東 海 大 學 資 訊 工 程 學 系 研 究 所

碩士論文

指導教授：林祝興 博士
Dr. Chu-Hsing Lin

使用協同式強節點機制解決無線感測網路擁塞問題之研究

Using Cooperative Strong Node Mechanism to Solve Congestion Problem in Wireless Sensor Networks

研究生：林泓彥
Hung-Yan Lin

中 華 民 國 一 〇 一 年 六 月

東海大學碩士學位論文考試審定書

東海大學資訊工程學系 研究所

研究生 林 泓 彥 所提之論文

使用協同式強節點機制解決無線感測網路擁塞問題之研究

經本委員會審查，符合碩士學位論文標準。

學位考試委員會
召 集 人 ＿＿＿＿＿＿＿＿ 簽章

委 員 ＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿

＿＿＿＿＿＿＿＿

指 導 教 授 ＿＿＿＿＿＿＿＿ 簽章

中華民國 101 年 6 月 26 日

Abstract

In recent years, due to fast development of wireless sensor networks, the numbers of nodes are increasing, and their scope of applications is continuously expanding, including environmental monitoring, military and Smart home applications. The power supply, memory and computing power of wireless sensor nodes are greatly hampered in wireless sensor networks so that the wireless sensor networks are classified as a task-oriented framework. This study focused on exploring problems caused by traffic congestion on the wireless sensor networks with a large amount of flow, such as packet loss, bandwidth reduction, and waste of energy on the sensor nodes. We proposed a cooperative strong node mechanism, in which a threshold is set to determine whether the node traffic is over. When the load exceeds, the privilege of corresponding sensor nodes is upgraded so that it can command its child nodes to change the transmission path to effectively distribute the traffic; furthermore, when the traffic exceeds preset overall network flow, new sensor nodes are added in the network to relieve the traffic. This mechanism can increase network throughput and effectively prevent the occurrence of congestion problems, and is suitable for a variety of routing protocols.

Keywords: Wireless sensor networks, Packet loss, Throughput, Congestion problems

TUNGHAI UNIVERSITY

中文摘要

近年來，因無線感測網路技術快速的發展，使得其應用範圍不斷地擴大，節點的數量也不斷地增加，包括環境監測(Environmental monitoring)、軍事用途(Military)、智慧家庭(Smart home)等方面。在無線感測網路中，無線感測節點裝置本身所配備之電源、記憶體以及運算能力等均受到極大的限制，因此無線感測網路是被歸類為以任務為導向的應用網路型態。此研究的重點在於探討當無線感測網路因為流量過大時而發生的擁塞問題，擁塞的發生可能造成封包遺失、頻寬降低及感測節點能量的浪費，我們以更改傳輸路徑的方式為基礎，提出一個協同式強節點機制，藉由設定一個門檻判斷節點流量是否超過危險值，當緩衝區剩餘的空間過低時，將該節點的權限提升，使該節點具有命令其子節點改變傳輸路徑的權力，可以有效的將流量分散，並且在網路超過負荷時，加入新的感測節點舒緩，而不需重新對原有的感測節點作設定，此機制能提高網路吞吐量且有效防止擁塞問題發生，此方法適用於多種路由協定。

關鍵詞：無線感測網路, 封包遺失, 吞吐量, 擁塞問題

致謝

在研究所學習的歲月中，首先感謝指導教授林祝興博士的諄諄教誨，老師給我充分的支持和指導，並給予很大的發揮空間，使我的研究能照自己的學習領域及興趣進行，老師不僅僅在學術方面讓學生有卓越的成長，在心靈層面更讓學生收穫良多。同時，也要感謝劉榮春教授，有了劉老師的大力幫忙與指導，使本篇論文的內容更加完美與嚴謹。感謝參與學生碩士班口試的委員：楊中皇教授、王旭正教授、陳雍宗教授、賴威伸教授。有了教授們的指正與建議，使得這篇論文更加完整。

這篇論文能順利地完成，更要感謝父親以及母親的支持與鼓勵，讓我可以在這段時間中無後顧之憂的專心在學業與研究上。接著要感謝鎮宇學長，學長在專業領域上給我非常多的幫助，遭遇困難時給我許多意見，還有同學棠滙、信斌、詩蓓，在這段時間彼此互相鼓勵成長。感謝奇軒學弟、明竑學弟、俊良學弟、侑廷學弟、紘侑學弟，因為有你們，實驗室總是充滿著溫馨歡樂的氣氛，以及在許多部分給予我幫助，使我能夠專注的準備論文及口試。最後要感謝的是郁淳，在這段期間給予我支持與包容，陪我度過這段時間的喜怒哀樂。

最後再次感謝所有的父母、師長、同學和學弟妹們，感謝你們的陪伴、支持與鼓勵。

林泓彥　謹識

於東海大學資訊工程學系研究所

資訊安全實驗室

2012 年 7 月

Contents List

Figure List

Table List

Chapter 1
Introduction

1.1 Overview

In recent years, wireless communications transmission gradually replaced the traditional wired transmission. The wireless sensor network composed by many sensor nodes is a major field of study in wireless communications. The sensor node has four units: sensing unit, processing unit, transceiver unit, and power unit. These nodes can detect states within its sensing range, such as temperature, humidity, sound, and pressure. The wireless sensor nodes equipped with limited power, memory and computing capability, so wireless sensor networks are classified as a task-oriented application network type. In addition, the main protocols of wireless sensor network is IEEE 802.15.4 for Low Rate-Wireless Personal Area Networks (LR-WPANs), task group 4 (TG4) within the IEEE 802.15 specifications. Characteristics of the LR-WPAN wireless sensor networks are a low rate, low energy consumption, low cost, and they support a large number of sensor nodes. In wireless sensor networks applications, there are hundreds to tens of thousands sensor nodes, which leads to very complex network operations. In this study, we focus on avoiding the congestion problems and increasing the packet arrival rate in a large network environment.

1.2 Motivation

In wireless sensor networks, energy management and packet loss have been the focus of discussion. Many routing protocols have been designed for these problems, such as Low-Energy Adaptive Clustering Hierarchy (LEACH), Threshold Sensitive Energy Efficient Sensor Network Protocol (TEEN), Hybrid Energy-Efficient Distributed Clustering (HEED), Geographic Adaptive Fidelity (GAF), Geographic and Energy Aware Routing (GEAR), and Simple Least-Time Energy Routing Protocol with One-Level Data Aggregation (LEO). These routing protocols can be used to reduce energy consumption and distribute traffic. However, with increasing number of nodes, packets processed by each node significantly increase. There is no guarantee that nodes with large flow do not exhaust all energy or have traffic congestion due to overloading, leading to packet loss or node failure. The existing routing protocol solution is to change the transmission path when packet traffic over the loading limit, which trades off the transmission efficiency for the benefit of traffic dispersion. Although it works in some cases, but when the traffic of all other paths exceeds loading limits in the same time, the wireless sensor networks will collapse. At this point, new nodes are needed to be added in the network to quickly work together with the original nodes.

In this thesis, we propose a Cooperative Strong Node Mechanism (CSNM) based on the change of the transmission path method. Compared with the previous protocols, it not only makes accurate selection of alternate paths, but also quickly adapt to the original network when a new node is required to be added in. Both in the Hierarchical protocols or Location-based protocols, when node traffic will soon exceed the load limit, the privilege level of nodes will be elevated and it can command its child nodes to change the transmission path. Compared to other distributed traffic agreements, we focus on the part of selection of alternate paths. In order to accurately select alternative paths, we will consider the following three factors: the remaining buffer size, residual energy, and the number of hops to the base station. In addition, this mechanism also has the advantage that the new added node can automatically adapt to the existing network and quickly become operational. The proposed method will be described in detail in later chapters.

1.3 Organization of Thesis

The rests of this thesis are as follows. Chapter 2 reviews related work and the basic concept of wireless sensor networks. Chapter 3 introduces the proposed method, the Cooperative Strong Node Mechanism (CSNM). In Chapter 4, we describe the simulation environment and method, and compare the simulation results of the proposed method with existing related agreements. Chapter 5 concludes this thesis.

Chapter 2
Related Work and Background

2.1 The Wireless Sensor Network

Wireless sensor networks consist of a lot of sensor nodes to monitor and measure sound, light, air vibration or temperature, etc. They can also send data to the base station with simple computing and wireless communication capabilities. In order to achieve a large scale of deployment, the sensor nodes have low cost, low power, small size and easy to deploy features and they can be used in a hospital, in the military, the warehouse, and at home for management and automation. Nowadays, ZigBee is referred to the wireless sensor network, rather than Wireless Ad-hoc Network (WANET), although both have similar structure, but there are many different natures between them. The focus of this study is on the ZigBee applications.

