ITEC 810

Security Framework for Wireless Sensor Networks

Final Project Report

Lecturer:	Robert Dale
Supervisor:	Rajan Shankaran
Student:	Stuart Stent
Student ID:	41149440
Submission Date:	5 June, 2009

Table of Contents

Stuart Stent
Student Number : 41149440

Abstract

Wireless Sensor Networks ('WSN') are a developing technology for the collection of data in various environments where traditional methods are neither viable, nor cost effective. Due to the restrictions imposed by the application requirements and hardware limitations, the implementation of data communications and security for these networks presents several challenges. This paper examines the various network routing protocols used in WSNs, the known attacks on these protocols, and the defensive strategies that may be employed to prevent these attacks.

The analysis undertaken in this paper reveals that in order to provide adequate security there is a need for the integration of security services into the existing routing protocols. To this end, an extension of the Low-Energy Adaptive Clustering Hierarchy ('LEACH') network routing protocol called the Security Enabled - Low-Energy Adaptive Clustering Hierarchy ('SE-LEACH') is proposed. This proposed protocol provides security services such as data encryption, secret key distribution, message integrity verification and message replay detection in the form of a flexible and extendable framework, thereby overcoming the lack of security in existing WSN protocols.

1 Introduction

The continued miniaturisation and commoditisation of computer hardware has created new possibilities in the area of data collection through the deployment of Wireless Sensor Networks ('WSN'). WSNs are becoming an invaluable tool in both the commercial and military sectors for the gathering of data in environments where traditional techniques are neither viable nor cost effective. The ease and minimal cost with which WSN technology can be deployed makes it an attractive alternative to traditional data collection methods. WSNs are an ideal solution in environments that are either too dangerous, such as a disaster area or battlefield, or areas where the traditional techniques are inefficient or costly, such as gathering information over large areas of difficult terrain. While the protocols required to gather data for analysis have undergone significant development, there is a distinct lack of mature integrated security solutions available for use in WSNs.

The purpose of this paper is to ascertain the current leading edge in attacks against WSNs and the corresponding defences and propose a solution for WSNs which integrates security services into the existing architecture. Section 2 of this review provides background information on WSNs, their applications and limitations. In order to understand the security challenges inherent in WSNs, it is necessary to first understand the network issues at play. To this end, Section 3 explores the various issues involved with the transmission of data within a WSN, as well as the various proposals currently being circulated for data transfer protocols. Section 4 analyses the security criteria specific to WSN deployments. A survey of the possible attacks is presented in Section 5, followed by a review of the various proposals for combating these attacks in Section 6. In Section 7, an extension to the Low-Energy Adaptive Clustering Hierarchy ('LEACH'), routing protocol, Security Enabled - Low-Energy Adaptive Clustering Hierarchy ('SE-LEACH'), is proposed. This extension aims to address the security issues of WSNs, by integrating a new extendable security framework into the existing LEACH routing protocol. Finally, Section 8 summarises the findings of this paper.

2 Background

2.1 What is a WSN?

A typical WSN consists of two main components – a central data gathering point, referred to as a 'sink' and multiple small autonomous sensor devices referred to as 'motes'. The system is deployed in an area of interest by either manually placing the devices at predetermined locations or randomly scattering them over the area. Once deployed, the sink and motes communicate via radio to build a data network, enabling the motes to transmit sensor data back to the sink device for analysis (Tilak, Abu-Ghazaleh, & Heinzelman, 2002).

The development of applications, network protocols and security technologies for use in WSNs requires the consideration of the various limitations and requirements of the technologies employed in WSNs.

2.1.1 Processing and Storage

Current node hardware is designed with a low unit cost as its primary criteria, which necessitates the use of low end hardware equivalent to desktop computer hardware of 6-7 years ago. Owing to the information processing and storage limitations imposed by these hardware implementations, new and innovative approaches to maximise the resources available are required (Walters, Liang, Shi, & Chaudhary, 2006, p. 3).

2.1.2 Power

With extremely limited available power (often 2 to 3 AAA batteries) and extended deployment durations (1 -2 years), the management of energy reserves is essential to maintaining operation of the WSN (Tilak, Abu-Ghazaleh, & Heinzelman, 2002). This restriction is likely to remain even as battery and renewable energy sources improve, as the node's capabilities (processing power, transmission range, etc) will increase to consume the extra energy available.

2.1.3 Reliability

Due to the difficulty and cost involved in physically managing the deployed nodes, each device must be robust and reliable (Walters, Liang, Shi, & Chaudhary, 2006; Akkaya & Younis, 2005). This is especially evident when looking at WSN deployments in environments that are particularly volatile and dangerous to humans such as an active volcano or a radioactive and contaminated area like Chernobyl.

2.1.4 Cost

Many applications involving WSN technology are only made viable if the cost of deploying a WSN is lower than the cost of traditional data collection methods (Tilak, Abu-Ghazaleh, & Heinzelman, 2002). Thus, not only does the cost of the hardware need to be minimised, but the administrative cost of configuring and deploying the hardware also needs to be kept low.

3 WSN Architecture and Routing Schemes

3.1 General Routing Issues

The specific requirements and limitations of WSNs provide a unique set of challenges when it comes to developing techniques for routing data from one node to another. Some of these challenges are outlined below.

Firstly, standard network routing protocols such as OSPF, RIP and BGP rely on logical addressing schemes such as IPv4 to calculate network topologies and provide routing services; however, due to the large numbers of nodes found in WSN deployments, the use of a global addressing scheme such as an IP-based system is not feasible. This is due to the memory requirements and management overheads of these protocols (Akkaya & Younis, 2005, p. 2). Therefore, new routing technologies are required for WSNs that can work efficiently without these addressing schemes.

Secondly, a primary requirement of WSN deployments is a long deployed operating life. As such, routing protocols must be aware of the energy reserves of a node and manage the use of this power efficiently (Akkaya & Younis, 2005, p. 3). As traditional routing technologies have no energy awareness built into their design, new approaches are required to meet this requirement.

Thirdly, the network topologies involved in WSNs differ from traditional network topologies in that they require a central collection point for the data (i.e. the sink node). Placement of the sink node is of critical importance as this can have major impact on the life of a network. This can be a challenge as the power requirements for transmission are proportional to the square of the transmission distance (Akkaya & Younis, 2005, p. 3) and therefore minimal transmission distances are preferable.

Finally, WSN routing protocols need to be to self-configuring once deployed, and also require the ability to recover from the inevitable node failures that will occur in the field (Tilak, Abu-Ghazaleh, & Heinzelman, 2002). Unlike standard networking environments, such failures and overheads can have a detrimental effect on the viability of the WSN.

3.2 Routing Protocol Classification

Owing to the fact that existing network routing protocols fail to meet the specific requirements of WSNs, researchers have proposed a number of more suitable protocols using various routing paradigms. These proposals can be broadly classified into four groups, as defined by Akkaya *et al.* (2005, p. 2).

These four classifications are:

1. **Data-Centric**

   Data-centric protocols are based on a query-driven model and depend heavily on the naming of data to allow the targeting of requests based on data types and value ranges.

2. **Hierarchical**

   Hierarchical protocols are defined as being those in which some form of clustering or tiering occurs. The aggregation of data also features prominently in these protocols. This data aggregation can take many forms; however, the basic principle is to de-duplicate or average the data from many nodes to reduce the number of transmissions required.

3. **Location-Based**

   Location-based protocols use geographical or topological information to target requests based on the desired area of interest, rather than flooding the entire network with the request.

4. **Network and Quality Of Service Aware**

   Network and Quality of Service ('QoS') aware protocols are based on an awareness of the network topology. A small number of these protocols are QoS-aware and can provide routing based on the latency requirements of specific data.

Another method of classification for routing protocols is according to the data delivery model used. This can have a great impact on the power utilisation requirements for a protocol as well as the protocol's suitability for various applications. Tilak *et al.* (2002) propose four classifications for data delivery models:

1. **Continuous**

   In this data delivery method, data is sent continuously from a sensor node to the sink. This model is particularly suited to applications such as audio or video monitoring.

2. **Event-Driven**

   In this method, data is only sent when an observed event occurs. This can be implemented using thresholds to govern what constitutes a notable event.

3. **Query-Driven**

   This is a query and response model in which the sink node sends a request for data to nodes when it wishes to collect information.

4. **Hybrid**

   Some protocols use a mixture of continuous, event-driven and query-driven methods. This 'hybrid' method is especially evident in applications using a variety of sensor types with varying sampling requirements.

3.3 Data Centric Protocols

3.3.1 Flooding and Gossiping

Conventional protocols for the routing of data in an unmanaged network such as Flooding and Gossiping present one possibility for transferring information in a WSN. These protocols do not require any overhead in terms of routing or topology maintenance, thereby reducing their power requirements. It should be noted, however, that Flooding introduces issues such as 'implosion', where multiple copies of the data are received by a node (see Figure 1 below), and 'overlap', where data from a single area is received twice due to the coverage of two nodes overlapping, thus consuming power unnecessarily (see Figure 2 below). Such issues were found to be major drawbacks to its use in WSN deployments (Heinzelman, Kulik, & Balakrishnan, 1999).

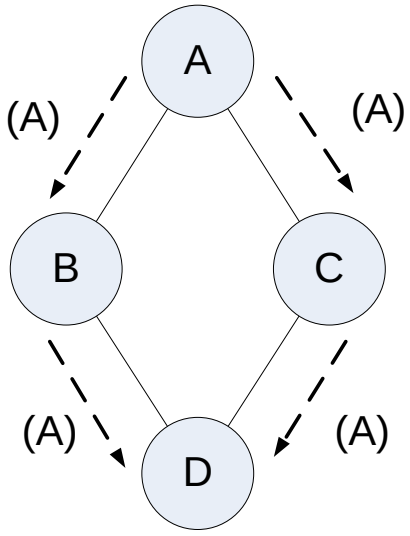

Figure 1 – Implosion

Node 'D' receives multiple copies of the data from node 'A', in this case via nodes 'B' and 'C'.

