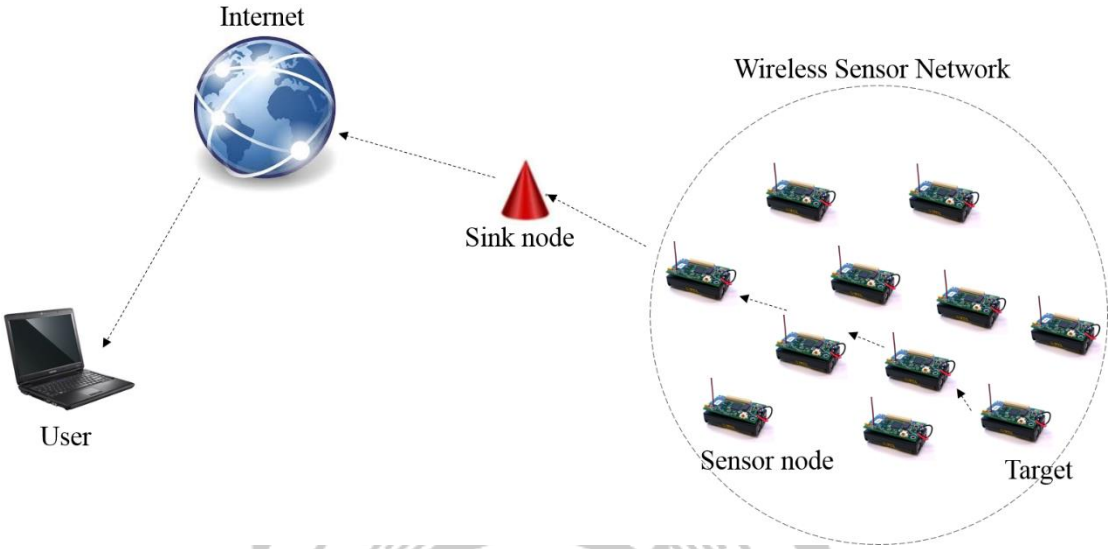

圖 1 WSN 基本組成

現今由於微機電系統和奈米科技的進步，讓感測網路的節點與佈線成本都能獲得有效的縮減，功能也越來越強，由眾多無線感測器所建構出來的 WSN，不僅涵蓋了大面積的資料收集、數據監控、自主運算、自主傳輸等現代化技術，其應用上也日漸蓬勃發展。2003 年美國 MIT《技術評論》認為，無線感測器網路技術是未來新興科技中最重要的一項關鍵性技術[48]；美國《商業周刊》也預測，無線感測網路是未來 4 大新技術之一[49]。因此可預見 WSN 的廣泛應用是一種趨勢，在未來的 5 至 10 年，會對許多產業和日常生活帶來衝擊性的影響。

2.1.1 WSN 節點架構

無線感測器網路主要由眾多的感測器節點構成，每一個節點都包含 4 大單元：感測單元(Sensing Unit)、處理單元(Processing Unit)、傳輸單元(Transceiver Unit)及電源供應單元(Power Unit)，如圖 2 所示。

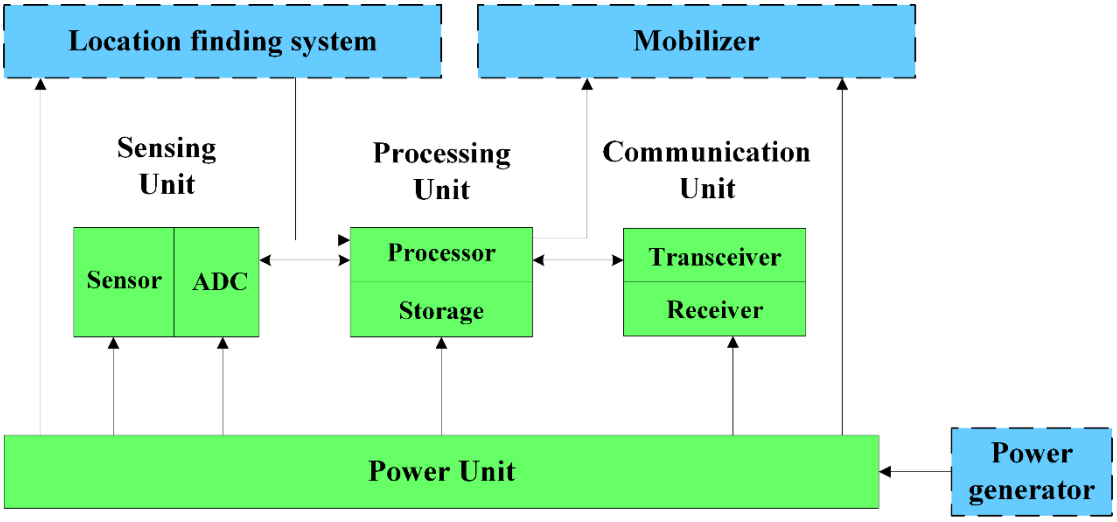

圖 2 感測節點之架構

1. 感測單元(Sensing Unit)：

(1) 感測元件（Sensor)：負責環境參數和資訊的量測，將收集到的資料(例如溫度、溼度、光度、壓力、加速度、紅外線等)使用類比訊號表示。

(2) 訊號轉換元件 ADCs（Analog-to-Digital Converters)：負責將感測元件感測到的類比訊號轉換成數位訊號，並將資料送到處理單位加以處理。

2. 處理單元(Processing Unit)：

(1) 儲存元件（Storage）：儲存元件的功能類似個人電腦中的硬碟等儲存裝置，將收集到的環境資訊儲存在儲存元件中。

(2) 處理元件 （Processor)：處理元件的功能類似個人電腦中的中央處理機(CPU)，負責執行事先儲存好的程式碼，以協調並控制感測器之間不同的單位元件。處理元件可以根據原先所儲存的程式指令、或是藉由後端伺服器所發送的命令，啟動感測單元收集環境的資訊，並將所收集的資料經過彙整後，透過傳輸單元將資料傳送回去。

3. 通訊單元（Communication Unit）：

(1) 接收元件（Receiver）:接收元件負責接收其他節點所傳來的資料，並且透過傳輸元件將資料轉傳給其他節點。

(2) 傳輸元件 （Transceiver）:傳輸元件負責感測節點和其他節點之間的溝通，或是將感測器的資料傳送給無線資料收集器。傳輸元件可使用的傳輸介質有紅外線(Infrared)、無線電波(Radio)、以及光纖介質(Optical Media)等，可因環境需求來選擇不同的傳輸方式。

4. 電源供應單元（Power Unit）：

電力供應單位，用來提供感測器運作所需的電源，無論任何一種功能運作都必須使用電源，是感測器中十分重要的單位；通常感測器的電力是由電池所支援，一般可選擇標準鋰電池，也可以選擇從環境中汲取能量的太陽能電池，因此在軟硬體的設計上，省電可以說是主要考量的因素之一。

感測器除了以上四個基本構成單位，也可以根據不同的環境、不同的應用來增加新的功能單位，例如可以新增用來辨識感測器本身位置的定位系統(Location Finding System)、外接或內建用來提供電源的電源產生器(Power Generator)、或是讓感測器具有行動能力且能夠攜帶感測資料的行動裝置(Mobilizer)等等。雖然感測器內部包含如此眾多的元件，但是感測器本身的硬體設計，最重要的是以體積小、重量輕、壽命長、成本低廉、以及高效能為設計的主要原則。

2.1.2 WSN 應用

目前無線感測網路在軍事[50]、環境監測[51]、工業[52]、居家[53]、健康照護[54]、教育娛樂[55]等有廣泛的應用。而目前是以環境監測應用最廣，軍事方面則是各政府最極為重視的，工業應用是許多工廠的當務之急。另外，從節省能源的商業應用，落實到一般民眾的居家應用、健康照護以及教育娛樂等，都是未來極具市場潛力。圖 3 說明了目前 WSN 各種不同的應用，無論在軍事、工業、商業、居家以及醫療照護上皆有相當廣泛的應用。

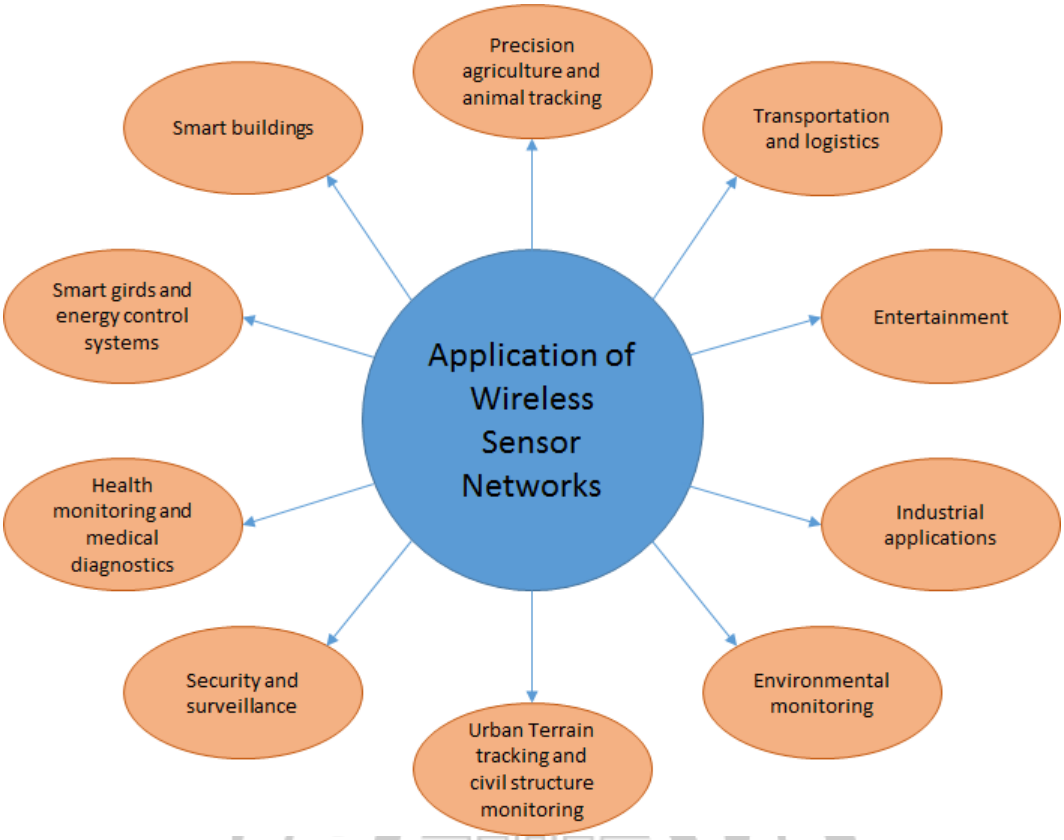

圖 3 WSN 之應用

2.2 無線感測網路功耗問題

無線感測網路的研究雖有極大的發展，然而，電池的能量密度並沒有隨之發展，功耗問題仍然是限制無線感測網路發展的重要因素，因此，無線感測網路的能耗問題受到了國內外研究學者高度的重視。