In December 2004, the official version for the ZigBee 1.0 specification was released by the ZigBee Alliance [1]. The alliance was initially set up by Honeywell, Invensys, Mitsubishi, Motorola and Philips, and the number of alliance members so far has more than 200 companies and extends to 26 countries. The name idea of ZigBee is by the bees: the bee doing the Z-shaped fly to inform peers of the pollen. The development objective is to create the wireless network with a low data transfer rate, low power and low complexity. It can work for at least a few months or even for a year with a battery. The ZigBee has three characteristics, as detailed below:

1. Low power consumption

The low data transfer rate of Zigbee devices let them send and receive data by less time. They are in the non-operating mode when the device is in the sleep mode. To send and receive data, they will wake up again. In the sleep mode, the device consumes very low power, and it allows ZigBee to operate on only batteries for several months or even up to one year.

2. High reliability

ZigBee employs a collision avoidance mechanism on the MAC layer. When a node receives a packet, it sends a confirmation message to inform the sender. If the sender does not receive a confirmation message, which means that the packet collided with other packets, then it will retransmit the same packet. The collision avoidance mechanism increases reliability of the transmission system.

3. High scalability

In order to achieve the aim of wide deployment, a ZigBee network can support up to 255 devices to each communication link; and the network can be expanded up to thousands or even tens of thousands of devices by using a ZigBee network coordinator.

ZigBee is a specification based on the IEEE 802.15.4 wireless standard that employs the standard of low-rate wireless personal area networks (LR-WPANs) such as physical layer (PHY) and media access control layer (MAC). ZigBee operates in three radio bands. The MAC layer provides flow control, network organization, and data encryption (AES-128) services. The radio band of its license-free radio channels and the application areas are as shown in Table 1, and its transmission range is from 10 to 75 meters.

Table 1 Operation bands of IEEE 802.15.4 specification

Operation Bands	868.0 ~ 868.6 MHz	902 ~ 928 MHz	2.4 ~ 2.4835 GHz
Area	Europe	Americas	Worldwide
Channels	1	10	16
Data rate	20 Kbps	40 Kbps	250 Kbps

While ZigBee and IEEE 802.15.4 architecture is similar, but there are some different as shown in Figure 1. In November 2007, the Alliance completes development of ZigBee 2.0 specification to provide more function of networks.

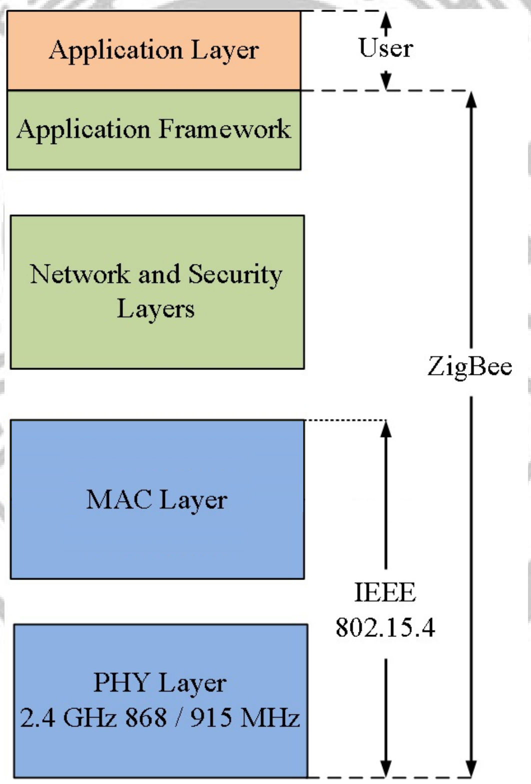


Figure 1 The relationship between IEEE 802.15.4 and ZigBee.

ZigBee supports the star topology, mesh topology (also known as point to point), and cluster tree topology networks as shown in Figure 2. There are three types of network devices:

- ZigBee coordinator (ZC)

It is the most powerful among these three devices. It can be used as the root of the network tree and can also be used as the router of the network. The coordinator has more memory than the other two types, and it has greatest computing and power supply abilities. There is only one coordinator in a network.

- ZigBee Router (ZR)

The ZigBee router can act as a relay router as well as a coordinator, but it has limited computing capacity and power. It can immediately communicate to all types of device, and relays data from other devices to the base station.

- ZigBee End Devices (ZED)

It contains the least functions. A router can only communicate with parent nodes (ZigBee routers only), and it has least memory. So it is less expensive than the ZigBee coordinator and router. The end device cannot relay data from other devices to reduce cost and setup complexity. It is suitable for simple applications because it can switch to the sleep mode to save energy.

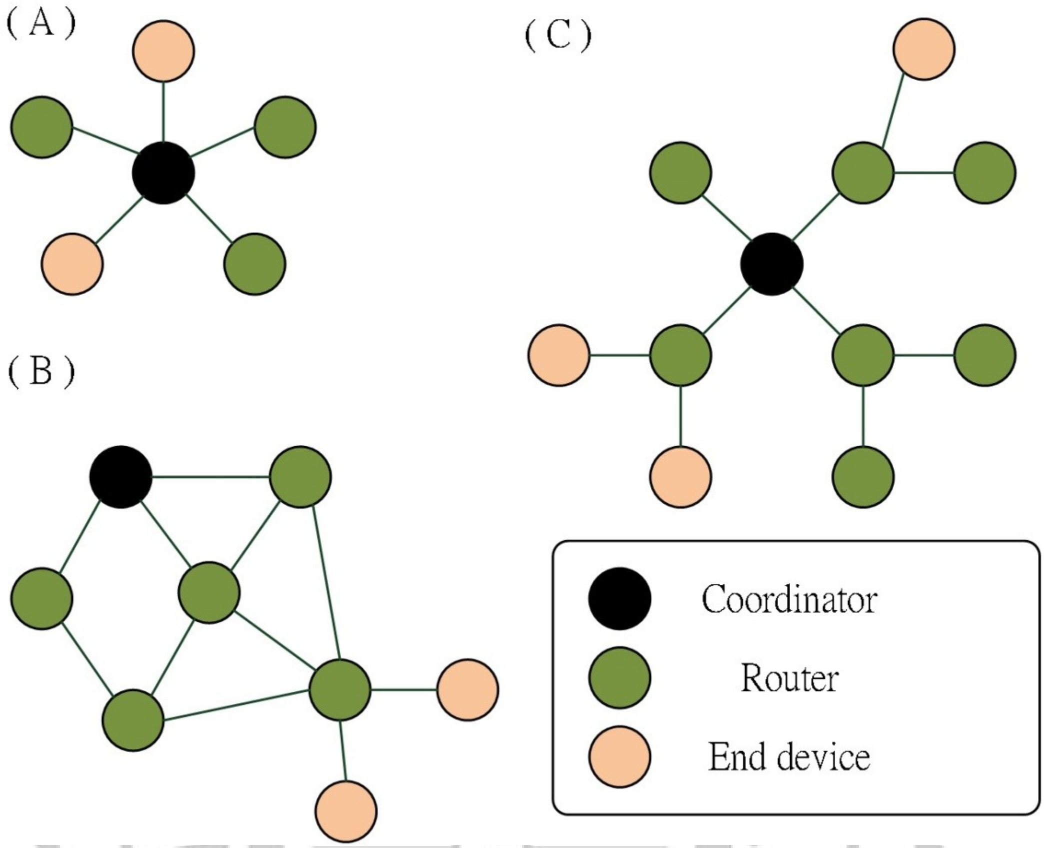


Figure 2 Topologies of ZigBee: (a) Star topology (b) Mesh topology (c) Cluster.

In Figure 2 (a), the devices in a star topology directly communicate with the central coordinator of the network. In this case, the ZigBee coordinator is the most powerful device in the network, and the other devices are only equipped with batteries to maintain operation. The star topology is more suitable for applications in smaller areas such as home. Figure 2 (b) shows that the mesh topology allows nodes transmit and relay by multi-hops to reach the ZigBee coordinator. The mesh topology provides high reliability structure with a scalable range. Figure 2 (c) shows a cluster tree topology, in which most devices are ZigBee routers. The ZigBee routers have communication links to ZigBee end devices as leaf nodes, and relay data to the ZigBee coordinator. The routers are responsible for communicating with the coordinator. There is only one coordinator for each network (the black node in Figure 2). The advantage of the cluster structure is that it can increase the range of the radio signal coverage for data communication.

2.2 Congestion Control Schemes

In this section, we briefly describe various congestion control schemes in WSNs. They can be classified into priority-based, rate-based, and buffer-based schemes.

2.2.1 Priority-Based Scheme

In the priority-based scheme [2], it emphasized the importance of priority mainly. Most recent researches about congestion control for wireless sensor networks only guarantee simple fairness, which means that the sink receives the same throughput from all sensors. In fact, sensors might deployment in different places, have the difference of hardware or capacity and the sensing events are different. Therefore, the priorities of sensors may be different. The importance sensors have higher priority, which means the importance sensors can gain higher throughput. In [3] a priority-based congestion control protocol is proposed. This scheme uses packet inter-arrival time along with packet service time to measure a parameter defined as congestion degree and furthermore imposes hop-by-hop control based on the measured congestion degree as well as the node priority index. The packet inter-arrival time (t_a^i) is defined as the time interval between two sequential arriving packets and the packet service time (t_s^i) is referred to as the time interval between the time a packet arrives at the MAC layer and the time its last bit is successfully transmitted. Based on the average inter-arrival time and average service time, It defines a new congestion index; congestion degree *d(i)* = t_s^i/t_a^i. If *d(i)* is larger than 1, the node experiences congestion. Each sensor node i has dependent congestion degree in the header of data packets to be forwarded. The notification is triggered when the node overhears a congestion notification from its parent node in a time period. Finally, each node allocates data rate to its upstream nodes according to their priorities.