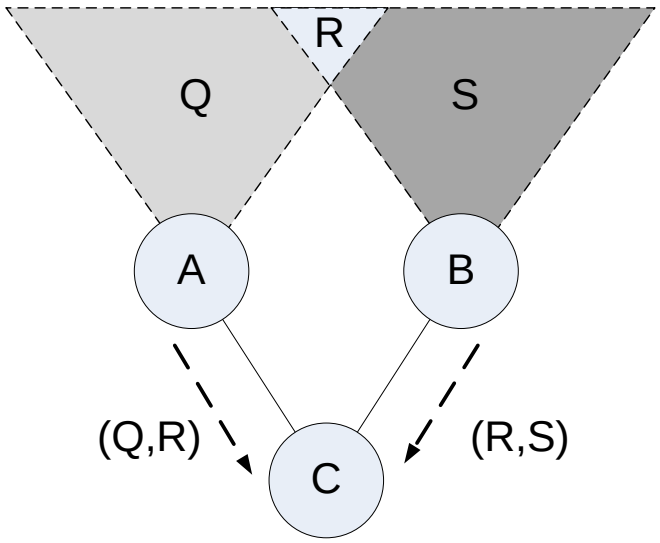

Figure 2 – Overlap

Node 'C' receives duplicate data about region 'R' from nodes 'A' and 'B'

Gossiping overcomes the implosion issue of Flooding by randomly selecting a neighbour node rather than broadcasting to all nodes; however, this does introduce delays in data propagation (Akkaya & Younis, 2005, p. 6).

Both Flooding and Gossiping are viable, albeit not very efficient, solutions for small WSN deployments. They do not, however, scale very well to larger network sizes due to the lack of network topology and energy usage awareness.

3.3.2 Sensor Protocols for Information via Negotiation

A new data-centric, event-based protocol, Sensor Protocols for Information via Negotiation ('SPIN') (Heinzelman, Kulik, & Balakrishnan, 1999) was proposed to provide an energy-aware protocol specifically designed for WSNs. The basic principle of SPIN is that nodes communicate about new data that is available, as it is generated by sensor events, as well as about data they require, via a series of requests and responses. The use of metadata to describe the information that is available removes the issues of overlap and implosion encountered in earlier protocols such as Flooding.

The SPIN protocol defines three messages which form the basis of the protocol: new data advertisement ('ADV'); request for data ('REQ') and data message ('DATA'). An example showing two rounds of this protocol is shown in Figure 3 below.

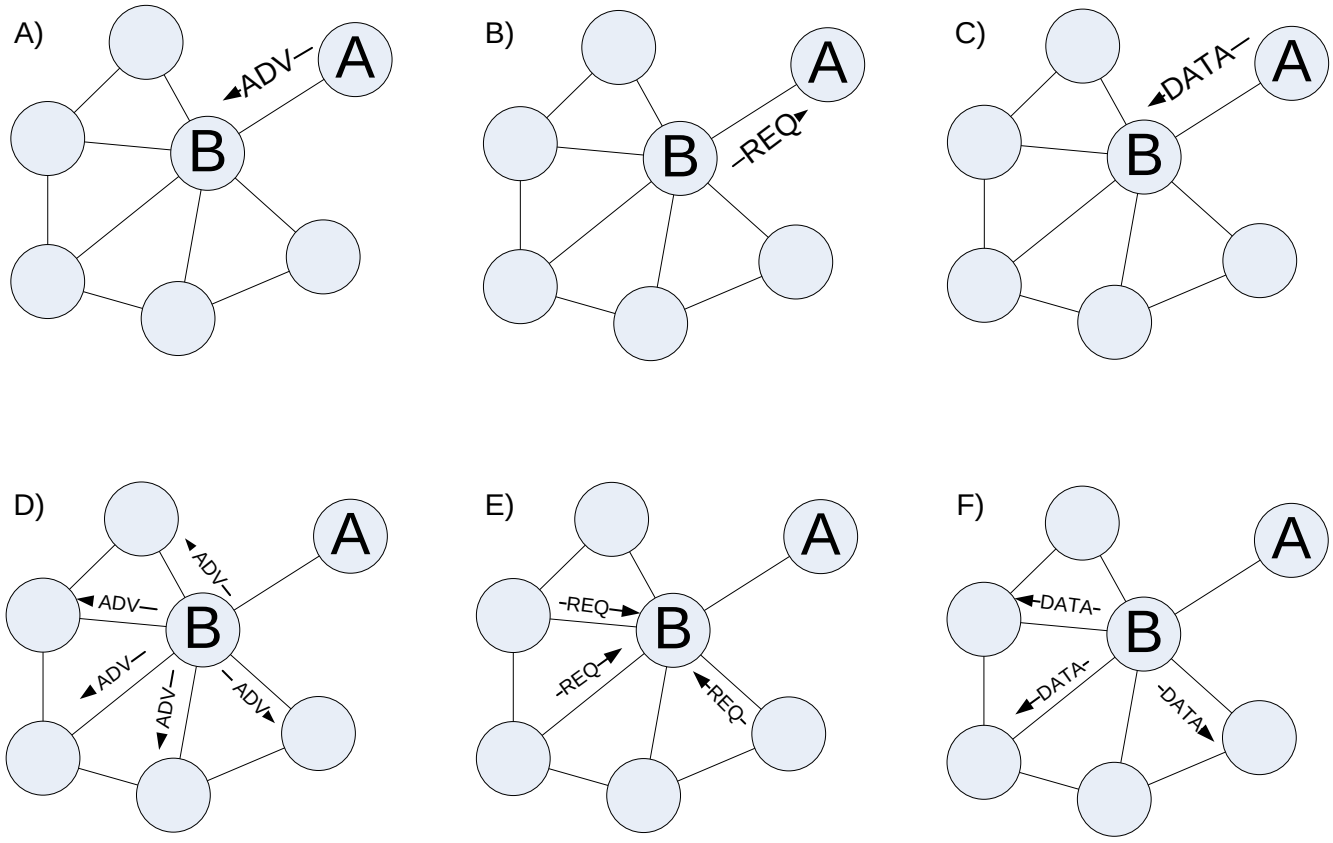

Figure 3 - SPIN protocol stages

Two rounds of the SPIN protocol are shown here

A) When node 'A' acquires new data, either through sampling the environment itself or receiving data from another node, it transmits an ADV message to all of its neighbour nodes (in this case node 'B') which contains metadata about the new information it has available.
B) Node B has not already received the data and transmits a REQ message to node A, requesting the new data.
C) Upon receiving the REQ message node A transmits the DATA to node B.
D) Node B then advertises the new data to all of its neighbours by sending an ADV message.
E) The neighbour nodes that require this information then send a REQ message back to node B.
F) Node B then forwards the data to each node that requested the data. This continues until the data has reached all interested nodes, including the sink node.

While this protocol is a major step forward in data transfer for WSNs, the non-guaranteed delivery of data and issues relating to data relaying over multiple hops make it a less than ideal protocol as the network size increases.

3.3.3 Directed Diffusion

As SPIN is an event-driven model, it is not a good candidate for applications that require data capture at regular intervals. Intanagonwiwat *et al.* (2000) proposed a data-centric, query-driven protocol called 'Directed Diffusion', where the sink generates an 'interest notification' specifying a data type with certain attributes that it is interested in. An example of an interest notification specifying an interest in temperatures in the range 10-15°C over the course of a 20 second period is shown in **Error! Reference ource not found.** below.

Type = Temperature;

Upper Limit = 15;

Lower Limit = 10;

Duration = 15;

Time Stamp = 13:45:23;

Figure 4 - Interest Notification

The interest notification is broadcast to all nodes in the network. When a node has information that meets the criteria specified in the interest notification, it forwards that data to the sink.

Directed Diffusion also provides the ability to transmit data between nodes over larger distances by using multiple nodes to reach a destination. This multi-hop capability is achieved through the use of 'gradients'

which are paths between the sensing node and the sink node. These paths or gradients are formed when an interest notification is sent by the sink node. As each node receives the interest notification it makes note of which neighbour it received the notification from. When a node forwards data back to the sink node, it sends the data to the neighbour it received the interest notification from. This continues until the data is received by the sink node. This use of gradients greatly increases the scalability of WSNs.

Subsequent proposals have been put forward that are based on Directed Diffusion, such as Energy-Aware Routing (Gura, Patel, Wander, Eberle, & Shantz, 2004) and Gradient-Based Routing (Gruteser & Grunwald, 2003), which detail techniques for achieving greater redundancy and more efficient energy usage.

3.4 Hierarchical Protocols

3.4.1 LEACH

While Direct Diffusion greatly increases the scalability of WSNs, there are still limits to the number of sensors and the range it can cover. In an effort to increase the scalability of these networks, Heinzelman *et al.* (2000) propose the Low-Energy Adaptive Clustering Hierarchy ('LEACH') protocol, a cluster-based approach to sensor network routing. In LEACH, the network is broken up into smaller networks or clusters, which designate a single node to communicate with the sink, referred to as a 'cluster head'. An example of LEACH clustering is given in Figure 5 below.