如前所述，無線感測網路其中的一部分是由為數眾多的感測器所組成，而這些感測器通常都相當的微小，本身所能攜帶的電量也相當有限，然而，這些感測器在偵測環境、資料處理運算或是將資料傳輸給後端的資料收集器時，都會耗費相當可觀的電力，若是沒有特別的省電機制，不僅感測器本身的生命週期會大幅縮短，也需要相當的人力和成本去更換感測器的電池，而在某些特殊的環境下，更換感測器並不是一件容易的事情。因此，如何提供感測節點良好的省電機制使之能夠長久使用，是目前無線感測網路的重要課題。

感測器中包含了感測、處理、傳輸以及電源供應 4 大單元，當感

測器在運作時，能量主要是消耗在感測節點上，而和數據處理相較起來，其中又以訊息的傳輸和接收消耗的最多，傳輸單一個 bit 的能量消耗大概和處理了數千個指令的感測器節點相同[27]。圖 4[28]顯示了節點在各狀態能耗的多寡，其中也顯示出了通信模組在傳送和接收以及空閒時消耗的能量遠大於休眠時間時所消耗的能量，因此，通信模組最好盡可能保持睡眠狀態。

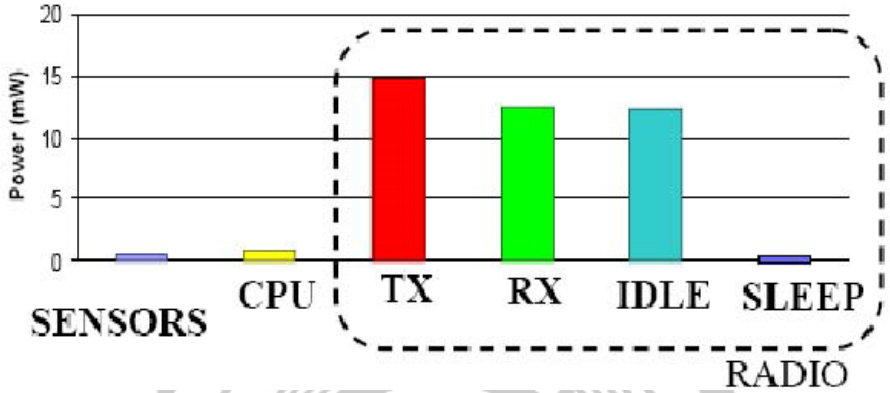

圖 4 節點狀態能耗分析[28]

表 1 表示出 Rockwell's WINS 節點的能耗分析[29]，它代表一個高端感測器節點，並配有 StrongARM 的 SA-1100 處理器，無線通訊系統模組，以及多種感測器。表 2 表示出了 MEDUSA-Ⅱ的特性，加州大學洛杉磯分校嵌入式系統實驗室開發的實驗感測節點。MEDUSA 節點，設計為超低功耗，為一個低端感測器節點。MCU Mode 為 Microcontroller unit 不同的模式，其中包含了工作模式(Active)、空閒模式(Idle)、睡眠模式(Sleep)，Sensor Mode 為感測器開和關兩種不同的模式，Radio Mode 為無線通訊的模式，包含了傳輸(Tx)、接收(Rx)、空閒(Idle)以及關閉(off)，Mod. Scheme 為調變，有 On Off Keying(OOK)以及 Amplitude Shift Keying(ASK)兩種，Data Rate 為資料傳輸速率，Power(mW)則為所消耗之能量。從表中可以看出，在兩個節點的功耗特性明顯不同。我們可以從這些表得出以下推論：

1. 節點的功耗大多是在主動模式上，尤其在傳輸模式下功耗更高。如表 1 所示，當 WINS 節點的 MCU 處於休眠模式時，比當它處於主動模式時消耗的電力大約只有六分之一。

2. 接收和空閒模式下的節點消耗的功率大致相同。因此，空閒模式相較於接收模式並不具有任何優勢。要達到節能的效果就必須完全的關閉無線傳輸模組。

因此，為了解決 WSN 的功耗問題，方法其一是讓感測器使用更有效的路由技術，使節點傳輸部分的能量降低，資料在傳輸上更有效率，進而達到降低能量消耗的效果[30]。除此之外，將感測器的電池效能加強或是從環境汲取能量來進行電源的補充[31-34]，也是可行的方法之一。另外使用電源管理能夠有效地去協調包括通訊模組在內的各模組的睡眠、空閒和工作時間，進而達到減少功耗的效果。因此，電源管理在無線感測網路中已經有廣泛的研究與應用。

表 1 Rockwell's WINS 節點之能耗分析[29]

MCU Mode	Sensor Mode	Radio Mode	Power(mW)
Active	On	Tx(Power:36.3mW)	1080.5
		Tx(Power:19.1mW)	986.0
		Tx(Power:13.8mW)	842.6
		Tx(Power:3.47mW)	815.5
		Tx(Power:2.51mW)	807.5
		Tx(Power:0.96mW)	787.5
		Tx(Power:0.30mW)	773.9
		Tx(Power:0.12mW)	771.1
Active	On	Rx	751.6
Active	On	Idle	727.5
Active	On	Sleep	416.3
Active	On	Removed	383.3
Sleep	On	Removed	64.0
Active	Removed	Removed	360.0

表 2 MEDUSA-Ⅱ節點之能耗分析

MCU Mode	Sensor Mode	Radio Mode	Mod. Scheme	Data Rate	Power(mW)
Active	On	Tx(Power:0.7368mW)	OOK	2.4 kb/s	24.58
		Tx(Power:0.0979mW)	OOK	2.4 kb/s	19.24
		Tx(Power:0.7368mW)	OOK	19.2 kb/s	25.37
		Tx(Power:0.0979mW)	OOK	19.2 kb/s	20.05
		Tx(Power:0.7368mW)	ASK	2.4 kb/s	26.55
		Tx(Power:0.0979mW)	ASK	2.4 kb/s	21.26
		Tx(Power:0.7368mW)	ASK	19.2 kb/s	27.46
		Tx(Power:0.0979mW)	ASK	19.2 kb/s	22.06
Active	On	Rx	Any	Any	22.20
Active	On	Idle	Any	Any	22.06
Active	On	Off	Any	Any	9.72
Idle	On	Off	Any	Any	5.92
Sleep	Off	Off	Any	Any	0.02

2.3 無線感測網路之電源管理方案

電源管理在現代電子、網路的組建或是自動控制方面都已經有所發展，甚至已經廣泛應用到工業、能源、交通、訊息、航空、國防、教育、文化等眾多領域。而電源管理在無線感測網路當中也非常重要，前面提到，感測器節點的功耗問題以及對電池壽命的重要，而一個有效的電源管理能夠使的整個無線感測網路有較長的生命週期，因此，電源管理也已經廣泛的應用於無線感測網路當中[56]。

在系統層級和硬體方面已經有提出許多的方法去設計高效節能的通訊處理、感測節點操作系統[35]和感測器電路。此外，動態電源管理通過選擇性去關閉空閒的組件以漸少電力消耗，像是利用睡眠狀態以及主動電源管理[36,37]、基於 sentry 的電源管理[38]、動態電壓及頻率調整[35,36,39]、應用驅動的方法[40]、動態電源管理與排程的切換模式[41]等。

2.3.1 高效節能通訊處理

無線感測網路在傳輸上若某些 Source 沒有協調到匯聚節點的路由，那一個或多個節點可能因過度使用而耗盡能量。如圖 5 所示，它包括十個節點，其中有三個 Source 節點和一個匯聚節點，每個 Source 節點都會確定一個到匯聚節點的最佳路徑，例如:G 到 Z 的最佳路徑為 G→F→Z，A 到 Z 的最佳路徑為 A→F→Z，B 到 Z 的最佳路徑為 B→F→Z，很明顯，上述所有的路徑都需要使用到節點 F，所以為了減少 F 的能量消耗，這需要 Source G 使用非最佳路徑 G→H→I→Z。因此，優化路由方案使之有高效節能的通訊，電源管理重要的一部份。優化路由方案可簡單分為以下四種[57]：

1. 最少能耗尋徑（Minimum Energy routing）

   傳輸和傳輸距離都需要能量，較長的序列的短跳(small hops)比較短序列的長跳(long hops)所需能量更少。Minimum Energy routing 會找尋最節省能量的路徑去進行傳輸。例如：Multi-stage data routing protocol（MLRP）。

2. 最少節點尋徑（Minimum hop routing）

   Minimum hop routing 必需選擇一個基於最小數目的跳的路徑來到達匯聚節點，最早的 Minimum hop routing 為 Dynamic Destination Sequence Distance Vector Routing（DSDV）後來被 Ad Hoc On-demand Distance Vector Routing(AODV)所取代。

3. 負載平衡尋徑（Load balancing routing）

   Load balancing routing 會盡可能給多個節點去分散部分路由負載，即使 sources 所選擇的路徑並沒有最佳的能量消耗。

4. 可能性尋徑（Potential Based routing）

   Potential Based routing 在節點發生故障或是找不到時，能夠重新尋找最佳的路徑，並調整整個子集的節點路徑，以確保其他到匯聚節點的路由不會因此遭受破壞。例如：Power aware multicast routing protocol(PMRP)。