2.2.2 Rate-Based Scheme

The basic idea of the rate-based scheme is for a forwarding node to estimate the number of flows coming from each upstream neighbor and assign transmission rate in accordance with the fairness when congestion is detected. In [4] an event-to-sink reliable transport protocol (ESRT) is proposed for congestion control. ESRT is a centralized protocol to regulate the reporting rate of sensors in response to congestion detected by sink. Each sensor node monitors its local buffer level and sets a congestion notification bit in the packets forwarded to sink if the buffers overflow. When the sink receives a packet with the congestion notification bit set, it infers congestion and broadcasts a control signal notifying all source nodes to reduce their reporting frequency. A distributed congestion detection and avoidance protocol (CODA) is proposed in [5]. In CODA, if congestion is detected, the receiver will broadcast a suppressive message to its upstream neighbors and at the same time make local adjustment to prevent propagating the congestion downstream. When an upstream node receives a backpressure message, based on its own local network conditions it determines whether to further propagate the backpressure signal or not. This scheme does not consider the fairness issue. The authors in [6] propose a mitigating congestion protocol which combines three congestion mitigating mechanisms, hop-by-hop flow control, rate limiting and prioritized MAC layer. This scheme requires a tree routing structure to work correctly. A localized algorithm for aggregate fairness protocol is proposed in [7]. When a sensor receives packets more than it can forward, the sensor will calculate and allocate the date rates of upstream neighbors by a weighted fairness function. However, the fairness function of this congestion control protocol was not considered carefully with the remaining buffer size and transmission rate at the same time. It only considers that the sum of data rate from upstream neighbors must be less than the sum of data rate it can forward to downstream neighbors when congestion is detected.

2.2.3 Buffer-Based Scheme

In the buffer-based scheme, the key for congestion control makes sure that a sensor node i sends a packet to its downstream neighbor sensor node j only when j has buffer space to hold the packet. This scheme is simple and effective, but it does not consider the data rate of upstream and downstream neighbors. It eliminates the complicated rate-based signaling required by many existing congestion control approaches. This scheme, unlike the rate-based approaches, it does not loss packets. Let N_i be the set of the neighbors of node i. The remaining buffer size of i changes when it receives a packet from upstream neighbors or forward a packet to a downstream neighbor. When node i sends out a packet, it piggybacks its current buffer state in the frame header of package. Consider a neighbor sensor $j \in N_i$. When j receives or overhears a packet from i, it caches the buffer state of i. The sensor j has a packet to forward i, only if the buffer of i is not full. If the buffer of i is full, j withholds the packet until it overhears a packet from i, piggybacking a non-full buffer state. In [8] a congestion avoidance protocol based on lightweight buffer management in sensor networks is proposed. Although it can realize and guarantee the packet does not loss in the forwarding way, the buffer utilization is low.

Most of congestion control protocols did not consider buffer state and date rate at the same time. The rate-based scheme is for a forwarding node to estimate the number of flows coming from each upstream neighbor and assign rate in accordance with the fairness when the congestion is detected. The buffer-based scheme makes sure that a sensor i sends a packet to its downstream neighbor j only when j has buffer space to hold the packet. Both the two schemes consider either in data rate or buffer state to allocate the data rate for its upstream neighbors.

2.3 Routing Protocol

Routing protocols can be divided into three types of wireless sensor networks respectively as flat-based routing, hierarchical-based routing and location-based routing. In this section, we present a detailed review for some routing protocols.

2.3.1 Flat Routing

With flat routing, each sensor node plays the same role, and sensor nodes collaborate to perform the desired sensing task. Generally, the application of such network is data-centric over the network [9]. The BS broadcasts queries packet to interest area and wait for data from the sensor located in selected region. Since data will continue relay through queries, it is necessary to specify the interest data until found. Since it is a simple protocol, it can be applied on sensor node lack of resource. But this category protocol does not possess effectively energy conservation due to the information obtained via broadcast coordination. At the same time, they transmit data to all sensor nodes by flooding. It has also bandwidth limited issue. In flat routing, they can be divided into several protocols. SPIN [10], and Directed Diffusion [11] provide obvious examples.

Sensor protocols for information via negotiation (SPIN) protocol is two network layer protocols based on data-centric routing, and the sensor nodes that have data to send broadcast to their neighbors and send the sensing data only to those nodes that are interested. To reduce the energy expended in the broadcast of advertisements, the SPIN protocol family uses meta-data descriptors, which describe the actual sensor data in a more compact size. SPIN works based on how much energy is remaining via access to the current energy level of the node and adapts the protocol. Besides, the SPIN family of protocols includes many protocols. The main two protocols are called SPIN-1 and SPIN-2.These protocols are suitable for an environment where the sensors are mobile, because they make their forwarding decisions based on local neighborhood information. In addition, one of the advantages of SPIN is that topological changes are localized since each node needs to know only its single-hop neighbors. However, SPINs data advance scheme cannot guarantee the delivery of data. Furthermore, the extravagant time spent in such activities might not suit some applications that require the sensor nodes to respond quickly to an emergency situation.

In Directed Diffusion, the base station broadcasts its interests to all sensor nodes in the network. Each sensor node stores the interest in its local cache, and uses the gradient fields within the interest descriptors to identify the most suitable path back to the base station. These paths are then used by source nodes to transmit the sensing data to the base station. For example, refer to Fig. 3(a), the base station initiates an interest flooding over the network. Each sensor setups a gradient toward the sensor nodes from which the interest was received (Fig.3 (b)). More generally, gradient information contains an attribute value and a direction. The strength of the gradient may be different among distinct neighbors, and thus results in different information flows. In Fig. 3(c), sensor node sending data to BS is along built gradient path. In addition, directed diffusion also combines the data coming from different sources route (data aggregation) by eliminating redundancy, minimizing the number of transmissions, thus saving network energy and prolonging its lifetime. However, this routing protocol can not apply to application that always requires delivery to the base station, because the query-driven on demand data model may not support in this regard. Furthermore, the sensor node may cause extra overhead for matching data by queries.

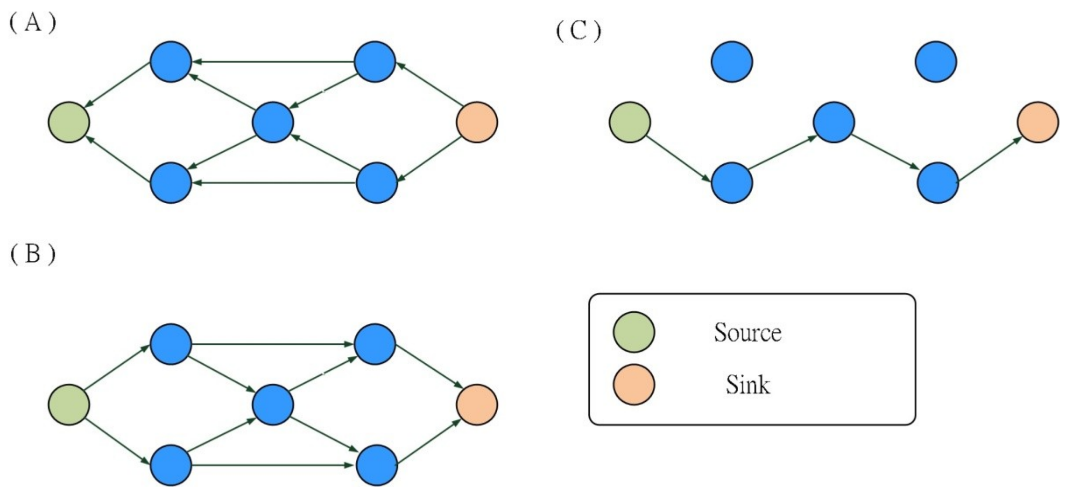


Figure 3 An instance of interest diffusion in sensor network.

2.3.2 Hierarchical-Based Routing

In this protocol, it has well-known techniques with special advantages related to scalability and efficient communication. As such, the concept of hierarchical routing is also utilized to perform energy efficient routing in WSNs. In hierarchical routing, during the network set up phase, sensor nodes are first grouped into a number of clusters by certain criteria (e.g. distance, location). For each cluster, a node is elected as cluster head (CH). Clusters in turns collectively formulate a hierarchical routing architecture. In data dissemination phase, member nodes in each cluster first transmit respective sensed data to their cluster heads, in which data aggregation or data fusion will be performed. The purpose of data aggregation is aimed at reducing the amount of transmitted messages, and thus saving energy expense. In addition, the cluster heads send them to the base station, using direct or multi-hop transmission methods. Most previous research on hierarchical network routing focused on the protocol design and performance evaluation in terms of the power conservation and prolong lifetime. Hierarchical routing makes its main contributions on network scalability, data reduction and energy conservation. Related researches include LEACH [12], LEACH-C, TEEN [13], APTEEN [14], DECHP [15], PEGASIS [16], etc.