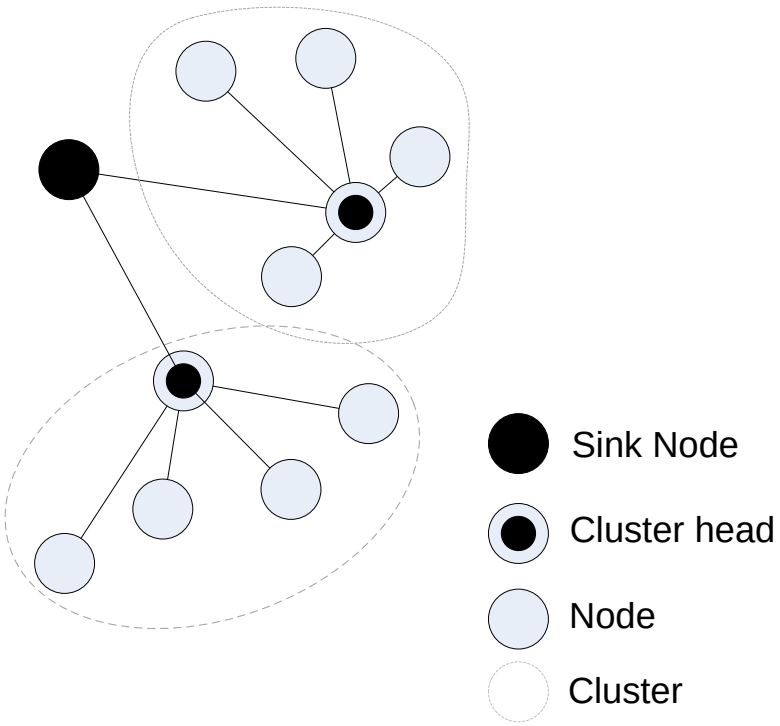

Figure 5 - LEACH network

The cluster head is responsible for aggregating all of the data generated by the cluster and transmitting it back to the sink. As the cluster head normally has the same power and processing restrictions as every other node, the role of cluster head is randomly changed within the cluster to spread the resource usage.

The LEACH protocol is very flexible, and while the original proposal defines a continuous data delivery method, it should be possible to modify the protocol to accommodate both event-driven and query-based delivery models.

Other protocols inspired by LEACH that utilise a hierarchical approach include PEGASIS and Hierarchical PEGASIS (Lindsey & Raghavendra, 2002), TEEN (Manjeshwar & Agrawal, 2001) and APTEEN (Manjeshwar & Agrawal, 2002).

The PEGASIS protocol uses a chain system in preference to the cluster-based system used in LEACH. A chain is made up of single nodes forming a path to the base station. When node 'A' has data to transmit to the base station, it transmits to its nearest neighbour 'B' that is part of the chain to the base station. Node B then aggregates the data it has with the data from node A and forwards this aggregated data to the next node 'C', where the process repeats until the data arrives at the base station. Lindsey *et al.* (2002) demonstrated through experimentation that PEGASIS can achieve a 100%-300% improvement in efficiency over LEACH.

Hierarchical PEGASIS is an extension to the PEGASIS protocol which uses the metric $Energy\ Expenditure\ x\ Delay$ for path selection rather than the simple nearest neighbour model used in PEGASIS.

The TEEN protocol proposed by Manjeshwar *et al.* (2001) is an event-based system that extends the cluster paradigm used in LEACH to a second level of clusters (see Figure 6, reproduced from (Manjeshwar & Agrawal, 2001)). TEEN combines this second level of clustering with a threshold system where 'hard' and 'soft' threshold levels are transmitted to all nodes by the base station. These thresholds specify when a node should transmit data back to the base station.

APTEEN extends the TEEN protocol by adding 3 types of query to the protocol: historical, one-time and periodical. These new query types allow the base station to request previously collected data over a particular time period (historical), a snapshot of the current data values (one-time), or request data to be transmitted at set intervals (periodical).

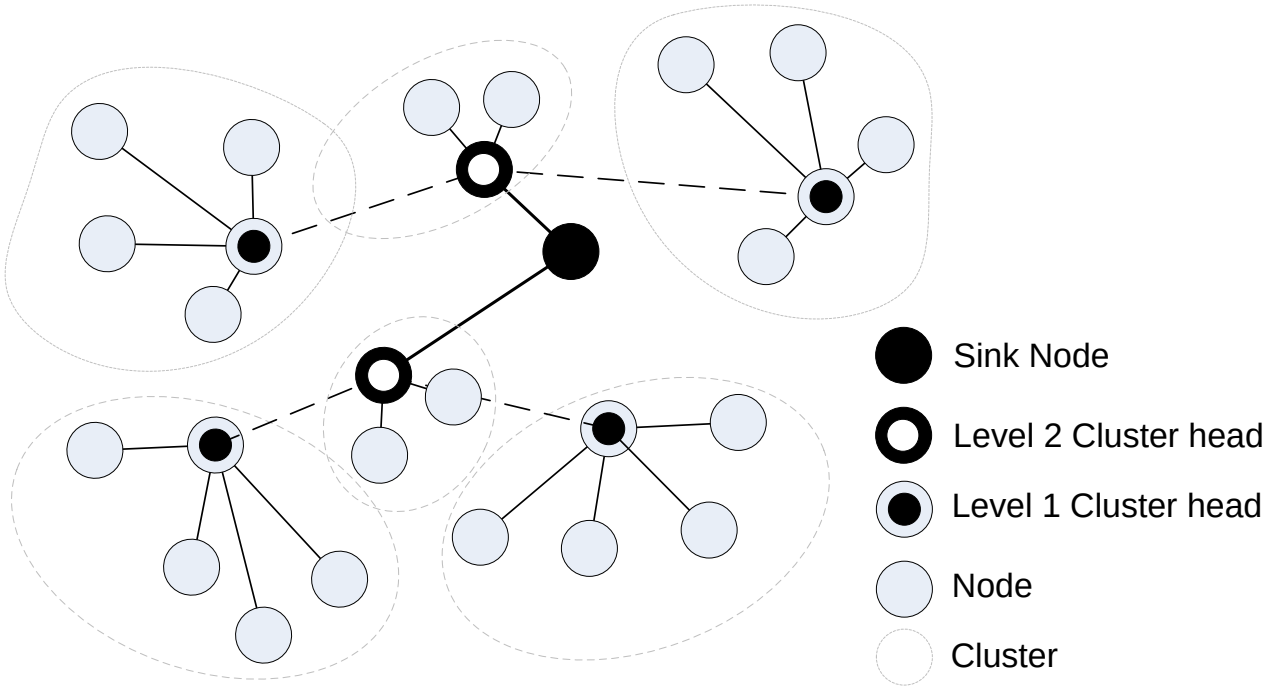

Figure 6 - TEEN Hierarchical Clustering

3.5 Location-Based Protocols

3.5.1 MECN & SMECN

The Minimum Energy Communication Network ('MECN') and the Small Minimum Energy Communication Network ('SMECN') protocols outlined by Rodoplu & Meng (1999) and Li & Halpern (2001) use location information provided by GPS-equipped sensor motes to geographically define relay regions. This geographical data is used to determine the lowest power routes between nodes on the network.

3.5.2 GAF

Another location-aware approach, Geographic Adaptive Fidelity ('GAF'), is given by Yu (2001), which uses a grid system to determine sensor overlaps. GAF assigns a single node in each grid reference to relay data for all devices in that region. Other nodes in that region are set to sleep mode to conserve energy. Relay responsibilities are rotated between the nodes in each region to spread resource usage.

3.6 Network Flow and QoS-Aware Protocols

3.6.1 Energy-Aware QoS Routing Protocol

Protocols such as the Energy-Aware QoS routing protocol defined by Akkaya *et al.* (2003) provide the capability to route traffic based on the delay requirements of the data. For example, real time data that

has a requirement for a short transmission delay will be prioritised for transmission back to the sink node, whereas data with a less critical delivery timeframe will be queued for transmission. This protocol provides an important capability for applications where timely data delivery is critical.

3.7 Routing Protocol Design and Security

All of the protocols detailed above are primarily concerned with the energy efficient transmission of data from the sensing node to the base station for analysis. These protocols achieve this goal with varying levels of success; however, little if any consideration seems to have been given to securing these data transmissions. In the early stages of development it is acceptable for researchers to ignore the issue of security in an effort to make the protocols and their concepts easy to understand and evaluate. As the technology matures, however, it is necessary for the focus on security to increase when developing a protocol. A protocol such as the SEAMAN network routing protocol (Bongartz, Ginzler, Bachran, & Tuset, 2008) developed for use in Mobile Ad-hoc Networks that are deployed in hostile environments, is a prime example of a well-designed protocol with security integrated from the ground up.

The integration of security services at the network access/routing protocol level is advantageous as it means that all transmissions can be secured, thereby mitigating a large range of attacks including routing protocol attacks.

4 Security Considerations

4.1 Issues

The implementation of security services in a WSN is difficult due to the many restrictions and issues associated with the hardware and routing protocol implementations.

Classical cryptography techniques which form the basis for the majority of security algorithms and protocols are mathematically, and therefore computationally, intensive. This is a major issue in providing security for a WSN as the hardware deployed in the field is very limited by current standards. For example, the Imote2 hardware from Crossbow Technologies Inc. contains a 416 MHz XScale© processor, 256k SRAM, 32MB Flash and 32MB SDRAM and is designed to run on 3 AAA batteries for extended periods (Crossbow, 2007). The use of standard cryptographic algorithms and protocols on such computationally limited hardware would require longer computation times and therefore consume more energy (Walters, Liang, Shi, & Chaudhary, 2006, p. 3). Subsequently, techniques that minimise processing and transmission requirements and conserve energy are required.