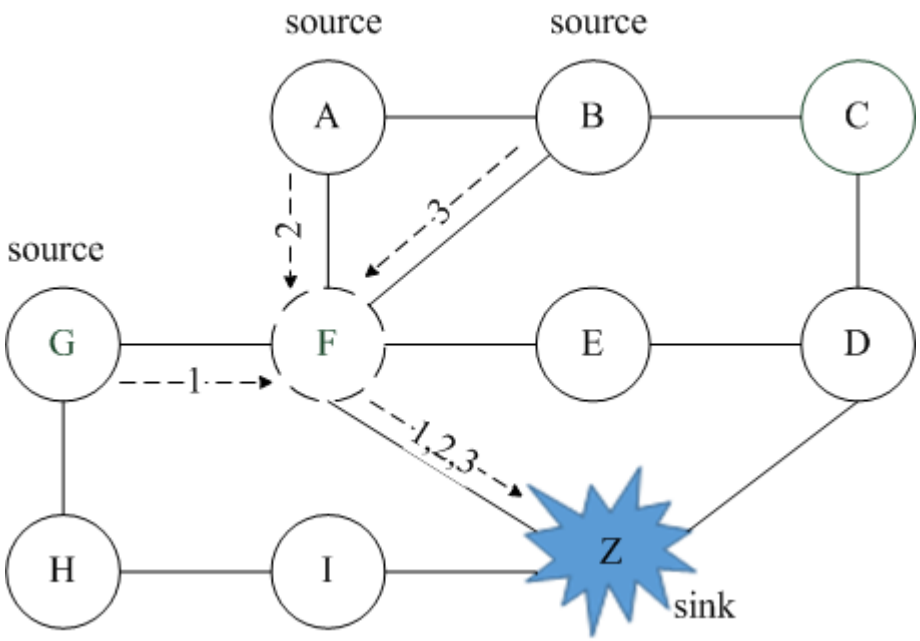

圖 5 WSN 路由示意圖

2.3.2 動態電源管理

動態電源管理策略可以有局部、全部或是兩者兼具的不同方案。局部的動態電源管理策略目的在於盡量減少各節點的功率消耗，只提供每個系統足夠進行目前任務的功耗，當沒有任務進行處理時，動態電源管理使部分系統以最節省功耗的模式運作，或是使其進入睡眠模式；全部的動態電源管理策略通過限定一個網路範圍使之保持睡眠狀態以達到減少整個網路的功率消耗。

有非常多種方式可以達到個目標，其中一種方式是讓各節點定義自己的睡眠時間排程以及分享這些時間排程給他們周邊的節點進而去啟用協同感測及高效的節點內通訊，這就是所謂的同步睡眠，這種方法的問題在於鄰近節點需要同步時間和時間排程以及整個過程是能量密集型的。另一種方式是讓各節點保持自己的睡眠時間排程，當一個節點開始一個通訊前需要先傳送一個前置訊息直到他接收到一個鄰近節點回覆的確認訊息，這種方法被稱做異步睡眠，避免了需要同步時間排程，但是在數據傳輸上會有延遲的副作用。

一旦時間參數固定，動態電源管理策略通過定義對節能的運作條

件以達到減少系統電力的消耗。儘管有不同的方法能達到動態電源管理策略，但他們都能歸類於以下三種方法[58]:

1. 動態操作模式

無線感測網路的子系統依他們目前或預期的活動被配置在不同的功率模式下操作，動態電源管理的任務是使活動中的無線感測網路有最佳的配置。表 3 顯示了不同的元件在不同狀態下的配置，在工作狀態下，所有的組件皆處於開啟的狀態，在 Sleep state 1 、Sleep state 2 及 Sleep state 3 的狀態下，分別使記憶體及處理器進入休眠狀態，以及關閉無線傳輸模組，來降低功率消耗，Sleep state 4 則是使所有組件都進入休眠狀態或是關閉以達到最低的功率消耗。

表 3 WSN 元件狀態之差異

State	Processor	Memory	Sensor	Radio
Active	Active	Active	On	Tx, Rx
Sleep state 1	Idle	Sleep	On	RX
Sleep state 2	Sleep	Sleep	On	RX
Sleep state 3	Sleep	Sleep	On	Off
Sleep state 4	Sleep	Sleep	Off	Off

2. 動態調整(Dynamic scaling)

動態電壓調節和動態頻率調節是能夠增強動態電源管理的方法，這兩種方法是當組件處於主動狀態時，透過調整電壓以及頻率來節省功耗。

3. 任務排程

透過任務排程這種方式使處理器不會停留在空閒狀態並且消耗多餘的功率。

這些常見的電源管理方法都只是注重於改善效率或是性能，卻極少有能夠防禦惡意攻擊的機制，一旦無線感測網路遭受到惡意攻擊時，這些電源管理系統將無法分辨是正常訊號或是惡意訊號，這將導致了電源管理喪失了原有的功能，無法有效的達到省電的功能。

第三章 安全電源管理實現方法

3.1 系統架構

3.1.1 惡意攻擊對電源的影響

在無線感測網路中，存在著各種不同類型的攻擊，而其中又有一些攻擊會對電源造成影響[42]。電源可以說是最有價值的資產，但大部分安全性的防護並沒有著重於電源相關的方面，節點中通常都只有一個壽命有限的電池，一旦攻擊者對節點進行攻擊並試圖耗近其資源，則會大大的降低其生命週期，嚴重一點甚至有可能會癱瘓整個網路的通訊。

下面將介紹三個常見的無線感測網路攻擊對於能耗所造成的影響：

1. Hello Flood attack

圖 6 為 WSN 發生 Hello Flood attack 示意圖，網際網路上的 Flood attack 是要阻斷或延遲使用者所要享受的服務，無線感測網路的 Flood attack 主要是要讓感測節點的電池沒電，而 Hello Flood attack 則是藉由發送 Hello 訊息來達成此目的。在無線感測網路中，一個正常的感測節點接受到鄰近感測節點送來的 Hello 訊息時，會回應一個確認(acknowledgement)訊息，讓彼此知道處於鄰近位置。而 Hello Flood attack 中，是惡意節點會不斷傳送 Hello 訊息，迫使其他節點反覆回應，直到電量耗盡為止[43][44]。

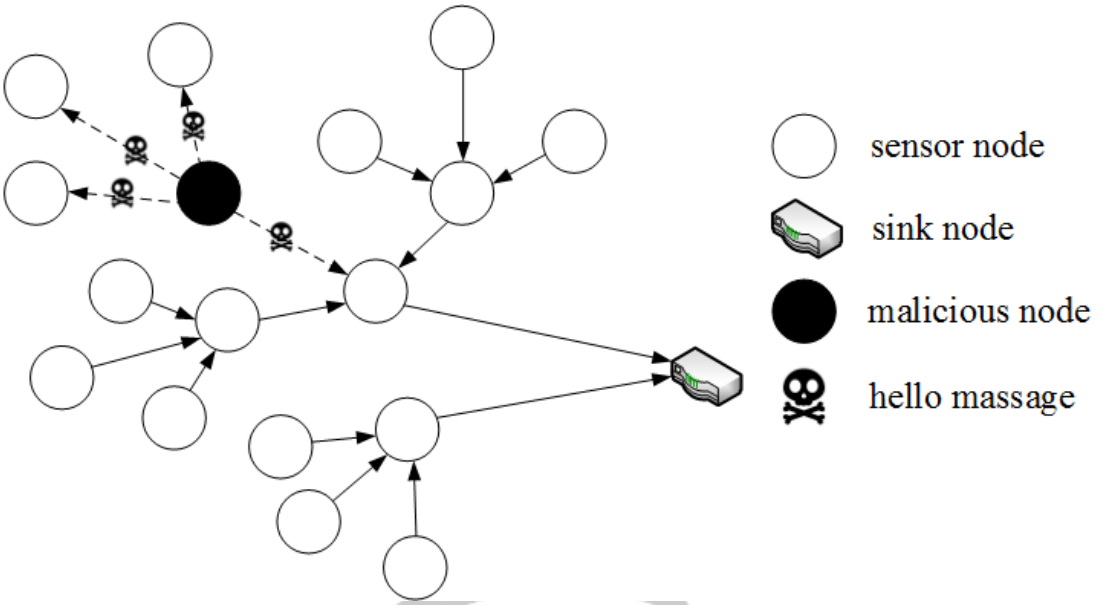

圖 6 WSN 遭受 Hello Flood attack

2. DOS attack

圖 7 為 WSN 發生 DOS attack 示意圖，DOS 攻擊種類非常多且以不同的方式去降低網路壽命，其中之一為攻擊節點會傳送大量的資料封包給受害節點，使受害節點或是整個網路無法正常的運作，持續的接收資料封包除了會導致節點無法和其他節點溝通，也會導致電量耗盡，進而縮短電池壽命[42]。

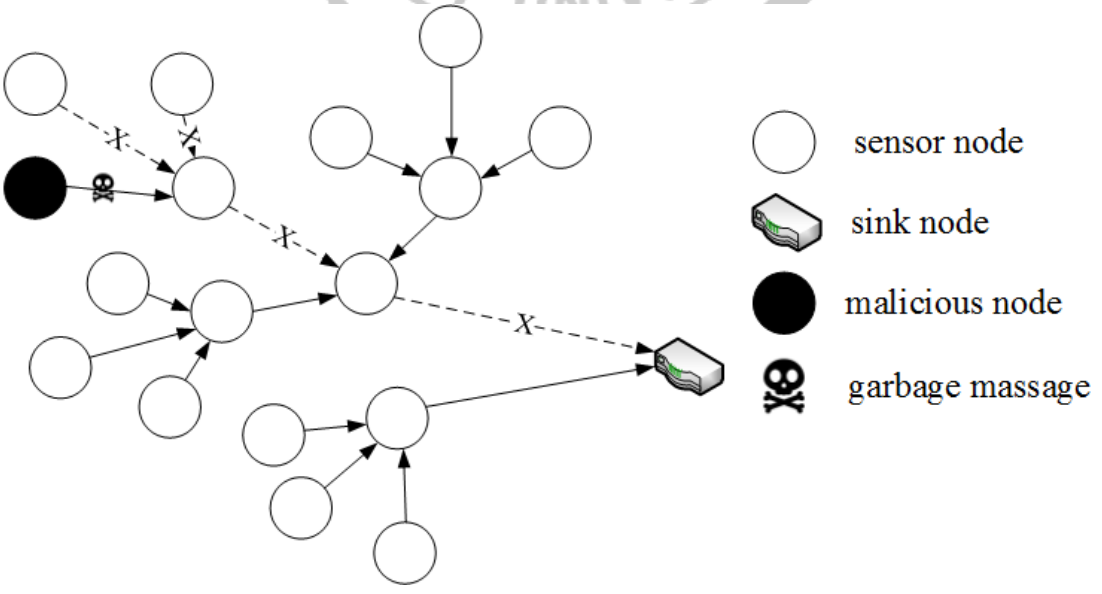

圖 7 WSN 遭受 DOS attack

3. Sinkhole attack

圖 8 為 WSN 發生 Sinkhole attack 示意圖，Sinkhole attack 是一種特別嚴重的攻擊，攻擊者會使基地台無法獲得完整和正確的感測數據，構成了嚴重威脅。在 Sinkhole attack 中，惡意節點讓自己看起來比周圍節點具有更好的路由路徑，並吸引資料流向自己，通過路由過程的參與，他可以選擇性地轉傳資料封包，甚至能夠修改或是丟棄資料封包，而不斷地轉傳資料封包也導致了整個網路的能源耗竭[42,45]。