The LEACH routing protocol makes contribution to balancing energy consumption of nodes, and constructs a simple two-level routing architecture for data transmission. The cluster head is formed by randomly selecting a few sensor nodes, and rotating this role to evenly distribute the energy load among the sensor in WSNs. During creation of clusters, each node decides to become a cluster or not in current round. This decision is made by node n to choose a random number between 0 ~ 1. When the number is less than a threshold T(n), the node becomes a cluster-head for the current round. P is the cluster-head probability and G is the set of nodes. The threshold is set as:

$$T(n) = \begin{cases} \frac{1}{1-p\times\left(r \bmod \frac{1}{p}\right)}, & if\ n\ \in G \\ 0, & otherwise \end{cases} \qquad (1)$$

Although LEACH is able to prolong the network lifetime, there are still issues with energy consumption in this protocol. For example, when cluster heads are far away from the base station, the energy may be quickly depleted and thus the whole network becomes out-of-function. In addition, the assumption on unlimited transmission range for sensor node makes it impractical. Moreover, the LEACH protocol always needs to rebuild its routing architecture after transmitting a certain amount of data. This implies that the protocol will increase some extra energy expenses, and thus shorten system lifetime. Beside, the head election of LEACH is random that that the desired number of cluster heads cannot be guaranteed to be elected or the elected heads be evenly positioned.

Another one routing protocol is a centralized version of LEACH. LEACH-C selects cluster head by the base station (BS). BS collects information regarding the location and energy level in sensor networks. Then, base station employs an annealing algorithm and average energy threshold condition to predetermine number of cluster heads and configure the network into clusters. These non-cluster heads are chosen as cluster head by minimizing the energy cost to the transmission distance. A centralized version of LEACH improves issue of random cluster head, but it still unsuitable for a large range of sensing environment.

On the other hand, TEEN and APTEEN reduce energy consumption by restricting the transmission number of data. They have two setup phases, i.e. proactive networks and reactive networks. The proactive networks are periodically switched on their sensors and transmitters to sense the environment and transmit the data of interest. This method is suitable for periodic data monitoring. By the way, reactive networks respond to violent changes of sensing environment. This scheme is suitable for time critical conditions. They filter available data by set up two thresholds: Hard/Soft threshold according to end user requirement to reduce transmissions of unnecessary data and energy consumption. The hard threshold tries to reduce the number of transmission by allowing the nodes to transmit only when the sensed attribute is in the range of interest. Another one, the soft threshold advance reduces the number of transmission that might have otherwise occurred when there is little or no change in the sensed attribute. Nevertheless, this scheme has one main drawback: if the thresholds are not received, the nodes will never communicate, and the user will not get any message from the network at all. Beside, this protocol still depends on architecture of LEACH, so it has energy conservation limits.

DECHP is a distributed cluster-based routing protocol, in which, each sensor node first computes its neighbor set, and then broadcasts its set to the neighbors for organizing local clusters. Only node with sufficient energy can by turns act as cluster head in each cluster. The CHs use a geographical (by GPS) and energy aware neighbor cluster head selection heuristic to relay their aggregated data. All non-cluster head nodes send their message to the CH, while the CH node receives message from neighbors of the cluster members, performs signal processing functions on the data (data aggregation) and forwards data to its upper level CH and so on still the data reaches the BS. Besides, based on the minimum learned cost, the CH picks up the suitable neighbor cluster head as its next-hop destination. Although this protocol can yield an improvement on network lifetime and averaged energy savings, it may consume a lot of energy on local cluster formation. Additionally, the cluster head may also pay much more time and energy to use a heuristic to choose its next hop. Moreover, a GPS system installed with the nodes also introduces a significant increase on hardware cost.

Lindsey and Raghavendra proposed a PEGASIS routing scheme. In their protocol, an optimal chain-based routing path is built before transmission. The basic method of the protocol is that in order to prolong network lifetime, each node in this chain communicates only with the nearest neighboring node, and will be elected as cluster head by turns for data aggregation. Thus, PEGASIS has two goals. First, to extend the lifetime of each node by employing collaborative skill and as a result the network lifetime will be increased. Second, each node is close together to reduce bandwidth consumed in communication due to local coordination. Although the PEFASIS avoids clustering overhead by dynamic form cluster, but it still requires dynamic topology adjustment since that a sensor node needs to know about adjustment can introduce significant overhead especially for highly utilized network. In addition, the protocol must take at least *O(n)* communication overheads to build its routing chain. It is therefore unsuitable for large sensor networks.

2.3.3 Location-Based Routing

In this routing, every node is known by its location, and the routing algorithm improves energy consumption and target tracing problem by location. The distance between neighboring nodes is able to be estimated by incoming signal strengths, and such information between neighbor forms relative coordinates of neighboring nodes. The location of nodes may be available directly by communicating with a satellite, or using Global Positioning System (GPS) if nodes are equipped with a small low power GPS receiver. To save energy, some location based schemes demand that nodes should go to sleep if there is no activity. Here we summarize the location or geographic based routing protocol. The GAF [17], GEAR [18] are used in this routing architecture.

The concept of virtual grids in the context of routing is used in GAF. All nodes in a virtual grid are equal from a routing perspective. GAF identifies redundant nodes within each virtual grid and switches off their radios to achieve energy savings. According to this protocol definition of a virtual grid, any node in an adjacent grid can communicate with each other. Therefore, GAF conserves energy by turning off unnecessary nodes in the network without affecting the level of routing fidelity. At the same, each node has GPS-indicated location to associate itself with a point in the virtual grid. But GAF cannot be used for flooding because of the small size of its grids; the density in the Network has to be very high for nodes to take advantage of GAF for saving energy. GAF is mainly designed for routing where nodes in a virtual grid maintain the condition that at least one node in the virtual grid is awake. This results in a significant overhead if used for minimizing retransmissions.

Geographic and Energy Aware Routing (GEAR) uses energy aware and geographically-informed neighbor selection heuristics to route a packet towards the destination region. It uses a recursive geographic forwarding technique to disseminate the packet on the inside of the region. In GEAR, each node keeps an estimated cost and a learning cost of reaching the destination by its neighbors. The estimated cost includes residual energy and distance to destination. The learned cost is exquisite estimated cost that accounts for routing around holes in the network. The key idea is to restrict the number of interests in directed diffusion by only considering a certain region rather than sending the interests to the whole network. Although these protocols can save the most energy consumption, they spend more cost on installing GPS device in the sensor node, a drawback for hardware design of sensor nodes.

In above description, we know that energy consumption mainly depends on transmission and reception in wireless sensor networks. As the results, they show that the hierarchical-based routing has obvious efficacy on energy conservation. It also prolongs system lifetime via data aggregation scheme. As a consequence, we develop an efficient energy routing protocol with hierarchical architecture, and propose a multi-level cluster framework applied on a large environment, at the same time reducing unnecessary transmission. The details are described in Chapter 3.

Chapter 3
Cooperative Strong Node Mechanism (CSNM)

A wireless sensor network is composed of many sensors. The hardware conditions, such as energy and memory, of these sensors are limited. To effectively extend the operating hours of the wireless sensor networks and solve the congestion problems are very important. There are two types of congestion in wireless sensor networks. One is channel collision and the other is buffer congestion. The first type of channel collision can be solved in MAC layer by CSMA, FDMA, TDMA, and CDMA [8]. A growing number of sensor networks use CSMA for medium access. For example, the widely used Berkeley motes use a simple CSMA MAC as part of the TinyOS platform. The CSMA can improve channel collision but cannot solve the congestion problem. It may cause the buffer of a sensor overflow if several neighbors of the sensor have packets with high data rate to the sensor.

Here we propose a new mechanism that can effectively solve the buffer congestion. The method called Cooperative Strong Node Mechanism (CSNM). The method is response to ACK_Packet with a warning message when the node will have excess load. The warning message is used to notify the particular child nodes of the need to change the path. Child node then broadcasts query_Packet to obtain the weight value of the neighbor, and selects an alternate node to solve the congestion problem. The details of the method will be given in the next section.

3.1 The Mechanism Phases

The functionality of the proposed mechanism could be divided into two modes when the node receiving a packet: general node mode and strong node mode. This section presents each mode in detail.

3.1.1 General Node Mode

General node mode is the basic mode of operation. In this mode, the node adopts the selected routing protocol, and when the buffer loading exceeds the threshold, it will switch the mode to the strong node mode and then begins to perform traffic dispersing action. Table 2 shows parameters of the pseudo code. The pseudo code of general node mode is depicted in Figure 4.