Modern cryptographic techniques rely, to some extent, on the underlying mechanisms provided by the network protocols to ensure that messages have been received and that the message is complete. These basic services are not provided by WSN routing protocols and tasks like error correction and message acknowledgement are handled by the application layer (Walters, Liang, Shi, & Chaudhary, 2006, p. 4). Therefore, any security service that relies on guaranteed network delivery services will not work as expected and will need to be modified to handle such tasks.

Further, many security services rely on trust relationships between entities for key management and authentication services. A common method of providing these services is to have a central management entity, such as a certificate authority. In the case of WSNs, the implementation of a central management entity would introduce a single point of failure into the network, thereby making the network less resilient (Walters, Liang, Shi, & Chaudhary, 2006, p. 5).

Overall, the biggest security issue for WSNs is the unattended nature of the network devices (Walters, Liang, Shi, & Chaudhary, 2006, p. 5). The lack of physical security is of major concern in regards to trust relationships and ensuring that the network is not compromised.

4.2 Security Requirements

There are eight security services as outlined by Walters *et al.* (2006, pp. 5-10), that are required to ensure a secure sensor network. These are discussed below.

4.2.1 Data Confidentiality

A malicious entity that can capture data transmitted by the nodes in the network should not be able read the contents of the transmission. Data confidentiality services are normally achieved by enciphering the data with a specific key, with the receiving party decrypting the transmission with either the same key (symmetric cryptography) or a matching decryption key (asymmetric cryptography).

4.2.2 Data Integrity

Data integrity ensures that the data received is in fact the data that was transmitted and that it hasn't been tampered with or corrupted. A Message Authentication Code ('MAC') is normally transmitted with the data, which the receiving party can use to verify the veracity of the data. This MAC is generally in the form of a cryptographic one-way hash.

4.2.3 Data Freshness

Data Freshness ensures that the data received has not been received before. Each message can be transmitted with a single use number or 'NONCE', which may take the form of a sequence number, randomly generated number or, a timestamp. This is a common defence against replay attacks where a malicious entity replays an old captured message to disrupt or compromise the network.

4.2.4 Authentication

The reliable verification of the transmission source's identity is a vital component to various security services such as key exchange or data confidentiality. Creation of a reliable authentication service in a decentralised environment is problematic due to issues of trust between nodes. For example, if node 'A' states that it is node A, how can node 'B' confirm this claim without a reliable central authority?

4.2.5 Availability

The implementation of security services cannot adversely impact the lifespan or availability of the network in any way. This requires the management of energy reserves and the maintenance of network resiliency. Network availability also implies the inclusion of adequate defensive mechanisms against Denial of Service attacks (see section 5.1 below).

4.2.6 Self Organisation

The security protocols, like the routing protocols detailed above, need to be self-organising and self-healing, as WSNs are commonly deployed in environments that are difficult or dangerous to access.

4.2.7 Time Synchronisation

The applications that a WSN runs often require the time on each node to be synchronised to allow the tracking of a moving event over time, such as tracking an animal's movement through the zone of interest. Time synchronisation is also required by some security protocols as time of transmission is used to evaluate data freshness.

4.2.8 Secure Localisation

Applications are often dependent on reliable location data from a sensor to provide accurate information analysis. Services should be provided to allow verification that a node's location is accurate and is not being faked.

5 Attack Types

5.1 Denial of Service

DoS attacks are defined by Wood *et al. (2002)* as *"any event that diminishes or eliminates a network's capacity to perform its expected function".* There are four primary vectors as detailed in *(Walters, Liang, Shi, & Chaudhary, 2006, pp. 10-15)* that an attacker might chose to implement a DoS attack.

1. **Radio Jamming**

   The blocking of radio transmissions, through the flooding of radio channels with noise.

2. **Link Layer**

   The intentional violation of the network communication protocols to cause network collisions and thereby cause packet/data loss.

3. **Routing Layer**

   The use of a compromised node to either misdirect or drop packets, thereby interrupting the routing of data.

4. **Connection Flooding**

   The initiation of multiple connection requests to a node with the aim of depleting the nodes resources. This can cause a node to permanently fail due to exhaustion of its energy reserves.

5.2 Routing Protocol Attacks

Karlof *et al.* (2003) propose a number of possible attacks on the routing protocols used in WSNs, including the altering of relayed data, selectively forwarding data, and sinkhole attacks. Such attacks can cripple a network, and defence against these attacks should be given high priority during network design.

5.2.1 Sinkhole Attack

A sinkhole attack refers to the injection of false replies to routing requests, which can be used to divert network traffic for the purpose of 'eavesdropping' on the data, or as part of a DoS attack by simply discarding the packets (Karlof & Wagner, 2003). An example of this attack is shown in Figure 7 below.

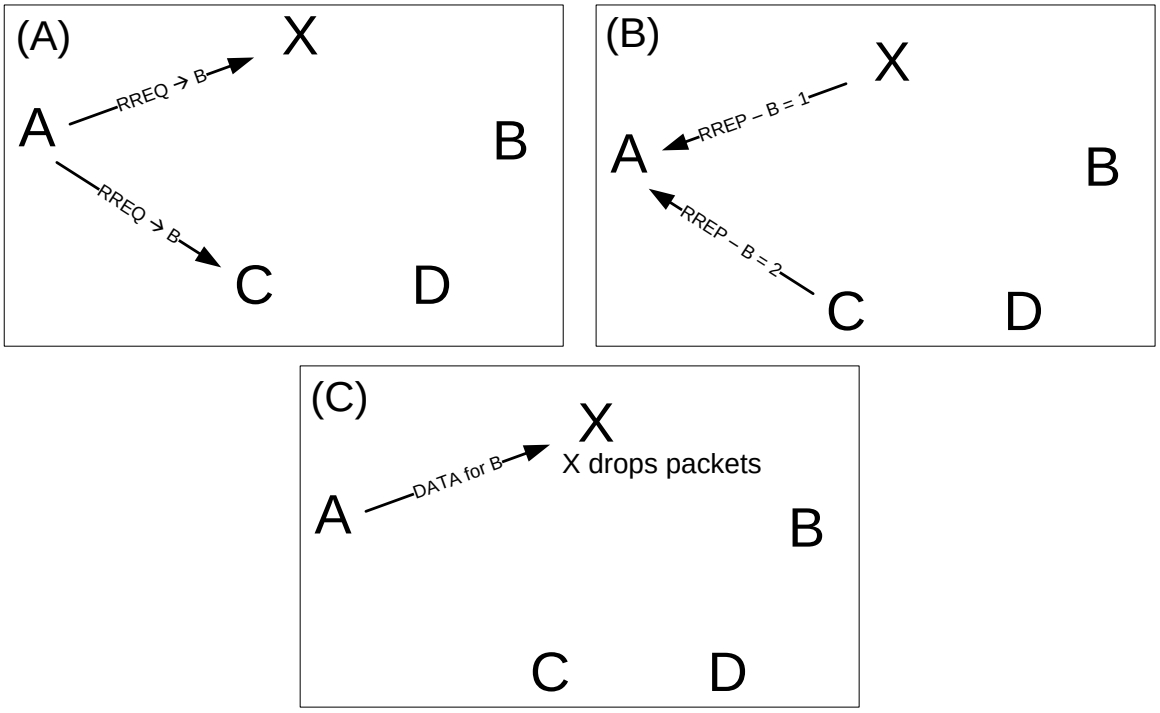

Figure 7 – Sinkhole Attack

A) Node 'A' sends out a route request ('RREQ') for a path to the sink node 'B'.
B) While node 'C' replies with a path to node B via 'D', a malicious node 'X' also replies, with a very low cost/metric.
C) Node A then selects the lowest cost route via X and transmits information to B via X. Node X then proceeds to either drop the data or sends it off network for some other nefarious purpose.

This technique can be used against any node whose transmission node X can receive and reply to, thus enabling a single node to disrupt a large section of the network.

5.2.2 Wormhole

A wormhole attack involves the tunnelling of captured data over a private link between two colluding nodes. The data can then be dropped, forwarded or modified at will by the malicious nodes (Hu, Perrig, & Johnson, 2003). This type of attack is an extension of the sinkhole attack detailed in section 5.2.1 above.

In Figure 8 below (reproduced from (Argyroudis & O'Mahony, 2005)), nodes 'X' and 'Y' are colluding to disrupt the network. They have replied to all route discovery requests with low cost/metric responses, thereby encouraging traffic to be relayed through them. Once the tunnel is set up, any relay traffic received by either node X or Y (in this case from nodes 'A' or 'B') is forwarded to its partner and back into the network, bypassing any intermediary nodes (in this case 'C' and 'D'). This example of the attack could be used to increase latency within the network by forcing data to take a non-optimal route, create a routing loop, or to modify or copy the data.