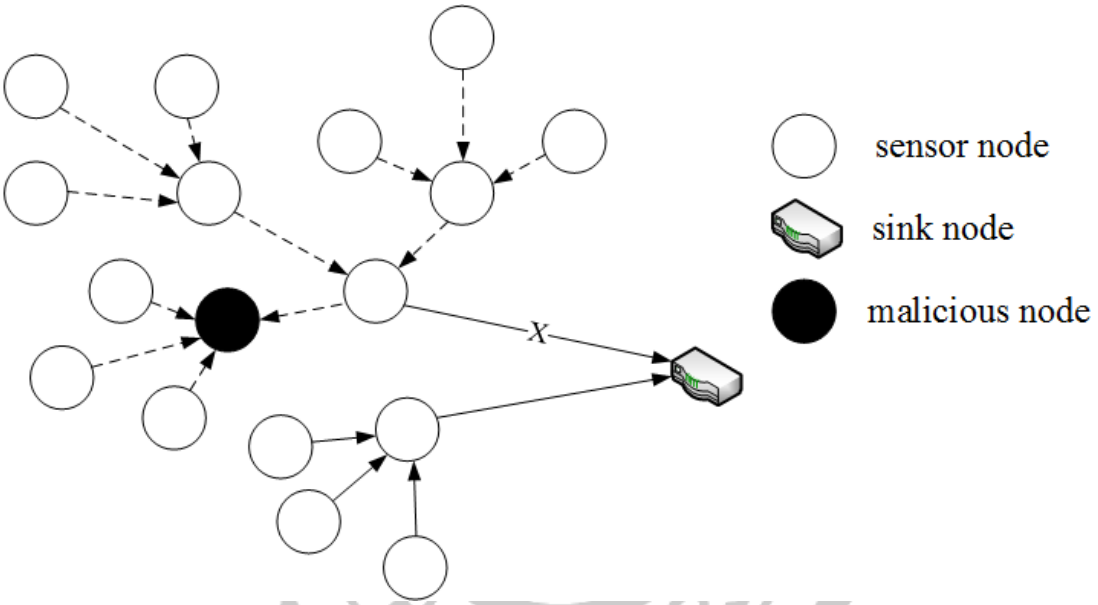

圖 8 WSN 遭受 Sinkhole attack

3.1.2 系統架構及攻擊模式的預測與防止機制

在整個系統中，我們採用常見的無線感測網路，並在每個節點上使用 SPM 機制，圖 9 為整個系統的架構，整個無線感測網路包含許多的感測節點以及匯聚節點，當感測器收集到環境資料時，會將其送至鄰近的匯聚節點彙整，再將資料傳送至使用者。每個感測節點中的 SPM 機制能夠有效的控制節點功耗，而當惡意攻擊發生時，也能夠經由 SPM 機制阻擋。

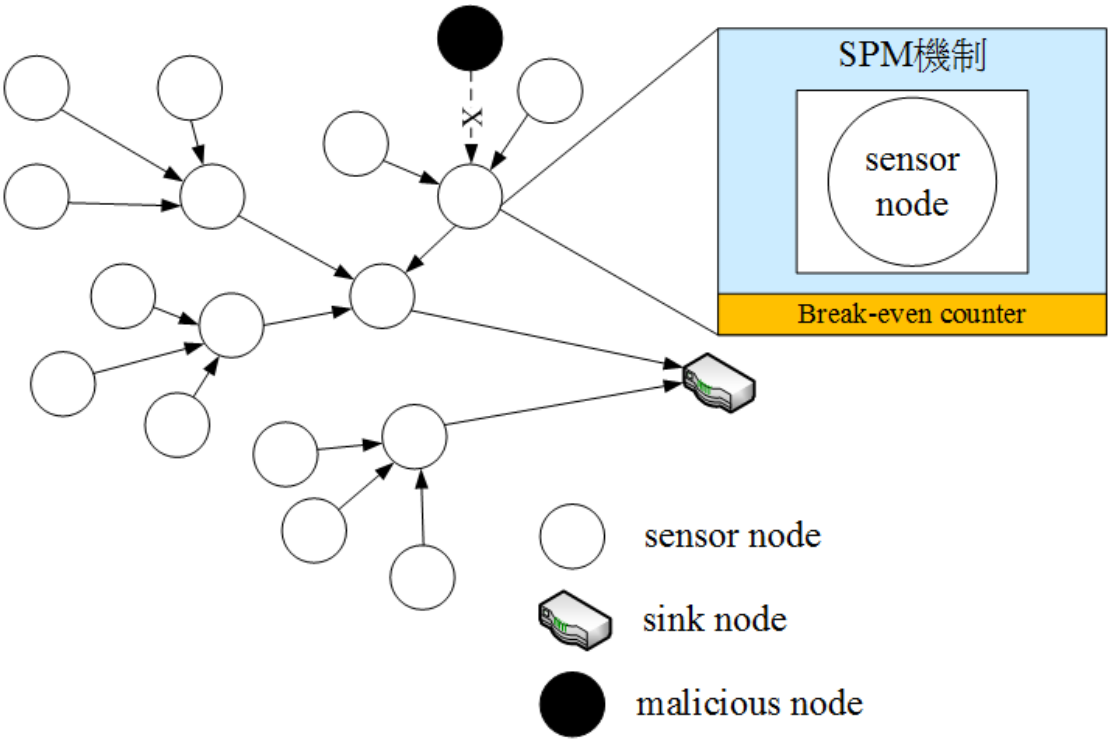

圖 9 SPM 系統架構

3.2 電源管理模型

電源管理是一個控制策略，以關閉（如：gating）系統電源或切換未使用的系統以達到到低功率狀態，例如：睡眠模式。這是一種有效的低功耗設計方法;但是，系統進入或離開其休眠模式時，將消耗額外的能量和導致額外的運行延遲。一旦系統的睡眠時間過短，額外的功率消耗可能會比它處於的活動模式時還高，例如：負省電。Hu 等人提出功率門控機制的 break-even point [24]，可用於達到正省電。它也確保了在系統被喚醒前停留在睡眠模式連續時鐘週期的最小數目。如果系統停留在睡眠模式不夠長，無法達到 break-even point，就會出現負省電，消耗更多的功率。

當系統的電源管理開啟/關閉系統，由於額外的控制操作，它會導致額外的能量 $E_{overhead}$，如公式(1)所示。

$$E_{overhead} = 2\frac{W_H}{\alpha}E_{cyc}^{S} \qquad (1)$$

其中 W_H 是該電路的門控系統的區域的總面積的比率，α為目標系

統的 active factor，以及E^{S}_{cyc}是由開/關的功能單元所消耗的能量。在切換週期（開/關打開）時，系統的電壓是不穩定的，並且不能用於正常的工作，但它仍消耗功率。E_{saved}為睡眠期間節省了 N 個時鐘週期的總能量，可以表示公式(2)。

$$E_{saved} = E^{L}_{cyc}\frac{DIBL}{mVt} \times \frac{N^2}{2} \times \frac{\alpha \mathrm{LV}_{dd}}{2(\frac{1}{2}+\frac{C_D}{C_S})} \quad (2)$$

其中 DIBL 是 drain-induce barrier lowering factor[25]，m是 slope factor[25]，V_{dd} 是電源電壓，V_t 為溫度電壓[25]，L 為 leakage factor，他被定義為開關能量洩漏的比例，其中$L=E^{L}_{cyc}/E^{S}_{cycs}$，$C_D$和 C_S分別表示去耦電容和開關電容。當睡眠所節省的能量等於開啟/關閉所導致的額外能量，$E_{saved}=E_{overhead}$，會得出 break-even point N。

$$\mathrm{N} = 2\frac{1}{L_\alpha}\sqrt{(1+2\frac{C_D}{C_S})\frac{mV_tW_H}{V_{dd}\times DIBL}} \quad (3)$$

若想使得目標系統能夠節省開啟/關閉所導致的額外能量，可以假設一變數 k，k 必須大於 N，並代入 N，會得到$E_{saved}>E_{overhead}$，所節省的能量就會比開啟/關閉所導致的額外能量還要多，如此一來就能確實節省開啟/關閉所導致的額外能量。

3.3 安全電源管理方法

本論文所提出的 SPM 是建立於 break-even point 的模型，使用增強的電源管理方案，以控制目標系統的功耗，像是微處理器和各種功能單位。圖 10 為 SPM 的架構，其中當所述目標系統進入空閒狀態時，會發送訊號告知 SPM，而 SPM 會傳送一個休眠訊號，以便該目標系統可以進入其休眠狀態，使其消耗之能量能夠確實地小於活動模式。一旦系統處於其睡眠模式時，SPM 中的 break-even counter 會開始計數時脈週期的數目。如果有輸入/輸出中斷或是惡意攻擊發生時，而 SPM 中的時脈週期數沒有達到 break-even point(公式(3))會暫時忽略此事件。當目標系統接收到一個內部事件訊號或睡眠時間達到 break-even point，SPM 就會傳送一個喚醒訊號喚醒目標系統。

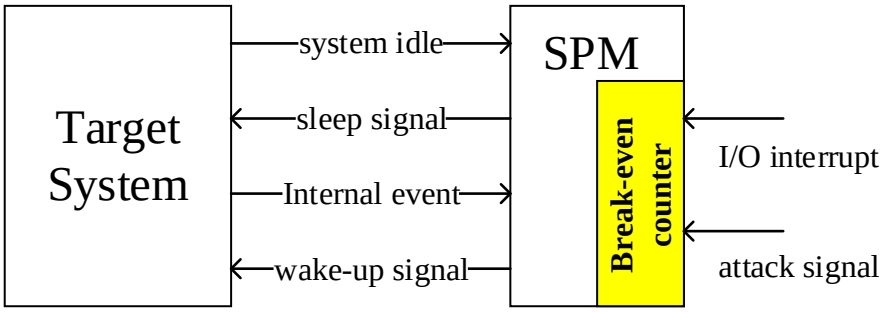

圖 10 SPM 架構

為了降低計算消耗，時間間隔 *Ti* 由使用者事先定義，並用來控制 SPM 的執行時間。此外，一個 sleeping token *k*（在 break-even counter）被用來記錄累積睡眠週期的數目，而 success token *s* 被用來記錄保持成功睡眠的次數，例：正省電。基本上，break-even point 被分為幾個時間間隔，在每一個間隔內，token *s* 或 *k* 將會增加/減少 1。