Table 2 The symbol definition for pseudo codes in Figure 4 and Figure 5.

Symbol	Definition
B_L	Buffer loading
B_S	Buffer size
HLTV_1	High load threshold value in general node mode
HLTV_2	High load threshold value in strong node mode
LL	Low load threshold

TUNGHAI UNIVERSITY 1955

```
General node mode( )
Function
Node receives the packet.
If(packet type is forwarding){
    Put the packet to the buffer.
    Update this node buffer load.
    If(buffer loading is higher than the HLTV_1){
        Return an ACK packet with a command to change the path.
        Set the node mode to strong node mode.
    }
    Else
        Return an ACK packet.
}
Else
    Put the packet to the buffer.
```

Figure 4 The pseudo code of general node mode.

3.1.2 Strong Node Mode

In the general node mode, when the buffer loading is higher than HLTV_1, the node will switch to the strong node mode. The node does not become an alternate node for the other nodes, when the node is in the strong mode. In strong node mode, the node will not respond to other nodes asking for the packet of node weight, and has permission to notify the child node to change the transmission path. In the strong node mode, when the buffer loading is lower than LL in the node, it switches back to the general node mode and provides an alternate node function. The pseudo code of strong node mode is depicted in Figure 5.

```
Strong node mode( )
Function
Node receives packet.
If(packet type is forwarding){
    Put the packet to the buffer.
    Update this node buffer load.
    If(buffer loading is higher than the HLTV_2)
        Return an ACK packet with a command to change the path.
    Else
        Return an ACK packet.
}
Else{
    Put the packet to the buffer.
    If(buffer loading is lower than the LL)
        Set the node mode to general node mode.
}
```

Figure 5 The pseudo code of strong node mode.

3.2 Congestion Avoidance and Control

Network congestion occurs when the assigned traffic load exceeds the available capacity at any point in the network [5]. Despite the fact that single path routing increases the probability of congestion occurrences, the congestion is very likely to happen even for multipath routing schemes. Congestion avoidance is the process of detecting incipient congestion and preventing its occurrence. Buffer loading is frequently used to detect incipient congestion [19][20]. Multipath routing is inherently an avoidance scheme since the traffic is distributed among the available paths and hence the congestion is somewhat avoided. The avoidance mechanism is designed to handle sudden increase in the amount of traffic. Although this kind of traffic is assumed to be transient and will stop when the event being monitored disappears, it is not always the case. The traffic may continue flowing in high rates if the sensors monitor a variety of physical phenomenon.

In our scheme, we use the buffer loading to detect occurrence of congestion problems. When the buffer loading is higher than the threshold, there are impending congestion problems, and so, the node mode is then switched into the strong node mode to disperse network traffic. When in the strong node mode, just change the transmission path of a child node, and observe changes of the node traffic. If it is not reduced or sustains in a saturated state, the node stays in the strong node mode. If the node traffic continues to increase, reaching the buffer loading threshold in the strong node mode, all its child nodes of the transmission path are changed into this state. As above, action to change the child nodes of the transmission path is divided in two stages. The reason is to avoid changing modes of all child nodes of the path at the same time, which will not alleviate congestion but only transfer the congestion to other nodes. Unless in the strong node mode, when the buffer loading is higher than HLTV_2, since the node has been unable to handle the current flow, a large number of sub-node path will be changed to effective relieve traffic. Figure 6 shows the state diagram of the node mode transfer.

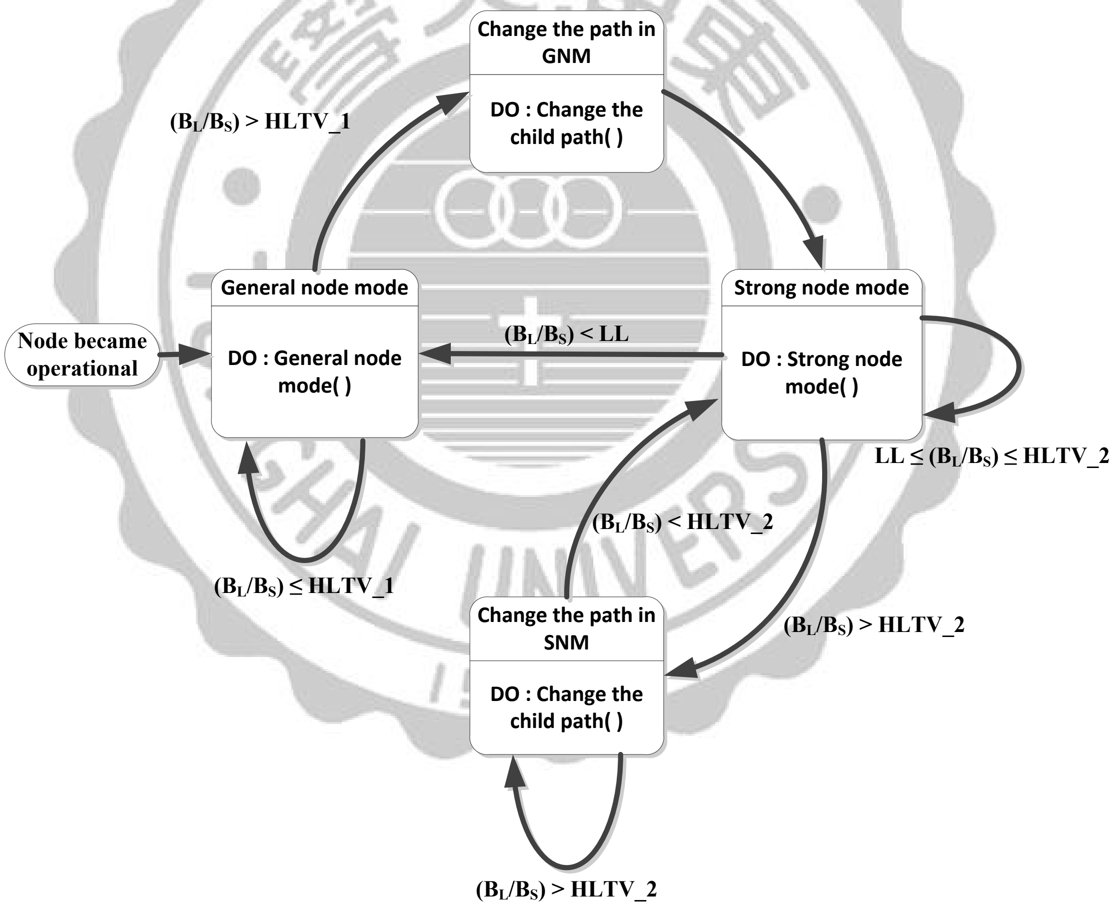


Figure 6 The state diagram of node mode transfer.

CSNM mainly avoids packets dropped by nodes due to high traffic loading. When a node is in danger of being overloading, part of the traffic is distributed to other nodes before the occurrence of the congestion problem. Figure 7 and Figure 8 show the operation of CSNM. Figure 7(a) indicates that the network in a normal state. Figure 7(b) shows an event occurs in node 9, and it transmits a large number of packets to the node 5, which is therefore changed to the strong node mode and responds an ACK packet with a warning message to replace its transmission path. In Figure 7(c), node 9 receives the ACK packet with a warning message and broadcasts query packets. In Figure 7(d), node 5 has entered a strong node mode, so it does not respond, only node 6 and node 8 returning information to node 9. In Figure 7(e), node 9 changes the transmission path to node 6, but since node 6 is transmitting to node 5, node 5 enters state of change the path in CSNM as shown in Figure 6. In Figure 7(f), node 6 received the ACK packet with a warning message. Figure 8(g), Figure 8(h) and Figure 8(i) are similar to Figure 7(c), Figure 7(d) and Figure 7(e). Figure 8(j) shows the operation of network to restore stability, in which node 5 is back to the general node mode, because the transmission path of node 6 and node 9 are changed.