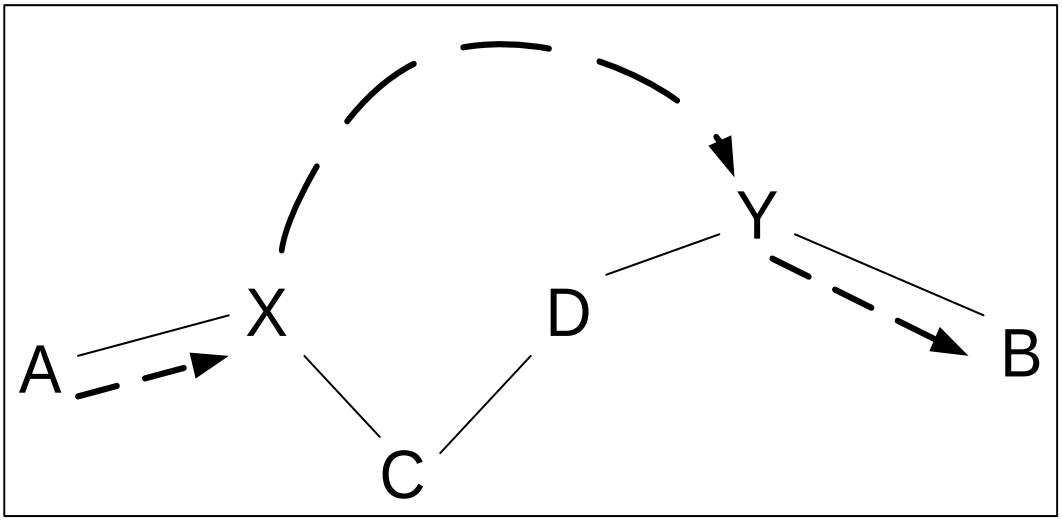

Figure 8 - Wormhole Attack

5.3 Replay Attack

Replay attacks are the re-transmission of captured messages, which can be used by an attacker to disrupt or compromise a network (Karlof & Wagner, 2003). This form of attack is typically a problem in WSNs where message contents are often repeated in a predictable manner. For example, a sensor may transmit a status update once every 30 minutes, stating "no intruders detected". If there is no protection in place it is possible for an attacker to change the sensor's environment or even destroy the sensor and retransmit an earlier copy of the "no intruders detected" message.

5.4 Sybil Attack

The Sybil Attack outlined by Newsome *et al.* (2004) defines an attack where a compromised node is employed to masquerade as multiple other nodes. This can have a large impact on data aggregation, cluster formation and routing. It is important to note that the false personas presented by the attacking node, need not be replicas of already existing nodes.

An example of a Sybil attack is shown in Figure 9 below .

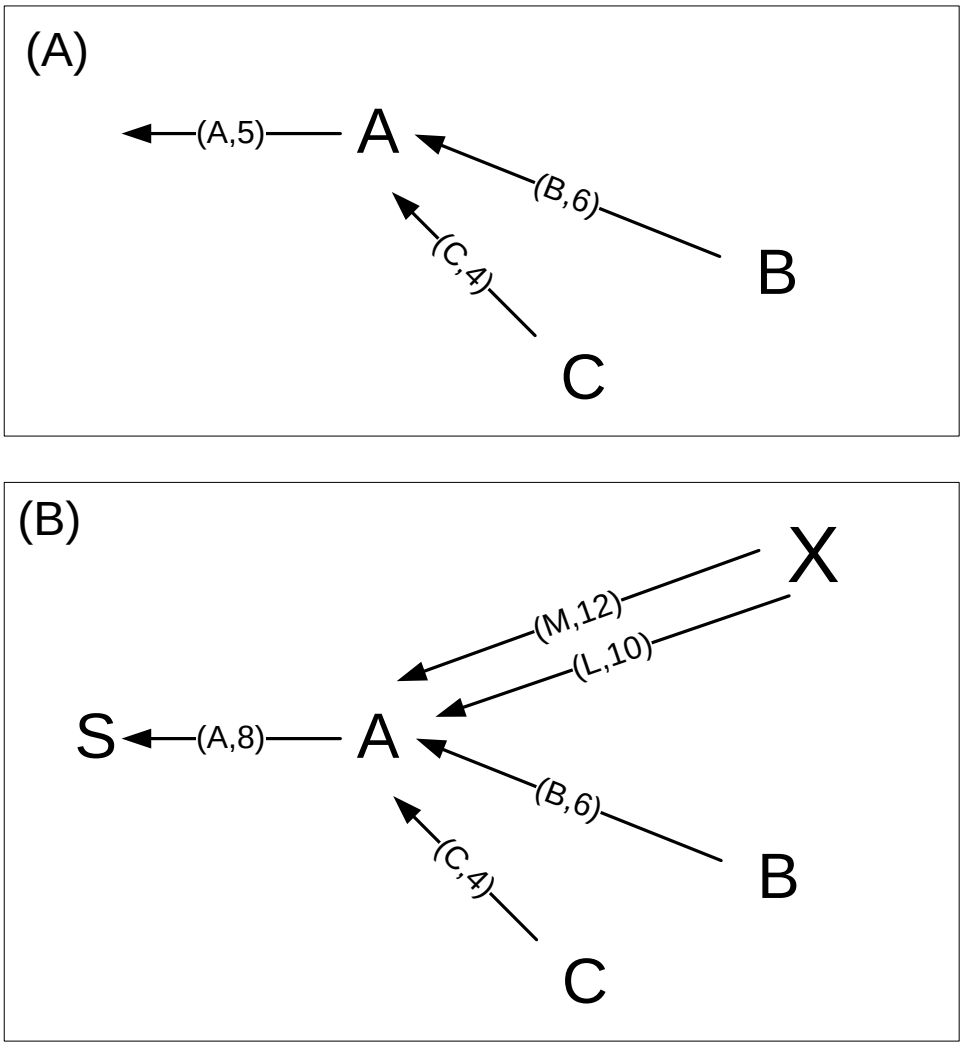

Figure 9 - Sybil Attack

A) Node 'A' collects data from other nodes (in this case nodes 'B' and 'C') and aggregates/averages the data with its own data (in this case A has a value of 0) before sending the result on to the sink node 'S'.

B) If node 'X' is masquerading as multiple false nodes (in this case nodes 'M' and 'L'), and forwarding false data to A, then the data A forwards to S will be inaccurate.

5.5 Node Replication

The attack methodology shown by Parno *et al.* (2005) is similar to the Sybil attack, except that the malicious node masquerades as one already existing node. This can allow the attacker to corrupt or misroute data, control segments of the network or possibly access cryptographic keys.

5.6 Traffic Analysis

Traffic analysis is used by an attacker to locate important nodes such as the sink, so that it can be either disabled or compromised. This attack is possible even if the data is encrypted, as shown in Deng *et al.* (2005). For example, if an attacker is able to monitor inter-node transmissions over a large area, it is possible by simply analysing the timing of these transmissions to determine the direction of data flow. By analysing a number of these flows an attacker can then determine the location of the sink node.

5.7 Attacks against Privacy

Walters *et al.* (2006, pp. 13-14) highlight a concern with respect to the transmission of potentially sensitive data (such as the position of subjects and nodes) over an unattended wireless network, as well as the storage of that information on unsecured hardware. This is a valid concern, particularly to those looking at the military and commercial applications of a WSN.

5.8 Physical Attacks

Owing to the unattended and unsecured nature of the devices employed in WSNs, the possibility of physical attacks on nodes is high. Simple attacks such as destroying or stealing nodes could have a significant impact on the survivability of the WSN. Hartung *et al.* (2005) show that the MICA2 mote can be compromised in less than one minute by a competent attacker. Demonstrations such as this highlight the need to improve the tamper resistance and detection technologies implemented in these devices.

6 Defensive Strategies

6.1 Key Establishment Protocols

The secure exchange and agreement of a cryptographic key, together with mutual agreement on the cipher algorithm to be used, are fundamental components of any confidentiality, integrity or authentication service implementation. The development of these protocols in WSNs is constrained by the resource limitations and self-managed infrastructure-less topology of these networks.

Various protocols for the secure exchange of keys have been posited using pre-shared keys to begin the key refresh process. Examples include those proposed by Huang *et al.* (Huang, Cukier, Kobayashi, Liu, & Zhang, 2003) and Eschenauer *et al.* (Du, Deng, Han, & Varshney, 2003; Molnar & Wagner, 2004; Hwang & Kim, 2004), as well as the Localized Encryption and Authentication Protocol ('LEAP') (Zhu, Setia, & Jajodia, 2003) and Peer Intermediaries for Key Establishment ('PIKE') (Chan & Perrig, 2005) protocols.

Protocols using public key approaches based on elliptic curve cryptography ('ECC') have also been proposed due to the short key lengths (160 bit) and performance advantages of ECC (Gura, Patel, Wander, Eberle, & Shantz, 2004).

The processing and energy restrictions of WSNs drive the need for careful selection of the cryptographic algorithm to be employed. Walters *et al.* (2006, p. 16) state that asymmetric algorithms require too much computation to be viable; however, other researchers have posited that asymmetric encryption could be used with careful algorithm selection (Gura, Patel, Wander, Eberle, & Shantz, 2004; Malan, Welsh, & Smith, 2004; Gura, Patel, Wander, Eberle, & Shantz, 2004; Watro, Kong, Cuti, Gardiner, Lynn, & Kruus, 2004). The alternative approach is to use less computationally expensive symmetric algorithms. Law *et al.* (2004) performed an analysis of the various ciphers and compared both the speed and computational load for each protocol, and found that while MISTY1 was the fastest overall and RC5-32 used the least memory, Rijndael was the most energy efficient.

The key establishment protocol and the cryptographic cipher used are critical elements to providing a secure and reliable network. The selection of a weak or inappropriate cipher can have major impact on both data security and network reliability. It is suggested that the use of dedicated cryptographic hardware may be one way in which the problem of processing power restrictions may be overcome. Devices such as 3G mobile phone handsets have similar limitations to those found in WSN hardware. During the development of the 3G architecture the MISTY1 cipher was optimised for implementation in hardware, creating the KASUMI block cipher. As the hardware required for the KASUMI cipher is becoming a commodity item, due to the fact that every 3G handset requires some implementation of this

cipher, it may be viable for the hardware to included in future WSN hardware. This advance would require the research and hardware communities to come to a consensus first. The use of such hardware, however, still leaves the issue of key management unaddressed.

6.2 Denial of Service Defences

The ability to mitigate or prevent DoS attacks is of critical importance in systems where availability is a key requirement, as it is in a WSN. Techniques such as increased redundancy of transmissions, transmission rate limiting, and area segregation as detailed by Wood *et al.* (2002) are vital to maintaining a network's ability to function while under attack.