圖 11 顯示了 SPM 的的控制流程。在一開始，SPM 會等待系統空閒。當目標系統的空閒週期比 doze 的門檻高時，這意味著在這段時間內，目標系統保持在非活動模式，此時 SPM 會傳送一個休眠信號到目標系統以降低系統的功率，然後將休眠標記 *k* 設置為 0。然後，在每個時間間隔開始時，SPM 會檢測是否有目標系統傳送一內部事件請求到 break-even counter，如果沒有，就會進入外部訊號的檢查，若沒有外部訊號，在睡眠模式下估計節電效率的 break-even counter 就會將 token *k* 增加 1。如果至少有一個內部事件請求被傳送到 SPM 中，SPM 將會檢查 sleeping token *k* 是否高於 break-even point *N*，如果是的話，*s* 就會被增加 1，這意味著睡眠是有效的，而且可以有效達到省電，然後，一個喚醒訊號就會被傳送到目標系統去啟動它。若是 *s* 小於 break-even point *N*，*s* 將會減少 1 以顯示在此沒睡眠期間沒有節省功率。

如果一外部信號到達時，即輸入/輸出的中斷或攻擊信號，喚醒信號並不會立即傳送到目標系統。這時 SPM 會先檢查 sleeping token *k* 是否高於收支相抵點 *N*。如果是的話，*s* 將會增加 1，並且傳送一個喚醒訊號到目標系統以啟動它。反之，在 sleeping token *k* 小於 break-even point *N* 時，SPM 在這種情況下是無法節省功率的，而為了防止

負省電，SPM 將不會傳送喚醒訊號到目標系統；相取而代之，它會使目標系統持續保持休眠狀態直到 $k>N$。

會選擇 token 計數作為保護機制的原因是，它不需要複雜的 power estimate circuits 或 functions。通過使用簡單的增加/減少，可以不進行複雜的計算就能使得系統的功耗能被有效的控制。

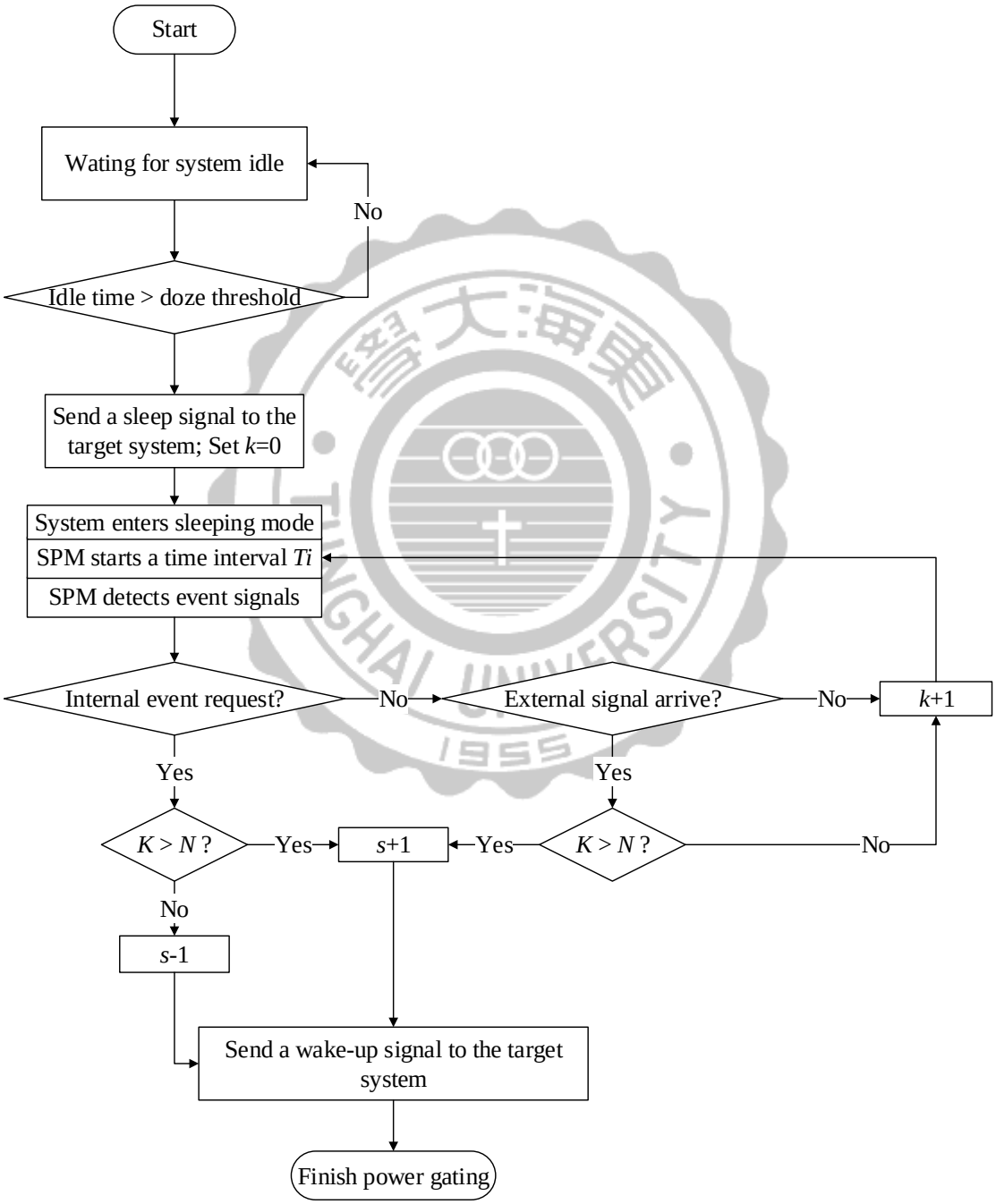

圖 11 SPM 控制流程圖

第四章 模擬結果

4.1 模擬環境

為了驗證 SPM 的可行性和正確性，我們使用了 NS2 模擬了 3 種在無線感測網路中常見的攻擊，分別是 Hello Flood attack、DOS attack、Sinkhole attack，並比較有無 SPM 的能耗差異。感測節點設定為睡眠 60 秒後進行一次資料傳輸，傳輸時間為 30 秒，在沒有傳輸的 60 秒內，感測節點會進入休眠狀態。

我們假設 break-even point N 為 1，而感測節點的睡眠時間為 60 秒，因此我們把時間間隔 Ti 設置為 30 秒，也就是每 30 秒 K 會+1。當時間為 60 秒時 $K>N$，這時若有訊號到達，節點就會被喚醒。時間間隔和睡眠時間的關係如下：

$$\mathrm{Ti} = \frac{sleep\ time}{N+1} \quad (4)$$

在 Hello Flood attack 中，惡意節點不斷的傳送 Hello 請求，周遭正常節點也回持續回應惡意節點，導致正常節點甚至是整個網路的電量持續的消耗。在 Hello Flood attack 中，設置 MAC 為 802.11，routing protocol 為 AODV，並且有 10 個節點，總模擬時間為 300 秒。在能量的部分，初始能量設置為 1000J，傳輸及接收能量設置為 0.03J，睡眠的能量為 3×10^{-4}J。圖 12 中為 Hello Flood attack 的模擬介面，其中節點 0 為 Source 端，節點 4 為 Destination 端，而節點 5 為攻擊節點。當攻擊發生時，可以看到攻擊節點持續傳送出 Hello 的訊息，而其餘節點也持續地回復攻擊節點，直至電量耗盡。

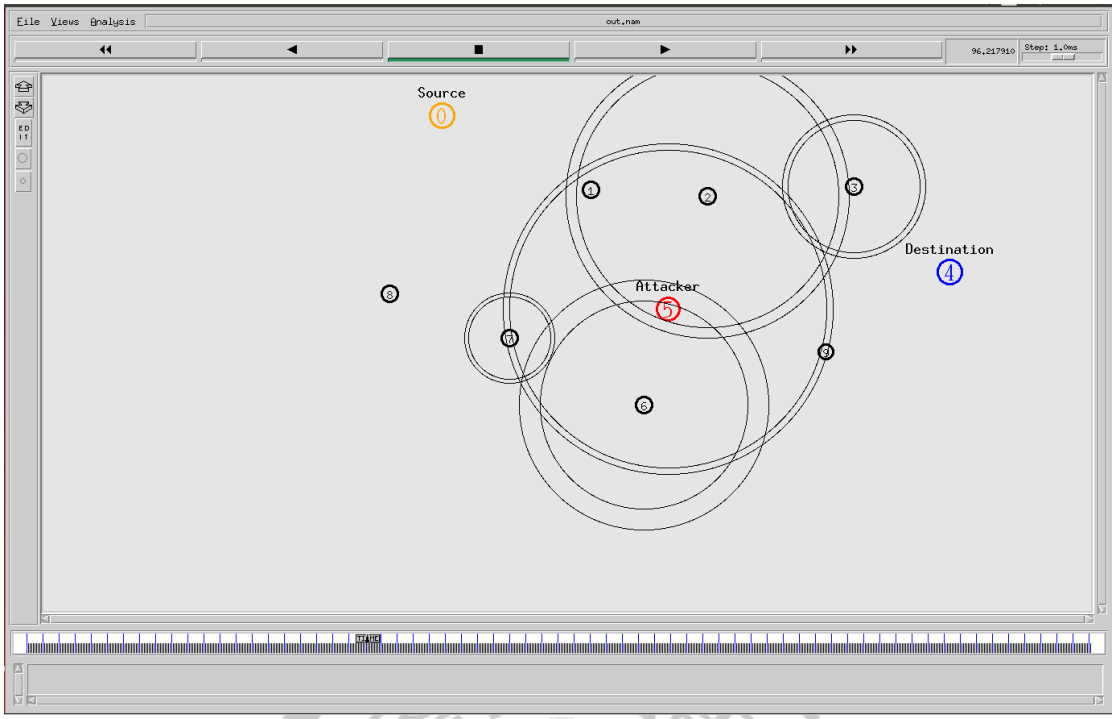

圖 12 Hello Flood attack 模擬介面

在 DOS attack 中，我們模擬了攻擊節點大量傳送資料封包給受害節點，導致受害節點電量耗盡，進而癱瘓整個網路。在這個模擬中，我們使用了 UDP 協定以及 CBR 應用程序來實現，一旦受害節點持續接收到攻擊節點的資料封包，他便無法及時的處理其餘正常節點的傳輸，並導致資料流失，長時間下來，受害節點的電量也將耗盡，使整個網路受到影響。在 DOS attack 中，設置 MAC 為 802.11，routing protocol 為 AODV，並且有 20 個節點，總模擬時間為 300 秒。在能量的部分，初始能量設置為 1000J，傳輸及接收能量設置為 0.03J，睡眠的能量為 3×10^{-4}J。圖 13 中為 DOS attack 的模擬介面，其中設置節點 4 設置為 Source 端，節點 10 為 Destination 端，節點 0 為攻擊者。在攻擊開始時，攻擊者會持續傳送資料封包給節點 1，使得 Source 端到 Destination 端的傳輸受到影響，造成資料封包的流失，且在持續一段時間之後，節點 1 將會耗盡電量。