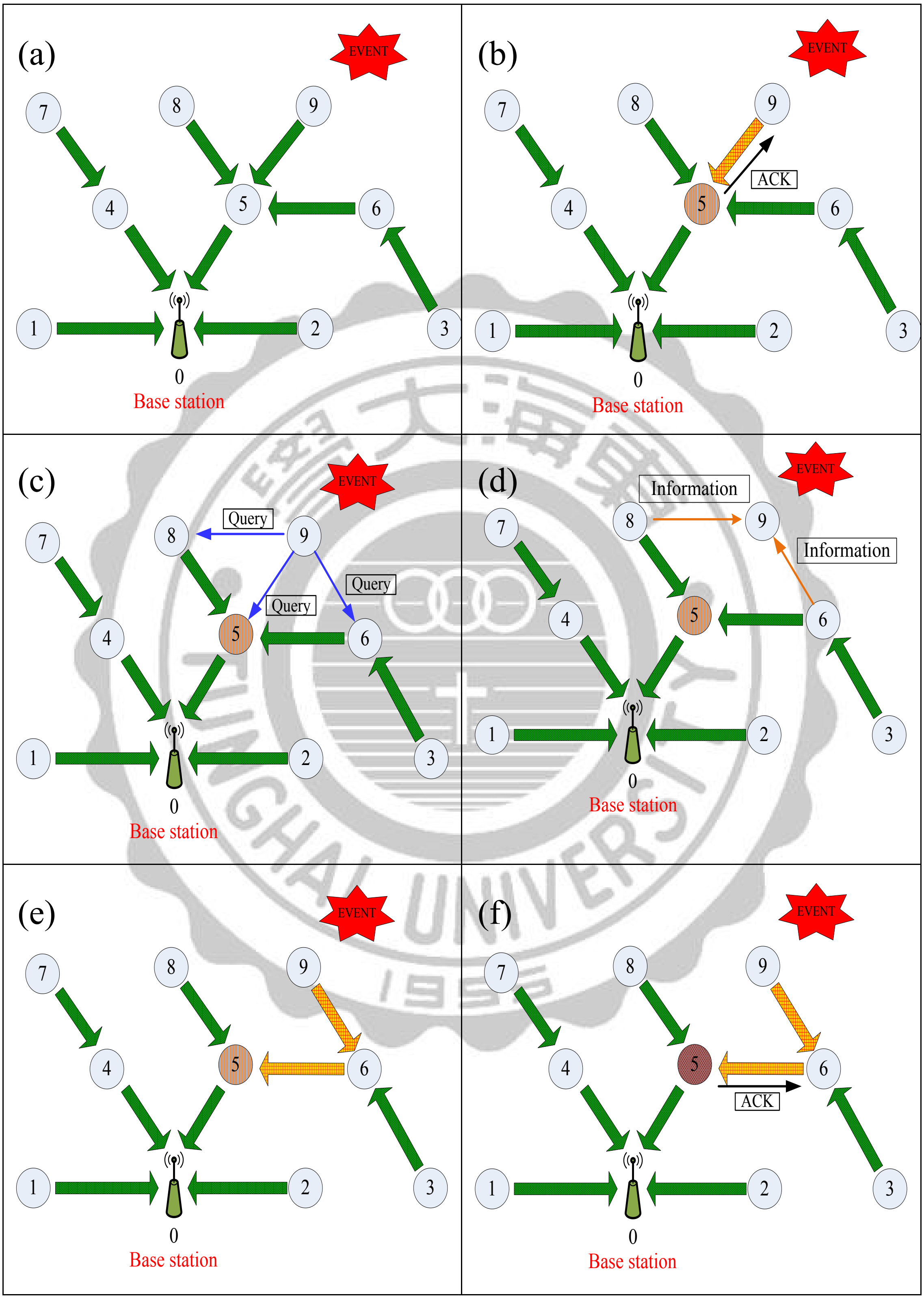


Figure 7 The operation of CSNM.

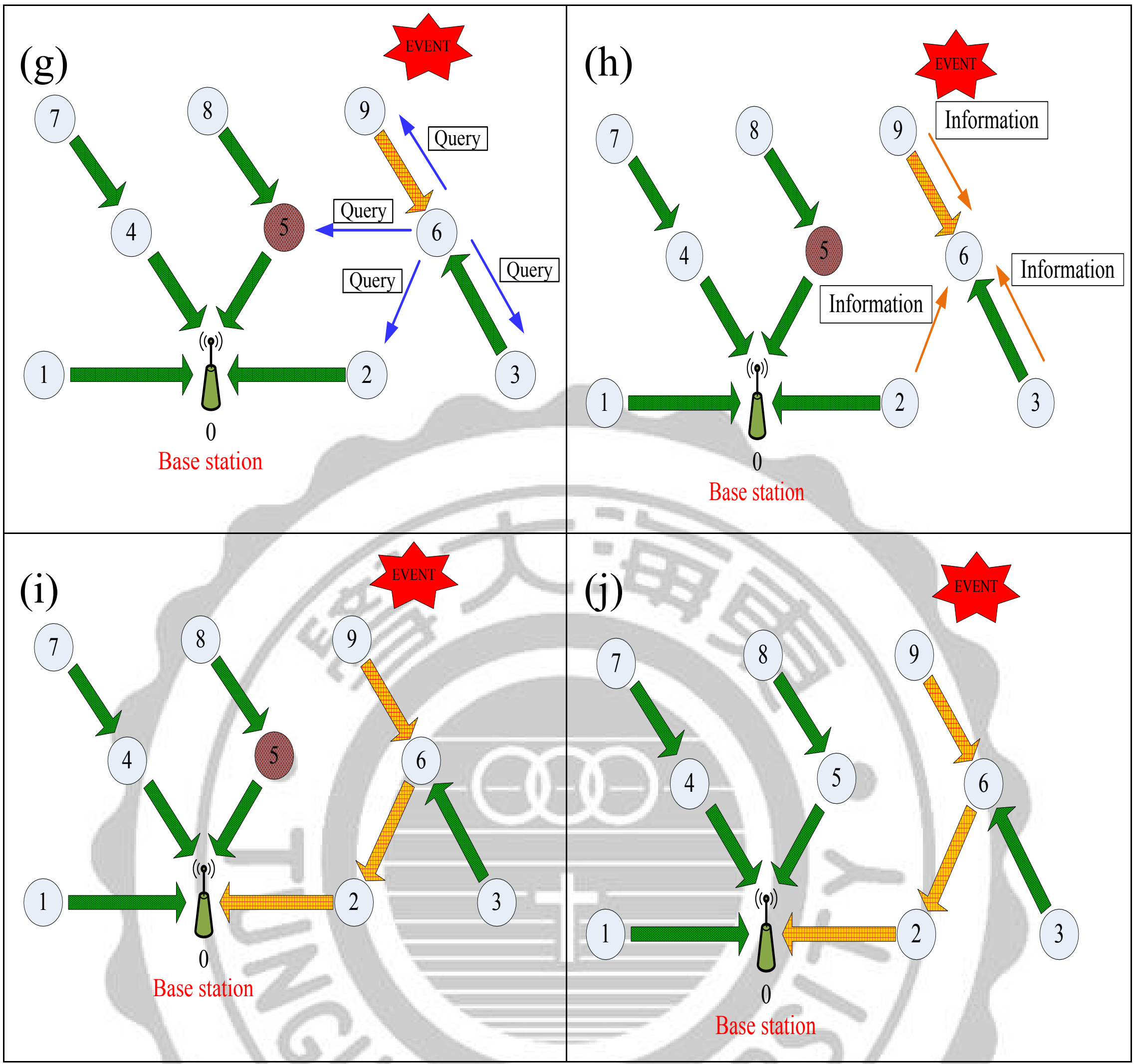


Figure 8 The operation of CSNM.

3.3 Node Weight

Three factors are used in the calculation of weight values: buffer loading, energy consumption, and hops the base station. To reduce the occurrence of congestion, and improve packets delivery ratio, reliability are the main goals of this mechanism. Weight values will affect selection of the alternate path. The number of hops decides the distance of this node to the base station, and it is the most important factor for selection of alternate path. If the hop count of alternate node is higher than the original node, it has longer distance. To calculate the priority, we first determine the number of hops, then the amount of residual energy, and the remaining buffer size. When the residual energy and the remaining buffer size weight are too high, the nodes on the alternate path will soon become the strong node mode. Threshold value is set to select alternate nodes with the most ability to assist the traffic. This method proposes a weight calculation by collecting three kinds of neighboring node information. It selects the nodes with the lowest W value to form a new transmission path. When several neighbors have same minimum Hops, the priority is calculated according to values of α and β, and the lowest value of W is picked, where α and β are between 0 to 1 and are controlled by the network administrator. Table 3 lists the definition of symbols used in Equation 2 and Equation 3 for calculation of weight values.

Table 3 The symbol definition for Equation 2 and Equation 3.

Symbol	Definition
W_i	The weight value of node i
E_i	Energy consumption of node i
B_i	Buffer loading of node i
H_i	The number of hops to base station from node i

$$W_i = \alpha E_i + \beta B_i + H_i \quad (2)$$

$$\alpha + \beta = 1 \quad (3)$$

Figure 9 shows a pseudo code of child node received an ACK packet with command for a path change.

Receive the ACK packet( )

Function

Receive the ACK packet.

If(receive the ACK packet with a command to change the path){

Drop this packet from the queue.

Broadcast the query packets to neighbor nodes.

Wait until the neighbor nodes respond to their buffer loading, energy consumption and hops, and calculated the weight value.

Select the alternative node with lowest weight value.

Change the parent node from original node to alternative node.

}

Figure 9 The pseudo code of the node receive the ACK packet.

TUNGHAI UNIVERSITY 東海大學 1955

Chapter 4
Experimental Results

4.1 The Setup of Experiments

This section shows the simulation framework and simulation results. The simulation framework describes simulation environment, simulation parameters, and the simulation program. The simulation results are shown and analyzed. Table 4 shows the parameters of experiments.