Techniques such as increased transmission redundancy, while effectively mitigating the issue, increase the energy consumed and thereby reduce the active lifetime of the network. As data transmission has a much higher energy cost than data processing, approaches that use 'passive analysis' of incoming transmissions are preferable.

6.3 Securing Broadcast and Multicast Traffic

Due to the power restrictions of WSNs, efficient transmission mechanisms such as broadcast and multicast are used in preference to unicast transmissions. The management of the re-keying process in such an environment is difficult without employing a central authority. Di Pietro et al. (2003) propose a secure multicasting approach that uses Directed Diffusion along with a logical key hierarchy to remove the need for external key management infrastructure. The proposed Logical Key Hierarchy for Wireless sensor networks ('LKHW") protocol re-uses elements of the Directed Diffusion protocol, such as the interest notification mechanism, to handle the re-keying process. It is important to note that the protocol inherits the issues of the Directed Diffusion protocol on which it is based. For example, the re-keying process relies on the sink node to be the central source of keys, thus providing a single point of failure.

6.4 Routing Protocol Defence

Mishra *et al.* (2006) put forward an interesting intrusion tolerance system, INtrusion-tolerant routing protocol for wireless SEnsor NetworkS ('INSENS'), which sends multiple copies of a message along multiple paths to reduce the impact of a node that is intentionally misrouting. They also propose using a series of one-way key chains to avoid various possible attacks on their protocol such as a rogue node sending request messages. While this method does provide protection against routing attacks it also increases the energy consumption of the network.

A second method of providing confidentiality and authentication services at the routing layer is Trust Routing For Location-aware Sensor Networks ('TRANS') (Tanachaiwiwat, Dave, Bhindwale, & Helmy, 2003) which uses Micro Timed Efficient Stream Loss-tolerant Authentication ('μTELSA') key chains and time synchronisation in a system of trust relationship based routing.

A third method, involving the use of a directional antenna, has been proposed to defend against wormhole attacks; however, this is seen as an expensive solution to the problem. Wang *et al.* (2004) propose a novel technique based on surface visualisation to detect wormhole attacks.

6.5 Sybil Attack Mitigation

The node validation techniques given by Newsome *et al.* (2004) provide a method for protection against Sybil attacks based on trust relationships within the network. A node is vouched for by the sink node, another sensor node or via a system of radio channel switching.

Walters *et al.* (2006, p. 27) propose a limited key system to provide protection against Sybil attacks. The premise behind this method is that by using a system of multiple, random keys a node could never have enough keys to emulate multiple nodes.

6.6 Detecting Replicated Nodes

One method for detecting replicated nodes is for each node to broadcast an authentication message and receiving nodes to look for duplicate claims from different sources; however, this node broadcast strategy may be seen as too expensive in terms of transmission cost (Walters, Liang, Shi, & Chaudhary, 2006, p. 28). Parno *et al.* (2005) propose two schemes for reducing the number of transmissions to be sent by using multicast instead of broadcast. Multicasts are sent either in a completely random fashion, or based on the routing chains that are maintained by the routing protocol

6.7 Traffic Analysis

Deng *et al.* (2005) suggest a method for combating traffic analysis attacks through the use of dummy transmissions to hide the location of the sink node. To defend against more advanced traffic analysis techniques, such as time correlation attacks, Deng *et al.* (2005) propose a fractal propagation strategy in which a node will randomly send a dummy packet on the receipt of any packet.

6.8 Privacy

Several techniques have been posited to improve the anonymity of subject and node location information. These include the decentralisation of data, the insertion of fake data into the network,

encrypted communications (Gruteser, Schelle, Jain, Han, & Grunwald, 2003) and data flooding techniques (Ozturk, Zhang, & Trappe, 2004). Techniques such as the insertion of fake data or data flooding, can greatly increase the energy usage of a network and therefore may not be appropriate in networks with long deployment lifetimes.

6.9 Intrusion Detection

Classical intrusion detection strategies work on either the detection of anomalous activity (as compared to a measured baseline) or signature-based detection, where a signature is created for each attack and the network is monitored for signs of these signatures (Walters, Liang, Shi, & Chaudhary, 2006, p. 34). Brutch *et al.* (2003) propose several methods for implementing a combination of anomaly and signature-based detection. The proposals range from an individual node system through to a multi-node distributed hierarchical system. Both of these methods rely on the intruding node actively transmitting malicious packets and therefore neither method is able to defend against passive intruder attacks

6.10 Authenticated Data Aggregation

The aggregation of data in a hierarchical network model requires a certain level of trust that the data being aggregated is correct and accurate.

A model based on the μTESLA protocol has been proposed by Hu *et al.* (2003), which leverages the delayed keying system of μTESLA. The basic principle of this protocol is that each node is preloaded with a symmetric key that only that node and the sink node know. When a node forwards data to the sink node it encrypts it with that round's key. The second node along the path to the sink will hold the encrypted data for aggregation. After a predetermined time, the base station will broadcast the key for that round to the aggregating node. If the keys do not match, then action can be taken to confine the compromised node.

Przydatek *et al.* (2003) propose a three-stage system based on node-to-cluster head key sharing, hashing of the aggregated data using 'Merkle hash-trees', and the eventual communication with the sink including both the aggregated data and a hash. The sink node can then match the hashes against the data to confirm that the data is valid.

6.11 Physical Security Measures

The unsecured nature of node placement requires robust physical security measures to prevent node tampering. A variety of techniques have been proposed to improve the physical security of these devices including tamper-proofing the sensor housings (Wood & Stankovic, 2002), tamper-proofing the internal hardware components (Anderson & Kuhn, 1998; Anderson, Kuhn, & England, 1996). Along with novel

approaches such as the shutting down of nodes based on the detection of signal-finding equipment (Wang, Chellappan, Gu, Yu, & Xuan, 2005; Wang, Gu, Chellappan, Schosek, & Xuan, 2005). Hardware vendors will need to balance the implementation of strategies like tamper proofing their devices with maintaining a low 'per unit' cost.

6.12 Trust Management Strategies

Walters *et al.* (2006, p. 42) posit that the management of inter-device trust relationships is a key component in the development of secure and reliable WSNs. Ren *et al.* (2004) propose a distributed trust model based on an initial seeding by a 'secret dealer', which requires some form of centralised management node to act as the secret dealer.

6.13 Defensive Strategy Analysis

While the defensive strategies outlined above provide techniques and mechanisms to defeat or mitigate the impact of various attacks, there are no cohesive 'strategies' for protecting the network as a whole from a broad range of attacks.

Additionally, it is proposed that before such targeted defensive techniques can be implemented, the basic security services, such as data encryption, must first be present. Furthermore, a sufficiently robust implantation of the basic security services would mitigate a large number of these attacks, thereby simplifying the protocols.

7 SE-LEACH

On analysis of the various routing protocols and security requirements for WSNs, it is apparent that further research is needed into new protocols that are designed with security in mind, as well as the extension of current protocols to integrate these security services. To this end, this paper proposes a theoretical extension to the LEACH protocol which integrates security services into the protocol, called Security Enabled - Low-Energy Adaptive Clustering Hierarchy ('SE-LEACH').

7.1 Assumptions

The following assumptions have been made while creating this model:

1) All devices are statically located;
2) All sensor nodes use the same hardware;
3) Some pre-configuration of the nodes will be undertaken; and
4) Additional pre-configuration is acceptable.

7.2 Goals

This theoretical model has been designed to meet the following requirements as defined in section 4.2:

- Data Confidentiality;
- Data Integrity;
- Data Freshness;
- Availability; and
- Self-Organisation.

While secure-localisation, time-synchronisation and authentication services are not implemented in the proposed SE-LEACH framework, extension of the framework to incorporate these features, if required, is possible.

The LEACH routing protocol was chosen as the basis for this proposal owing to its hierarchical structure and energy efficient design. The proposed additions to the LEACH protocol put forward in this paper may also be applicable to LEACH-inspired, cluster-based protocols such as TEEN and APTEEN.

Further design goals for the SE-LEACH protocol are that it should be both application and hardware agnostic, and allow for flexibility during configuration to take into account hardware limitations and specific deployment requirements. This flexibility enables changes to cryptographic algorithms as well as

the ability to take advantage of additional hardware features, such as a dedicated cryptographic hardware.

7.3 Design Principles

The issue of ensuring that network availability is not adversely affected by the security protocol implementation is difficult to address, particularly in the case of a theoretical model.

Nevertheless, in an effort to address this issue and reduce the impact of the additional security services on the performance of the WSN, the following design principles were employed:

1. **Modular Design**

   The use of a modular framework allows the user to implement only the services that they require for their application, thereby maximising the operating capacity of the network.

2. **Computation over Transmission**

   The energy cost of computation as compared to radio transmission is approximately 1000 calculations to 1 bit of data transfer; however, this depends on the distance that the data must be transferred as transmission cost increases by the square of the distance. Thus, if it is possible to reduce the amount of data to be transmitted by increasing the number of calculations, then this is preferable.

3. **Single-Way Methods**

   As mentioned above, the cost of data transmission is high in WSN systems. While there is an energy cost associated with each bit transmitted, there is also a cost associated with transmission overheads such as headers. It is therefore preferable to use single-way methods that require only one transmission as compared to a two or three-way method, which would require multiple transmissions. It is important to note that single-way methods are less secure than multiple transmission methods due to reduced validation and verification; however, with the focus on reducing energy consumption, this is a justifiable risk.