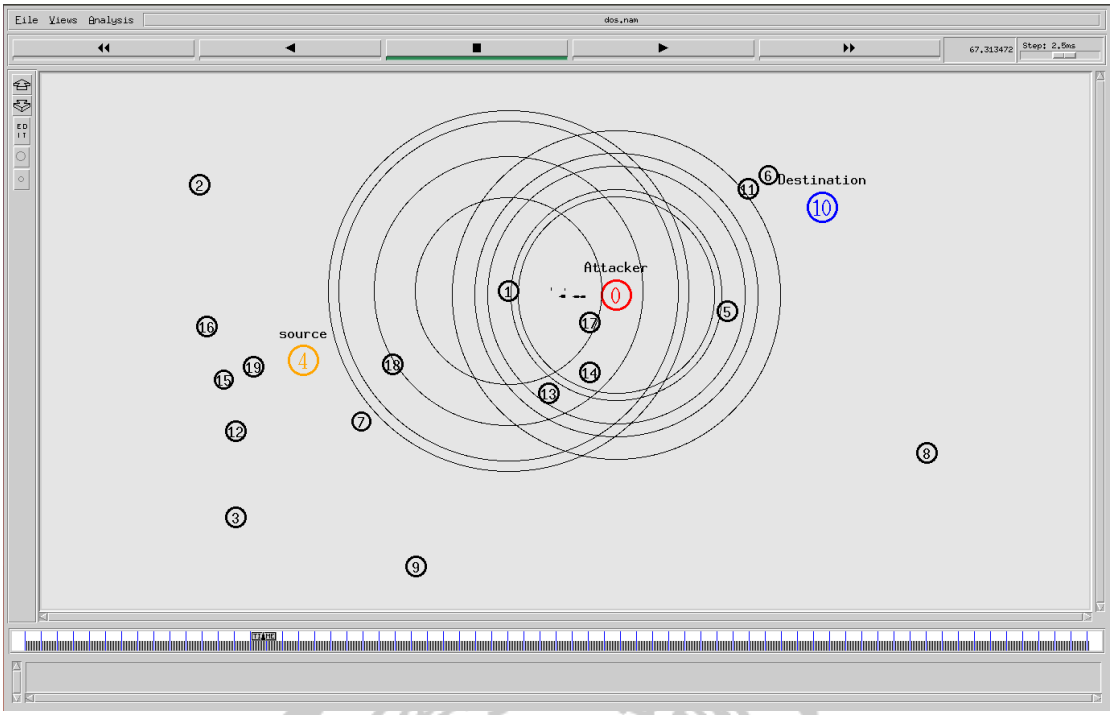

圖 13 DOS attack 模擬介面

在 Sinkhole attack 中，攻擊節點發送虛假訊息騙取傳輸端節點和其建立路由並使之資料流向攻擊節點。在 Sinkhole attack 中，設置 MAC 為 802.11，routing protocol 為 AODV，並且有 25 個節點，總模擬時間為 300 秒。在能量的部分，初始能量設置為 1000J，傳輸及接收能量設置為 0.03J，睡眠的能量為 3×10^{-4}J。圖 14 中為 Sinkhole attack 的模擬介面，其中節點 21 設為 Source 端，節點 11 設為 Destination 端，節點 1 為攻擊者。正常狀況下，資料封包會從節點 21 經由節點 23、9、10 傳送至節點 11，一旦攻擊發生時，資料封包則會從節點 21 經過節點 23、15，最後傳送至節點 1，導致資料的遺失或竊取，也導致節點 15 的電量增加了不必要的消耗。

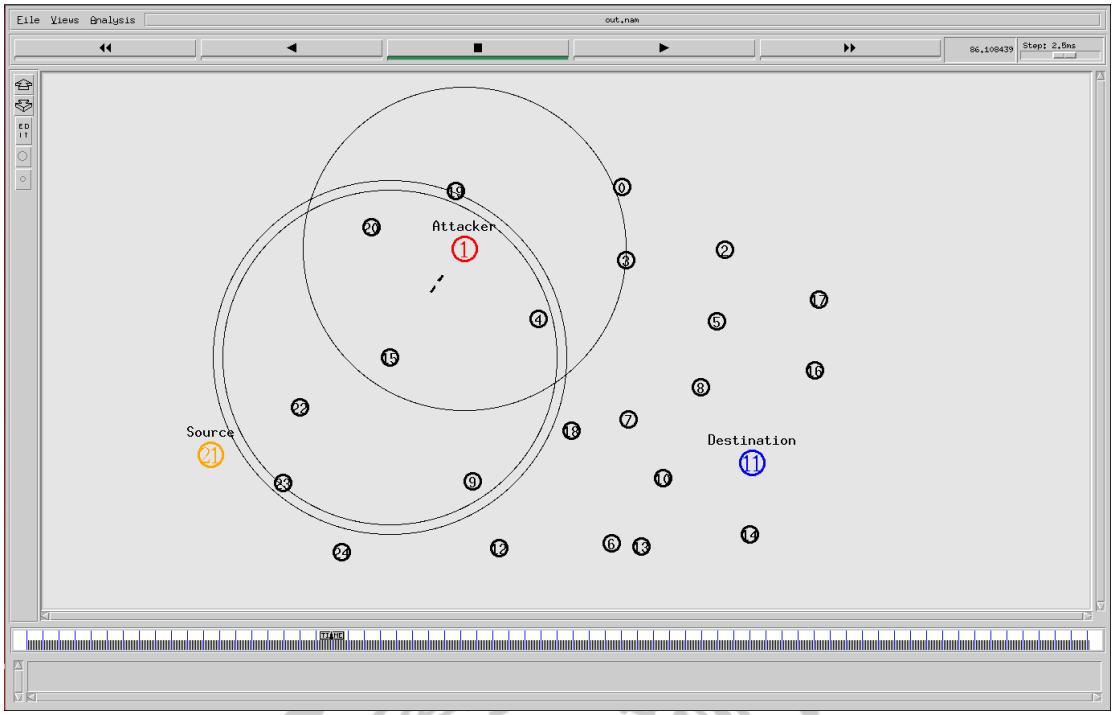

圖 14 Sinkhole attack 模擬介面

4.2 模擬結果

我們模擬了一般電源管理系統以及使用了 SPM 的結果，並分別測試三次循環後所剩餘的能量。我們將初始能量設為 1000J，模擬時間為 300 秒，觀察感測節點 1 在 Hello Flood attack 影響下所剩餘的能量並進行比較。圖 15 為使用 SPM、使用一般 PM 在工作狀態被攻擊及使用一般 PM 在睡眠狀態被攻擊之比較，use general PM (attack in active)這條線代表為使用一般 PM 時，攻擊節點在 Source 端開始進行資料封包傳送時進行攻擊，一但攻擊開始，節點 1 則會持續處於工作狀態。use general PM (attack in sleeping)這條線為使用一般 PM 時，攻擊節點在其他節點處於休眠狀態時就進行攻擊，當於休眠狀態發生攻擊時，感測節點會被喚醒並且回復攻擊節點的訊息。而若攻擊持續的進行，可以明顯的看到，在 90~150 秒、180~240 秒以及 270~300 秒這段時間，感測節點應該是處於休眠狀態，但卻因為持續回復攻擊節點的訊息而導致無法進入休眠狀態。attacked by using SPM 為加入了 SPM 後的剩餘能量圖，感測節點在接收到攻擊節點的訊號會因為還沒達到 break-even point 而無法被喚醒，如此一來就能有效的防止感

測節點持續的傳送回復訊息。表 4 表示出各狀態轉換點之能量，分別為使用 SPM 的情況、在工作狀態開始時遭受攻擊以及在休眠狀態下就遭受攻擊。模擬結果顯示出 SPM 能夠有效的防止 Hello Flood attack 所造成的能量損耗。在經過 300 秒後，模擬結果比較顯示出，SPM 比起一般的 PM 能夠有效的節省約 6.5%的能量，如表 6 所示。

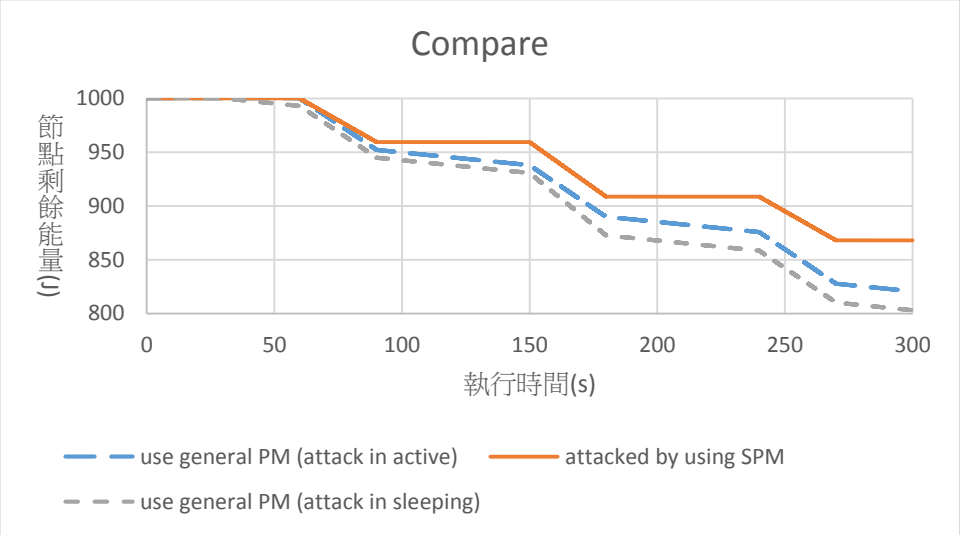

圖 15 使用 SPM、使用一般 PM 在工作狀態被攻擊及使用一般 PM 在睡眠狀態被攻擊比較圖

表 4 使用 SPM、使用一般 PM 在工作狀態被攻擊及使用一般 PM 在睡眠狀態被攻擊比較表

能量 / 時間	attacked by using SPM	use general PM (attack in active)	use general PM (attack in sleeping)
60 秒	99.9%	99.9%	99.1%
90 秒	95.9%	95.2%	94.5%
150 秒	95.9%	93.7%	93%
180 秒	90.9%	89%	87.3%
240 秒	90.9%	87.4%	85.8%
270 秒	86.8%	82.8%	81%
300 秒	86.8%	82.1%	80.3%