Table 4 The parameters of experiments.

Simulation parameter	Value
Topology size	300 x 300 m^2
Number of sensors	150
Deployment type	Random
The way of events occur	Random
Radio range	30 m
Initial sensors energy	1J
Sensor buffer size	30 data packets
Data packet size	128 bytes
Traffic type	Variable bit rate
MAC layer protocol	CSMA/CA
Simulation time	45 seconds

4.1.1 The AODV Protocol

Our experiments are based on Ad-Hoc On Demand Distance Vector (AODV) routing [21]. We will briefly describe the AODV protocol here. AODV is based on the flooding broadcast scheme to search the path and a routing protocol for dynamic wireless networks. In the search path, each node in establishing a single minimum path to the destination node records path length and the information in the routing table by passing messages. AODV defines three types of messages to notify the different status of the event, including the route request, the route reply and the route error. These messages are based on the format of the packet to pass. AODV defines path search method in two phases. The first phase is to broadcast the route request message and establish a return path. The second phase is to return the route reply message and establish the transmission path. AODV defines route request message containing the following important information:

- Originator IP Address
- Originator Sequence Number
- Destination IP Address
- Destination Sequence Number
- Hop Count

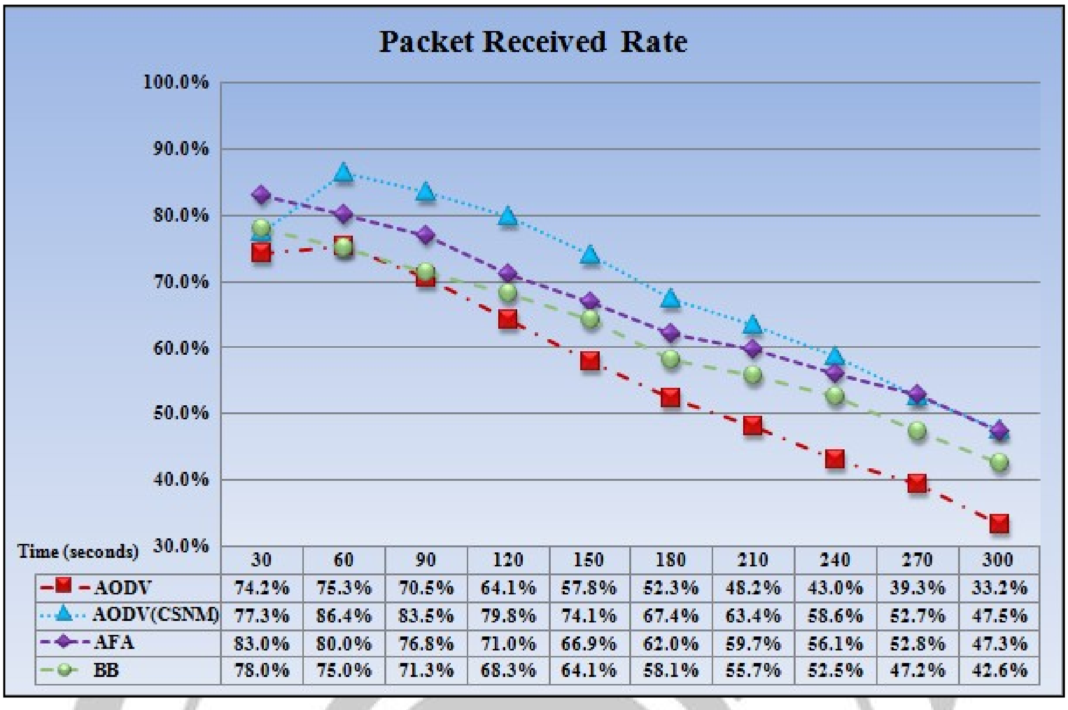
4.1.2 Comparison of Packet Received Rate

We compare our scheme with the Aggregate Fairness Algorithm (AFA) [7] and Buffer-Based Congestion Avoidance scheme (BB) [8]. In the AFA scheme, a sensor node i has a packet to forward sensor node j, only if the buffer of sensor node j is not full. If the buffer of sensor node j is full, sensor node i will hold the packet until it overhears a packet piggybacking a non-full buffer state from sensor node j. Thus, it does not cause packet loss. The AFA scheme is a rate-based scheme. The BB scheme must make sure that a sensor node i sends a packet to its downstream neighbor sensor node j only when sensor node j has buffer space to hold the packet. It does not cause packet loss, too. The BB scheme is a buffer-based scheme.

4.2 The Experimental Results

The experiment is performed by adding CSNM mechanism to the AODV protocol. When the node traffic exceeds the threshold, it will lead to switching of the node mode, and then the child nodes will change the path of the received command according to the CSNM mechanism, avoiding drop of packets due to a full buffer. Current thresholds HLTV_1 is set as 70%, HLTV_2 is set as 80% and LL is set as 50%.

Figure 10 shows comparisons of the packet receiving rates of AODV-CSNM and other schemes. As shown the packet receiving rate of CSNM mechanism with the AODV protocol is better than other schemes. So, the proposed CSNM mechanism is able to reduce congestion problem and avoid drop of packets. In the traffic environment, because of the buffer size of a single node being limited in the AFA scheme and BB scheme, the effect of congestion avoidance is limited. Our mechanism is cooperative, and able to use the resources of each node. Thus, in the traffic environment, the performance will be better than other schemes.



Time (seconds)	30	60	90	120	150	180	210	240	270	300
AODV	74.2%	75.3%	70.5%	64.1%	57.8%	52.3%	48.2%	43.0%	39.3%	33.2%
AODV(CSNM)	77.3%	86.4%	83.5%	79.8%	74.1%	67.4%	63.4%	58.6%	52.7%	47.5%
AFA	83.0%	80.0%	76.8%	71.0%	66.9%	62.0%	59.7%	56.1%	52.8%	47.3%
BB	78.0%	75.0%	71.3%	68.3%	64.1%	58.1%	55.7%	52.5%	47.2%	42.6%

Figure 10 Comparison of packet receiving rate of AODV-CSNM and AODV.

Figure 11 shows the average residual energy of nodes. The BB scheme is best in this respect. Since the total packet flow of BB scheme is the least, the energy consumption is smaller. Our mechanism is only better than the original AODV protocol in view of energy consumption. In our mechanism energy consumption will increase when a node is about to exhaust, because the node to exhaust first is often around the base station and the traffic will be transferred to other nodes when the node is exhausted. In the experiment, we found that, because of increasing need to change the node path, the surrounding nodes have entered strong node mode when the node exhausted, resulting in a substantial increase in broadcasting of the query packet.