4. **Integration and Re-use of Existing Mechanisms**

   Where there are existing mechanisms in place in the LEACH protocol it is unnecessary to re-create those mechanisms within the security protocols of SE-LEACH. For example, the proposed SE-LEACH protocol integrates key distribution functionality and the existing cluster head role, thereby making good use of the existing mechanism already present in LEACH. This existing mechanism in the LEACH protocol provides energy-use-levelling via role rotation within a cluster. This integration

also allows the key management feature of SE-LEACH to take advantage of the self-organisation and self-healing features of LEACH.

7.4 Location of Services

The network model used in WSNs is much simpler than the standard 4 layer TCPIP model or the more complex 7 layer OSI model. The 'WSN network model' can easily be represented as 3 layers:

Layer 1 - The Physical Link Layer

This layer encompasses physical media access and serialisation of the data onto the physical medium, which may be 802.11 wireless, satellite, etc. The 'packetisation' and physical addressing of the data to be delivered is also handled at this layer. This layer is equivalent to OSI layers 1 and 2 (refer Figure 10 below).

Layer 2 - The Network Layer

This layer is concerned with the routing and logical addressing of data. The network routing protocol used, such as the LEACH or SPIN protocol, resides in this layer. This layer corresponds to layers 3-5 of the OSI model (refer to Figure 10 below).

Layer 3 - The Application Layer

This layer is concerned with general processing and generating transmission requests, and corresponds to layers 6 and 7 of the OSI model (refer Figure 10 below).

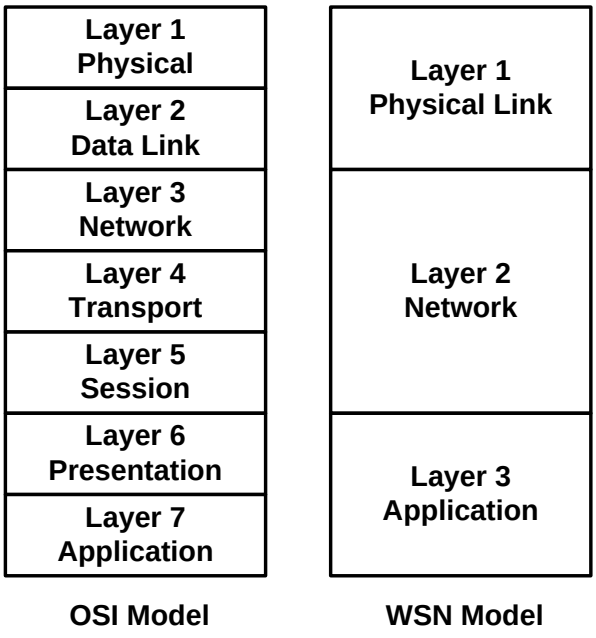

Figure 10- A Comparison of the OSI and WSN Network Models

Unlike the OSI or TCP/IP models found in standard network environments, there can be a great deal of interaction between the network layer and the application layer in the WSN model. This is especially so for routing protocols such as Directed Diffusion, that define interest statements and use query-based transfers. For this reason, it is necessary for the application to be written with a particular routing protocol in mind.

To protect the network from a range of attacks it is necessary to place the security services at the lowest possible position in the network stack, while maintaining the ability to port the protocol to various hardware platforms and transmission mediums. Subsequently, it is proposed that for the SE-LEACH protocol, the security mechanisms be placed between layer 1 and layer 2, with heavy interaction with layer 2 for key management etc.

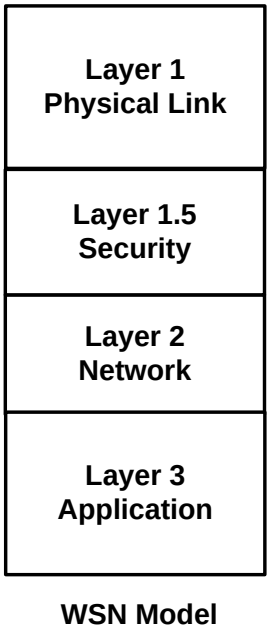

Figure 11 - Proposed Network Model

7.5 Modules

The proposed SE-LEACH protocol is designed in a modular fashion to allow flexibility during deployment. Further, the security services are to be divided into the following major modules:

- Data Confidentiality;
- Key Management;
- Data Integrity; and
- Data Freshness.

Due to the interdependency between these modules, an implementation of the Key Management module is required by the Data Confidentiality, Data Integrity and Data Freshness modules.

7.6 Key Management

The integration of data confidentiality services requires two components; an encryption mechanism to obfuscate the data and a method for distributing a secret key between authorised nodes.

The proposed key management system for SE-LEACH uses a variation of the SEAMAN protocol put forward by Bonartz *et al.* (2008), which defines a method for distributed key management within military, multicast, mobile, ad-hoc networks.

During the cluster formation phase of the LEACH protocol, a cluster head is elected which is responsible for aggregating all of the data for that cluster and forwarding it to the sink node. To ensure that the initialisation of the network is secure when using the SE-LEACH protocol, it is proposed that a preloaded encryption key be used. While not mandatory, its use removes a major attack vector.

It is also proposed that this cluster head node become the Key Distribution Centre ('KDC') for the cluster. The KDC/cluster head will generate a group key and forward it to all nodes in its cluster, including the sink node. Thus, the sink node will have a key for each cluster.

In order to allow time for all nodes to switch to the new key, both the old key and new key are acceptable as decryption keys for a brief period (see Figure 12 reproduced from (Bongartz, Ginzler, Bachran, & Tuset, 2008)).

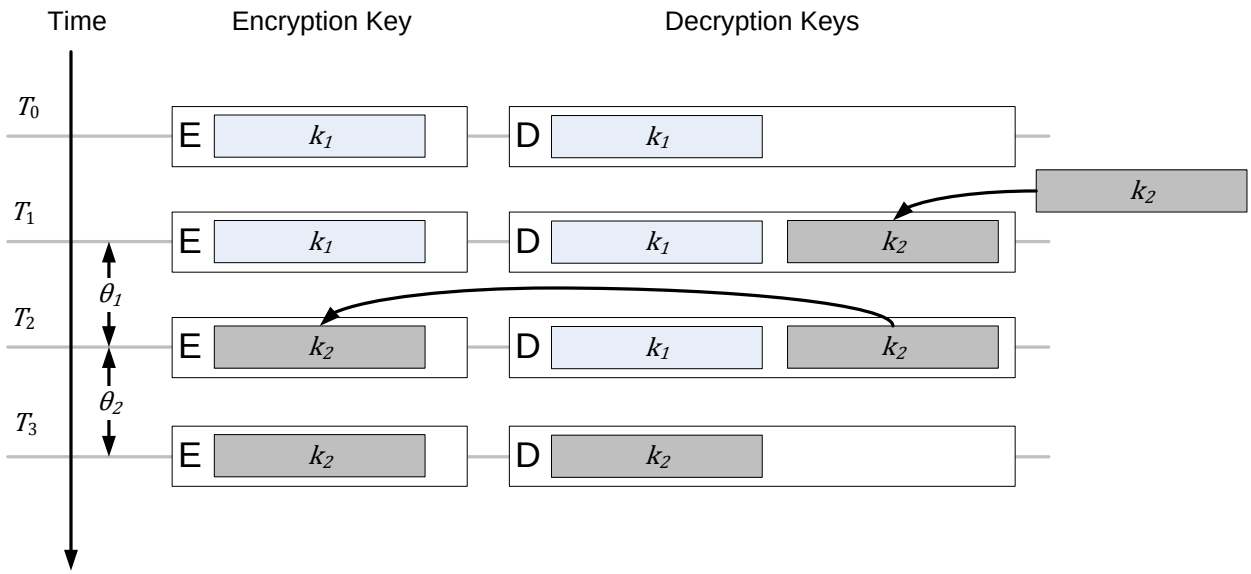

Figure 12 - Key Update Sequence

The key update process as shown in Figure 12 above has 4 steps. An explanation of each step is given below.

Time: T_0

All nodes have group key k_1 for both encryption and decryption. The network can be said to be in a converged state.

Time: T_1

At a predetermined interval, the cluster head transmits a new key k_2 to all nodes. Each node then allows both keys k_1 and k_2 for the decryption of messages.Θ

Time: T_2

After a predetermined time θ_1, each node replaces their encryption key with k_2.

Time: T_3

After a predetermined time θ_2, each node removes the decryption key k_1. At this point, all nodes will be using only k_2 for all decryption and encryption, and the network is again converged.

This key update process also allows for re-keying when a new cluster head is elected, or if a node fails. A node should only accept a new key from the current cluster head.

This module can be modified to use alternative key management strategies including the use of statically configured keys.

7.7 Data Confidentiality

In order to meet the design principles outlined in section 7.3, the encryption mechanism is designed to be modular. This allows the use of any symmetric key algorithm, such as Rijndael or MISTY1, and both software and hardware implementations of these algorithms.

The encryption module relies on the key management module to provide the cryptographic key required to encrypt and decrypt messages.

When a message is transmitted from one node to another, the source node will encrypt the message with the shared key. On receiving the encrypted message, the receiving node will decrypt the message with either the current key or, if the network is in a 'key update' phase, the previous key.

A message transmitted from 'A' to 'B' would take the form:

$$(Message)_{k_1}$$

7.8 Data Integrity

Thus far, while the SE-LEACH protocol provides data confidentiality and protection from routing attacks, it provides no mechanism for data integrity. It is proposed that a Hashed Message Authentication Code ('HMAC') be transmitted along with the actual message so that the receiving node can validate the message.

A message transmitted from 'A' to 'B' would take the form:

$$(Message)_{k_1} + H(Message \oplus k_1)$$

Upon receiving the transmission, B would decrypt the message using k_1. B can then XOR the received message with k_1 and hash the result. If the received HMAC matches the calculated value, then the message is valid and has not been tampered with.