DOS attack 的模擬中，初始能量設置為 1000J，模擬時間為 300 秒，觀察感測節點 1 在 DOS attack 影響下所剩餘的能量並進行比較。圖 16 為使用 SPM、使用一般 PM 在工作狀態被攻擊及使用一般 PM 在睡眠狀態被攻擊之比較，use general PM (attack in active)這條線代表為使用一般 PM 時，攻擊節點在 Source 端開始進行資料封包傳送時進行攻擊，use general PM (attack in sleeping)這條線為使用一般 PM 時，攻擊節點在其他節點處於休眠狀態時就進行攻擊，當攻擊發生時，感測節點會持續接收攻擊節點的垃圾封包，導致節點 1 電量耗盡。attacked by using SPM 為加入了 SPM 後的剩餘能量圖，感測節點在接收到攻擊節點的訊號會因為還沒達到 break-even point 而無法被喚醒，如此一來就能有效的防止感測節點持續的接收攻擊節點的垃圾封包。表 5 表示出各狀態轉換點之能量，分別為使用 SPM 的情況、在工作狀態開始時遭受攻擊以及在休眠狀態下就遭受攻擊。模擬結果顯示出 SPM 能夠有效的防止 DOS attack 所造成的能量損耗。在經過 300 秒後，模擬結果比較顯示出，SPM 比起一般的 PM 能夠有效的節省約 78.6%的能量，如表 6 所示。

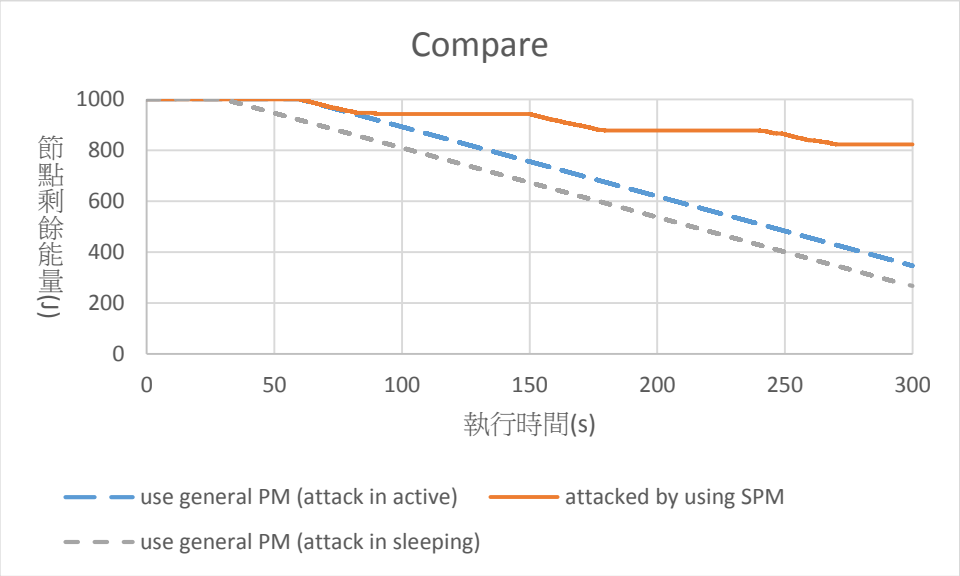

圖 16 使用 SPM、使用一般 PM 在工作狀態被攻擊及使用一般 PM 在睡眠狀態被攻擊比較圖

表 5 使用 SPM、使用一般 PM 在工作狀態被攻擊及使用一般 PM 在睡眠狀態被攻擊比較表

能量 / 時間	attacked by using SPM	use general PM (attack in active)	use general PM (attack in sleeping)
60 秒	99.9%	99.9%	91.4%
90 秒	94.2%	92%	83.9%
150 秒	94.2%	75.5%	67.5%
180 秒	87.7%	67.2%	58.7%
240 秒	87.7%	50.8%	24.2%
270 秒	82.3%	42.6%	34.6%
300 秒	82.3%	34.7%	26.7%

表 6 模擬 300 秒之能量節省比較

	Hello Flood attack	DOS attack
attacked by using SPM V.S. use general PM (attack in active)	4.7%	55.6%
attacked by using SPM V.S. use general PM (attack in sleeping)	6.5%	78.6%

在 Sinkhole attack 的攻擊模式下，初始能量設置為 1000J，模擬時間為 300 秒，觀察感測節點 15 在 Sinkhole attack 影響下所剩餘的能量並進行比較。圖 17 為模擬結果比較，模擬結果顯示，無論使用一般電源管理或是 SPM 都無法有效地阻止 Sinkhole attack 並節省能耗。最大原因在於 Sinkhole attack 的攻擊模式中，攻擊節點只會在受害節點在工作模式下才會發送虛假訊息騙取傳輸端節點和其建立路由， SPM 是採取 break-even point 的機制，因此，加入 SPM 並無法有效的防禦 Sinkhole attack。

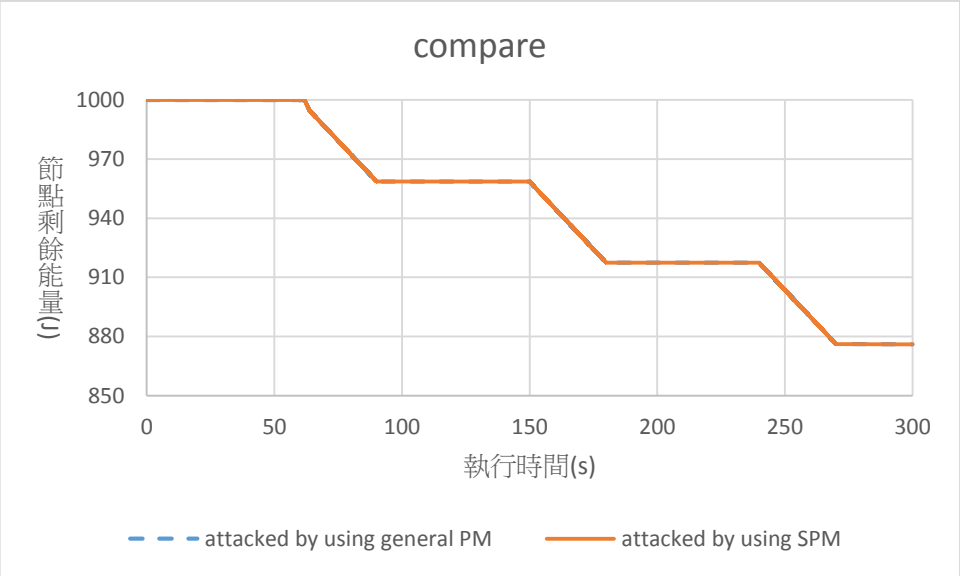

圖 17 使用 SPM、使用一般 PM 被攻擊比較圖

模擬結果經過分析後顯示出，和一般電源管理方案比較，使用 SPM 能夠有效的抵禦攻擊對電源造成的影響，節省不必要能耗，使感測節點的壽命能夠延長。

第五章 結論與未來研究

在本論文中，提出了一個用於無線感測網路中的 SPM，以應對當惡意攻擊發生時無線感測網路所產生的電源問題。SPM 能有效地使處於空閒模式的無線感測網路節點進入睡眠模式，並且在必要的時候喚醒它們。標記策略使得無線感測網路在休眠模式和工作模式的切換上更能夠節省能耗。模擬結果表示出，當網路遭受攻擊時，和一般的電源管理方案[26]相比，SPM 在 Hello Flood attack 中能有效地降低 6.5%之能耗，在 DOS attack 中能有效降低 78.6%之能耗。

雖然 SPM 機制能夠有效的抵禦 Hello Flood attack 以及 DOS attack，但卻無法有效的抵禦 Sinkhole attack，甚至導致反效果，在未來的後續研究中，我們希望可以結合 SPM 以及其他的防禦機制來研究出能夠抵抗所有無線感測網路惡意攻擊的方法，以達到更有效的電源管理防禦機制。

參考文獻

[1] L.A. Barroso, "The Price of Performance," *ACM Queue*, vol. 3, no. 7, pp. 48-53, Sept. 2005.

[2] A. Gandhi, M. Harchol-Balter and R. Raghunathan, "Distributed, Robust Auto-Scaling Policies for Power Management in Compute Intensive Server Farms," *Proceedings of Open Cirrus Summit*, pp. 1-5, Oct. 2011.

[3] R. David, P. Bogdan, R. Marculescu and U. Ogras, "Dynamic Power Management of Voltage-Frequency Island Partitioned Networks-on-Chip using Intel's Single-chip Cloud Computer," *Proceedings of IEEE/ACM International Symposium on Networks on Chip*, pp. 257-258, May 2011.

[4] F. Shearer, *Power Management in Mobile Devices*, Elsevier, USA, 2008.

[5] A. Sinha and A. Chandrakasan, "Dynamic Power Management in Wireless Sensor Net-works," *IEEE Design & Test of Computers*, vol. 18, no. 2, pp. 62-74, Aug. 2002.

[6] R.C. Luo and O. Chen, "Mobile Sensor Node Deployment and Asynchronous Power Man-agement for Wireless Sensor Networks," *IEEE Industrial Electronics*, vol. 59, no. 5, pp. 2377-2385, May 2012.

[7] S. Aram, I. Khosa and E. Pasero, "Conserving Energy Through Neural Prediction of Sensed Data," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Depend-able Applications*, vol. 6, no. 1, pp. 74-97, March 2015.

[8] W. Dargie, "Dynamic Power Management in Wireless Sensor Networks: State-of-the-Art," *IEEE Sensors Journal*, vol. 12, no. 5, pp. 1518-1528, May 2012.

[9] D. Meisner, C. M. Sadler, L.A. Barroso, W. Weber, and T. F. Wenisch, "Power Manage-ment of Online Data-Intensive Services," *Proceedings of Annual International Symposium on Computer Architecture*, pp. 319-330. June 2011.