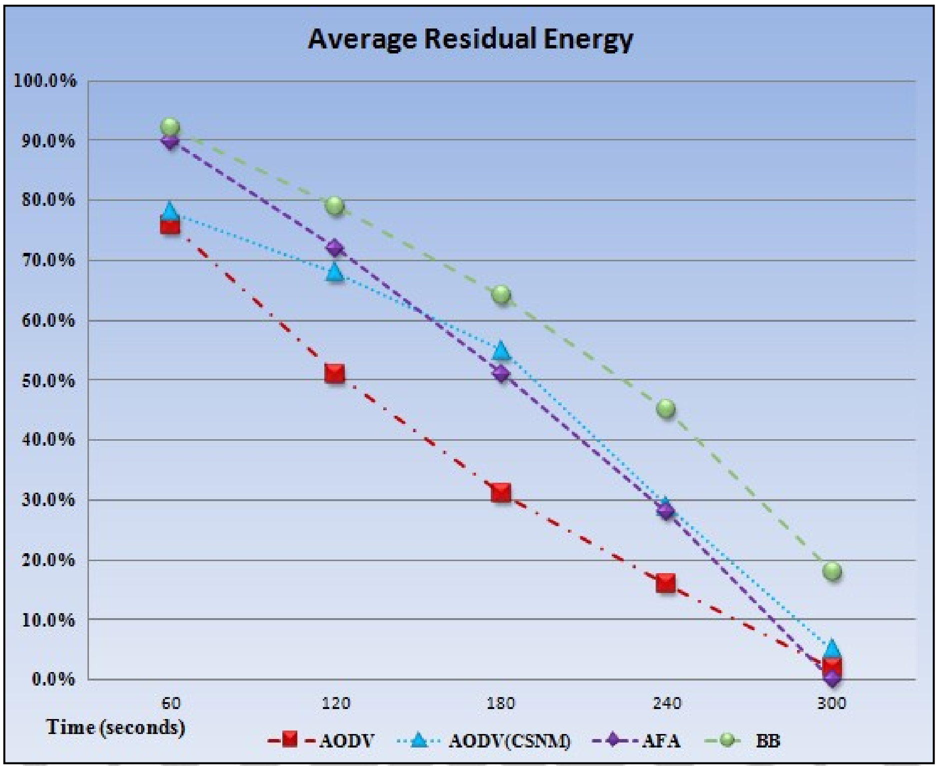
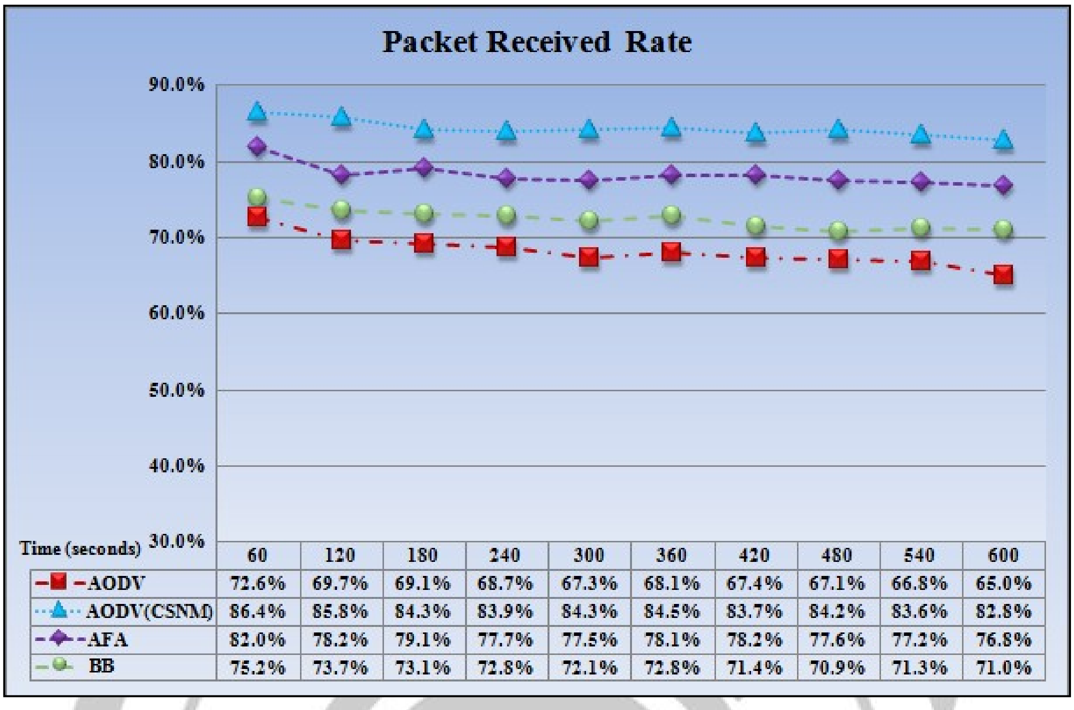


Figure 11 Average residual energy of AODV-CSNM and AODV.

Figure 12 shows comparisons of packet receiving rates without considering energy consumptions. In this environment, our mechanism will show more advantages. When the node does not exhausted by energy consumption, the node continues cooperation and maintains a high receiving rate. The experimental results show our mechanism is suitable for applications focus on the receiving rate of wireless sensor networks.



Time (seconds)	60	120	180	240	300	360	420	480	540	600
AODV	72.6%	69.7%	69.1%	68.7%	67.3%	68.1%	67.4%	67.1%	66.8%	65.0%
AODV(CSNM)	86.4%	85.8%	84.3%	83.9%	84.3%	84.5%	83.7%	84.2%	83.6%	82.8%
AFA	82.0%	78.2%	79.1%	77.7%	77.5%	78.1%	78.2%	77.6%	77.2%	76.8%
BB	75.2%	73.7%	73.1%	72.8%	72.1%	72.8%	71.4%	70.9%	71.3%	71.0%

Figure 12 Comparison of packet receiving rate of AODV-CSNM and AODV does not consider the energy consumption.

Chapter 5
Conclusion

In this thesis, we have improved the congestion problems that might occur in wireless sensor networks, considered the transmission delay, and extended the network lifetime. In the mechanism we propose to use a strong node mode. Strong node mode means that the node with large traffic has permission to its child nodes to decide whether to change the transmission path. We also propose ways to solve more than one child node transmission path change at the same time, which avoids propagating the problems caused by high load to the alternate node. This mechanism using three factors in the selection of an alternate node, there are remaining buffer size, residual energy and the number of hops. The alternate node is the shortest path in the surrounding neighbors of the original node and the most capable of handling traffic. The experimental results show our proposed mechanism can be applied in a variety of routing protocols, and is improve the packet arrival rate, minimize the packet delay, and be able to add new nodes when the entire network is overwhelmed by the load. However, the extra computing overhead for adding new nodes is a drawback of this mechanism.

Bibliography

[1] Paolo Barontib, Prashant Pillaia, Vince Chook, Stefano Chessa, Alberto Gotta, and Y. Fun Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15. 4 and ZigBee standards," Computer Communications, vol.30, no.7, pp. 1655-1695, May 2007.

[2] Mohammad Hossein Yaghmaee, Donald A. Adjeroh, "Priority-based rate control for service differentiation and congestion control in wireless multimedia sensor networks," Computer Networks: International Journal of Computer and Telecommunications Networking, vol.53, pp. 1798-1811, July 2009.

[3] Chonggang Wang, Kazem Sohraby, Victor Lawrence, Bo Li and Yueming Hu, "Priority-based congestion control in wireless sensor networks" in Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC), pp. 22-31, June 2006.

[4] Yogesh Sankarasubramaniam, Özgür B. Akan and Ian F. Akyildiz, "ESRT: event-to-sink reliable transport in wireless sensor networks" in Proceedings of the ACM International Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc), pp. 1003-1016, October 2003.

[5] Chieh-Yih Wan, Shane B. Eisenman, and Andrew T. Campbell, "Congestion detection and avoidance in sensor networks" in Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys), pp. 266-279, November 2003.

[6] Bret Hull, Kyle Jamieson and Hari Balakrishna, "Mitigating congestion in wireless sensor networks," in Proceedings of the ACM Conference on Embedded Networked Sensor Systems (SenSys), pp. 134-147, November 2004.

[7] Shigang Chen and Zhan Zhang. "Localized algorithm for aggregate fairness in wireless sensor networks," in Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCOM), pp. 274-285, September 2006.

[8] Shigang Chen and Na Yan, "Congestion avoidance based on lightweight buffer management in sensor networks," in Proceedings of the IEEE International Conference on Parallel and Distributed Systems (ICPADS), September 2006.

[9] Jamal N. Al-Karaki and Ahmed E. Kamal, "Routing Techniques in Wireless Sensor Networks: A Survey," IEEE Wireless Communications [see also IEEE Personal Communications], pp. 6-28, December 2004.
[10] Wendi Rabiner Heinzelman, Joanna Kulik, and Hari Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks," Proc. 5th ACM/IEEE Mobicom, Seattle, WA, pp. 174–185, August 1999.
[11] Chalermek Intanagonwiwat, Ramesh Govindan, Deborah Estrin, John Heidemann, and Fabio Silva, "Directed Diffusion for Wireless Sensor Networking," IEEE/ACM Transactions on Networking, pp. 2-16, February 2003.
[12] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan, "Energy-Efficient communication Protocol for Wireless Sensor Networks," Proc. of the 33rd Hawaii International Conference on System Sciences, pp. 1-10, January 2000.
[13] Arati Manjeshwar and Dharma P. Agrawal, "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," Proc. of the International Parallel and Distributed Processing Symposium, pp. 2009-2015, 2001.
[14] Arati Manjeshwar and Dharma P. Agrawal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive Information Retrieval in Wireless Sensor Networks," Proc. of the International Parallel and Distributed Processing Symposium, pp. 195-202, 2002.
[15] Omar Moussaoui and Mohaned Naimi, "A Distributed Energy Aware Routing Protocol for Wireless Sensor Networks," International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems archive, pp. 34-40, 2005.
[16] Stephanie Lindsey and Cauligi S. Raghavendra, "PEGASIS: Power Efficient Gathering in Sensor Information Systems," IEEE Aerospace Conference, Vol. 3, pp. 1125-1130, March 2002.
[17] Ya Xu, John Heidemann, and Deborah Estrin, "Geography-Informed Energy Conservation for Ad-hoc Routing," Proceedings of the 7th Annual ACM/IEEE Int'l. Conf. Mobile Computing and Networking, pp. 70–84, 2001.
[18] Yan Yu, Ramesh Govindan, and Deborah Estrin, "Geographical and

Energy-Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks," UCLA Computer Science Department technical report, CLA-CSD TR-010023, May 2001.

[19] Md. Abdur Razzaque, Choong Seon Hong, "Congestion detection and control algorithms for multipath data forwarding in sensor networks." International Conference on Advanced Communication Technology, February 2009.

[20] Mohammad Z. Ahmad, Damla Turgut, "Congestion avoidance and fairness in wireless sensor networks." Global Telecommunication Conference, November 2008.

[21] Charles E. Perkins, Elizabeth M. Belding-Royer, and Samir Das, "Ad Hoc On Demand Distance Vector (AODV) Routing." IETF RFC 3561, July 2003.