[10] E. Popovici, M. Magno, and S. Marinkovic, “Power Management Techniques for Wireless Sensor Networks: a Review,” *Proceedings of IEEE International Workshop on Advances in Sensors and Interfaces*, pp. 194-198, June 2013.

[11] Z. Wu, M. Xie, and H. Wang, “On Energy Security of Server Systems,” *IEEE Dependable and Secure Computing*, vol. 9, no. 6, pp. 865-876, Nov./Dev. 2012.

[12] P. Bose, A. Buyuktosunoglu, J.A. Darringer, M.S. Gupta, M.B. Healy, H. Jacobson, I. Nair, J.A. Rivers, J. Shin, A. Vega and A.J. Weger, “Power Management of Multi-core Chips: Challenges and Pitfalls,” *Proceedings of IEEE Design, Automation & Test in Eu-rope Conference & Exhibition Conference*, pp. 977-982, March 2012.

[13] A. Lungu, P. Bose, A. Buyuktosunoglu and D.J. Sorin, “Dynamic Power Gating with Quality Guarantees,” *Proceedings of ACM/IEEE International Symposium on Low Power Electronics and Design*, pp. 377-382, Aug. 2009.

[14] M. Pirretti, S. Zhu, V. Narayanan, P. McDaniel, M. Kandemir and R. Brooks, “The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defense,” *Hindawi In-ternational Journal of Distributed Sensor Networks*, vol. 2, no 3, pp. 267-287, Sept. 2006.

[15] T.K. Buennemeyer, M. Gora, R.C. Marchany and J.G. Tront, “Battery Exhaustion Attack Detection with Small Handheld Mobile Computers,” *Proceedings of IEEE Portable Infor-mation Devices Conference*, pp. 1-5, May 2007.

[16] S. Kundu, S. Das, A.V. Vasilakos and S. Biswas, “A modified Differential Evolution-based Combined Routing and Sleep Scheduling Scheme for Lifetime Maximization of Wireless Sensor Networks,” *Soft Computing*, vol. 19, no. 3, pp. 637-659, March 2015.

[17] K. Witheephanich, J.M. Escaño, D. Muñoz de la Peña and M.J. Hayes, “A Min–Max Model Predictive Control Approach to Robust Power Management in Ambulatory Wire-less Sensor Networks,” *IEEE Systems Journal*, vol. 8, no. 4, pp. 1060-1073, Aug. 2013.

[18] F. Salvadori, M. de Campos, P.S. Sausen, R.F. de Camargo, C.

Gehrke, C. Rech, M.A. Spohn and A. C. Oliverira, "Monitoring in Industrial Systems Using Wireless Sensor Net-work With Dynamic Power Management," *Instrumentation and Measurement*, vol. 58, no. 9, pp. 3104-3111, Sept. 2009.

[19] M.R. Ogiela, A. Castiglione and I. You, "Soft Computing for Security Services in Smart and Ubiquitous Environments," *Soft Computing*, vol. 18, no. 9, pp. 1655-1658, Aug. 2014.

[20] T.A. Zia and A.Y. Zomaya, "A Lightweight Security Framework for Wireless Sensor Networks," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, no. 3, pp. 74-87, Sept. 2011.

[21] G. Wu, Z. Liu, L. Yao, Z. Xu and W. Wang, "A Fuzzy-based Trust Management in WSNs," *Journal of Internet Services and Information Security*, vol. 3, no. 3/4, pp. 124-135, Nov. 2013.

[22] K. Ren, W. Lou and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Secu-rity in Wireless Sensor Networks," *IEEE Mobile Computing*, vol. 7, no 5, pp. 585-598, May 2008.

[23] Smart Dust Project, http://robotics.eecs.berkeley.edu~pisterSmartDust

[24] Z. Hu, A. Buyuktosunoglu, V. Srinivasan, V. Zyuban, H. Jacobson and P. Bose, "Microar-chitectural Techniques for Power Gating of Execution Units," *Proceedings of ACM/IEEE International Symposium on Low Power Electronics and Design*, pp. 32-37, Aug. 2004.

[25] C.C. Hu, *Modern Semiconductor Devices for Integrated Circuits*, Pearson College Div., March 2009.

[26] Q. Wang and W. Yang, "Energy Consumption model for Power Management in Wireless Sensor Networks," *Proceedings of IEEE Conference on Sensor, Mesh and Ad Hoc Com-munications and Networks*, pp. 142-151, June 2007.

[27] G. J. Pottie and W. J. Kaiser, "Wireless integrated network sensors," *Communications of the ACM*, vol. 43, pp. 51-58, 2000.

[28] M. Pedram and J. M. Rabaey, *Power aware design methodologies*: Springer Science & Business Media, 2002.

[29] WINS project, Rockwell Science Center. Available: http://wins.rsc.rockwell.com

[30] M. Younis, M. Youssef, and K. Arisha, 'Energy-aware routing in cluster-based sensor networks,'' in *Modeling, Analysis and Simulation of Computer and Telecommunications Systems, 2002. MASCOTS 2002. Proceedings. 10th IEEE International Symposium on*, 2002, pp. 129-136.

[31] M. Magno, D. Boyle, D. Brunelli, B. O'Flynn, E. Popovici, and L. Benini, "Extended wireless monitoring through intelligent hybrid energy supply," *Industrial Electronics, IEEE Transactions on,* vol. 61, pp. 1871-1881, 2014

[32] D. Boyle, M. Magno, B. O. Flynn, D. Brunelli, E. Popovici, and L. Benini, "Towards persistent structural health monitoring through sustainable wireless sensor networks," in *Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2011 Seventh International Conference on*, 2011, pp. 323-328.

[33] H. Ishikuro, "Energy Harvesting Technology," 2011.

[34] S. Roundy, P. K. Wright, and J. M. Rabaey, *Energy scavenging for wireless sensor networks*: Springer, 2003.

[35] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," in *ACM SIGOPS operating systems review*, 2000, pp. 93-104.

[36] A. Sinha and A. Chandrakasan, "Dynamic power management in

wireless sensor networks," *Design & Test of Computers, IEEE,* vol. 18, pp. 62-74, 2001

[37] B. Brock and K. Rajamani, "Dynamic power management for embedded systems," in *Proceedings of the IEEE SOC Conference*, 2003, pp. 1-25.

[38] J. Hui, Z. Ren, and B. H. Krogh, "Sentry-based power management in wireless sensor networks," in *Information Processing in Sensor Networks*, 2003, pp. 458-472.38

[39] B. H. Calhoun and A. P. Chandrakasan, "Standby power reduction using dynamic voltage scaling and canary flip-flop structures," *Solid-State Circuits, IEEE Journal of,* vol. 39, pp. 1504-1511, 2004.

[40] R. M. Passos, C. J. Coelho Jr, A. A. Loureiro, and R. A. Mini, "Dynamic power management in wireless sensor networks: An application-driven approach," in *Wireless On-demand Network Systems and Services, 2005. WONS 2005. Second Annual Conference on,* 2005, pp. 109-118.

[41] P. S. Sausen, J. R. de Brito Sousa, M. A. Spohn, A. Perkusich, and A. M. N. Lima, "Dynamic power management with scheduled switching modes," *Computer Communications,* vol. 31, pp. 3625-3637, 2008.

[42] K. Venkatraman, J. V. Daniel, and G. Murugaboopathi, "Various attacks in wireless sensor network: survey," *International Journal of Soft Computing and Engineering,* vol. 3, 2013.43

[43] M. C. Domingo, "Securing underwater wireless communication networks," *Wireless Communications, IEEE,* vol. 18, pp. 22-28, 2011.

[44] D. E. Burgner and L. A. Wahsheh, "Security of wireless sensor

networks," in *Information Technology: New Generations (ITNG), 2011 Eighth International Conference on*, 2011, pp. 315-320.

[45] J. Malhotra, "Review on Security Issues and Attacks in Wireless Sensor Networks," *International Journal of Future Generation Communication and Networking*, vol. 8, pp. 81-88, 2015.

[46] T. Issariyakul and E. Hossain, *Introduction to network simulator NS2*: Springer Science & Business Media, 2011.

[47] S. Kurkowski, T. Camp, and M. Colagrosso, "MANET simulation studies: the incredibles," *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 9, pp. 50-61, 2005.

[48] Technology Review, http://www.technologyreview.com

[49] Z. Zhuohui, "21 ideas for the 21st century", Business Week, Aug. 30 1999.

[50] M. A. Hussain, P. Khan, and K. K. Sup, "WSN research activities for military application," in *Proceedings of the 11th international conference on Advanced Communication Technology-Volume 1*, 2009, pp. 271-274.

[51] D. Anguita, D. Brizzolara, A. Ghio, and G. Parodi, "Smart plankton: a nature inspired underwater wireless sensor network," in *Natural Computation, 2008. ICNC'08. Fourth International Conference on*, 2008, pp. 701-705.

[52] M. A. Mehaseb, Y. Gadallah, and H. El-Hennawy, "WSN application traffic characterization for integration within the internet of things," in *Mobile Ad-hoc and Sensor Networks (MSN), 2013 IEEE Ninth International Conference on*, 2013, pp. 318-323.

[53] J. Kenyeres, Š. Šajban, P. Farkaš, and M. Rakus, “Indoor experiment with WSN application,” in *MIPRO, 2010 Proceedings of the 33rd International Convention*, 2010, pp. 863-866

[54] A. Mathur, T. Newe, and M. Rao, “Healthcare WSN: Cluster Elections and Selective Forwarding Defense,” in *Next Generation Mobile Applications, Services and Technologies, 2015 9th International Conference on*, 2015, pp. 341-346.

[55] D. Li, W. Liu, Z. Zhao, and L. Cui, “Demonstration of a wsn application in relic protection and an optimized system deployment tool,” in *Information Processing in Sensor Networks, 2008. IPSN'08. International Conference on*, 2008, pp. 541-542.

[56] M. Lombardo, J. Camarero, J. Valverde, J. Portilla, E. de la Torre, and T. Riesgo, “Power management techniques in an FPGA-based WSN node for high performance applications,” in *Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 2012 7th International Workshop on*, 2012, pp. 1-8.

[57] E. P. kaur and A. Nayyar, “Conceptual representation and Survey of Dynamic Power Management (DPM) in Wireless Sensor Network,” *International Journal of Future Generation Communication and Networking*, vol. 3, pp. 165-169, 2013.

[58] J. P. Singh and L. Kumar, “A Survey on Power Management Techniques in Wireless Sensor Network,” *International Journal for Science and Emerging Technologies with Latest Trends*, vol. 1, pp. 31-35, 2013.