7.9 Data Freshness

The proposed SE-LEACH protocol can be extended to ensure data freshness. The message and HMAC could also contain a single use number or 'NONCE' to prevent message playback. This protocol uses a random number generated by the sender, which is appended to the message text. This combination is then hashed as part of the HMAC process.

For example:

$$(Message + NONCE)_{k_1} + H((Message + NONCE) \oplus k_1)$$

If the receiver sees two messages with the same NONCE then it determines that the message is being replayed and discards the message. To allow for matching of past NONCE values, the receiving node will need to store these values in memory. Due to variations in hardware capability and security level requirements, SE-LEACH permits the length of the NONCE and the number of past NONCE values to be configurable.

7.10 Further Extension

As mentioned above, it is possible to extend the SE-LEACH framework to provide secure localisation, time-synchronisation and authentication mechanisms if required by the deployment. These services could be used to further enhance the services proposed above. For example, a secure authentication mechanism would provide an additional layer of security to the key management service.

8 Conclusion

This paper examined the various architectural requirements and restrictions of, network routing protocols used in WSNs. The research community's discourse on the possible attacks on these networks has provided a new array of malicious techniques that must be taken into account when designing a WSN security strategy. To combat these new attacks, security techniques and services have been developed; however, there has been little investigation into the integration of these security services into existing network protocols. Following an analysis of some of the more prominent network protocols used in WSNs, it was determined that the current protocols provided minimal, if any, security.

An extension to the LEACH protocol, SE-LEACH, was proposed to demonstrate one method of implementing security services in WSNs, such as data integrity, data freshness and data confidentiality. It is proposed that these basic services, if implemented correctly, can overcome many of the security issues of WSN deployments. Furthermore, the proposed SE-LEACH protocol's flexible design enables additional security services, such as authentication or time-synchronisation, to be integrated into the framework.

It is also recommended that future research and development in the area of WSN protocols focus on both improving the efficiency of the network, as well as integrating security services within either the routing or the data link protocols.

List of Acronyms

µTESLA	Micro Timed Efficient Stream Loss-tolerant Authentication
APTEEN	Adaptive Periodic Threshold-sensitive Energy Efficient Sensor Network Protocol
BGP	Border Gateway Protocol
DoS	Denial of Service
ECC	Elliptic Curve Cryptography
GAF	Geographical Adaptive Fidelity
GPS	Global Positioning System
HMAC	Hash Message Authentication Code
IP	Internet Protocol
IPv4	Internet Protocol version 4
INSENS	Intrusion-Tolerant Routing in Wireless Sensor Networks
KDC	Key Distribution Centre
LEACH	Low-Energy Adaptive Clustering Hierarchy
LEAP	Localized Encryption and Authentication Protocol
LKHW	Logical Key Hierarchy for Wireless Sensor Networks
MAC	Message Authentication Code
MECN	Minimum Energy Communication Network
MISTY1	Mitsubishi Improved Security Technology version 1
NONCE	Number Once
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
PEGASIS	Power Efficient GAthering in Sensor Information Systems

PIKE	Peer Intermediaries for Key Establishment
QoS	Quality of Service
RC5-32	Rivest Cipher version 5 32bit
RIP	Routing Information Protocol
SDRAM	Synchronous Dynamic Random Access Memory
SE-LEACH	Security Enabled - Low-Energy Adaptive Clustering Hierarchy
SEAMAN	Security-Enabled Anonymous MANET protocol
SIA	Secure Information Aggregation
SMECN	Small Minimum Energy Communication Network
SPIN	Sensor Protocols for Information via Negotiation
SRAM	Static Random Access Memory
TCPIP	Transmission Control Protocol Internet Protocol
TEEN	Threshold sensitive Energy Efficient sensor Network protocol
TRANS	Trust Routing for Location Aware Sensor Networks
WSN	Wireless Sensor Network

Table of Figures

Bibliography

Akkaya, K., & Younis, M. (2005). A Survey on Routing Protocols for Wireless Sensor Networks.

Akkaya, K., & Younis, M. (2003). An energy-aware QoS routing protocol for wireless sensor networks., (pp. 710-715).

Anderson, R. J., & Kuhn, M. G. (1998). Low Cost Attacks on Tamper Resistant Devices. (pp. 125-136). Springer-Verlag.

Anderson, R., Kuhn, M., & England. (1996). Tamper Resistance - a Cautionary Note., (pp. 1-11).

Argyroudis, P. G., & O'Mahony, D. (2005). Secure routing for mobile ad hoc networks. *Communications Surveys \& Tutorials, IEEE , 7*, 2-21.

Bongartz, Ginzler, T., Bachran, T., & Tuset, P. (2008). SEAMAN: A Security-Enabled Anonymous MANET Protocol. *NATO Research and Technology Organisation.*

Brutch, P., & Ko, C. (2003). Challenges in intrusion detection for wireless ad-hoc networks., (pp. 368-373).

Chan, H., & Perrig, A. (2005). PIKE: peer intermediaries for key establishment in sensor networks., *1*, pp. 524--535 vol. 1.

Crossbow. (2007). *Imote2 Datasheet.* Crossbow Technology, Inc.

Deng, J., Han, R., & Mishra, S. (2005). Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks., (pp. 113-126).

Deng, J., Han, R., & Mishra, S. (2005). Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks., (pp. 113-126).

Deng, J., Han, R., & Mishra, S. (2006). INSENS: Intrusion-tolerant routing for wireless sensor networks. *Computer Communications , 29*, 216-230.

Du, W., Deng, J., Han, Y. S., & Varshney, P. K. (2003). A pairwise key pre-distribution scheme for wireless sensor networks. (pp. 42-51). ACM Press.

Gruteser, M., & Grunwald, D. (2003). A Methodological Assessment of Location Privacy Risks in Wireless Hotspot Networks. *2802*, pp. 10-24. Springer.

Gruteser, M., Schelle, G., Jain, A., Han, R., & Grunwald, D. (2003). Privacy-aware location sensor networks. (p. 28). USENIX Association.

Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs.

Hartung, C., Balasalle, J., & Han, R. (2005). *Node Compromise in Sensor Networks: The Need for Secure Systems.* University of Colorado at Boulder. University of Colorado at Boulder.

Heinzelman, W. R., Ch, A., & Balakrishnan, H. (2000). Energy-efficient communication protocol for wireless microsensor networks. 3005-3014.

Heinzelman, W. R., Kulik, J., & Balakrishnan, H. (1999). Adaptive protocols for information dissemination in wireless sensor networks. (pp. 174-185). ACM Press.

Hu, L., & Evans, D. (2003). Secure aggregation for wireless networks., (pp. 384-391).

Hu, Y. C., Perrig, A., & Johnson, D. B. (2003). Packet leashes: a defense against wormhole attacks in wireless networks., *3*, pp. 1976--1986 vol.3.

Huang, Q., Cukier, J., Kobayashi, H., Liu, B., & Zhang, J. (2003). Fast authenticated key establishment protocols for self-organizing sensor networks. (pp. 141-150). ACM.

Hwang, J., & Kim, Y. (2004). Revisiting random key pre-distribution schemes for wireless sensor networks. (pp. 43-52). ACM.

Intanagonwiwat, C., Govindan, R., & Estrin, D. (2000). Directed diffusion: a scalable and robust communication paradigm for sensor networks. (pp. 56-67). ACM Press.

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures., (pp. 113-127).

Law, Y. W., Doumen, J., & Hartel, P. (2004). Survey and benchmark of block ciphers for wireless sensor networks. *ACM Transactions on Sensor Networks , 2*, 447-456.

Li, L., & Halpern, J. Y. (2001). Minimum-energy mobile wireless networks revisited., *1*, pp. 278--283 vol.1.

Lindsey, S., & Raghavendra, C. S. (2002). PEGASIS: Power-efficient gathering in sensor information systems., *3*, pp. 3-1125--3-1130 vol.3.

Malan, D. J., Welsh, M., & Smith, M. D. (2004). A public-key infrastructure for key distribution in TinyOS based on elliptic curve cryptography., (pp. 71-80).

Manjeshwar, A., & Agrawal, D. P. (2002). APTEEN: a hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks., (pp. 195-202).

Manjeshwar, A., & Agrawal, D. P. (2001). TEEN: a routing protocol for enhanced efficiency in wireless sensor networks., (pp. 2009-2015).

Molnar, D., & Wagner, D. (2004). Privacy and security in library RFID: issues, practices, and architectures. (pp. 210-219). ACM Press.

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). The Sybil attack in sensor networks: analysis \& defenses., (pp. 259-268).

Ozturk, C., Zhang, Y., & Trappe, W. (2004). Source-location privacy in energy-constrained sensor network routing. (pp. 88-93). ACM.

Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks., (pp. 49-63).

Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks., (pp. 49-63).

Pietro, R. D., Mancini, L. V., Law, Y. W., Etalle, S., & Havinga, P. (2003). LKHW: a directed diffusion-based secure multicast scheme for wireless sensor networks., (pp. 397-406).

Przydatek, B., Song, D., & Perrig, A. (2003). SIA: secure information aggregation in sensor networks. (pp. 255-265). ACM.

Ren, K., Li, T., Wan, Z., Bao, F., Deng, R. H., & Kim, K. (2004). Highly reliable trust establishment scheme in ad hoc networks. *Comput. Netw. , 45*, 687-699.

Rodoplu, V., & Meng, T. H. (1999). Minimum energy mobile wireless networks. *Selected Areas in Communications, IEEE Journal on , 17*, 1333-1344.

Tanachaiwiwat, S., Dave, P., Bhindwale, R., & Helmy, A. (2003). Poster abstract secure locations: routing on trust and isolating compromised sensors in location-aware sensor networks. (pp. 324-325). ACM.

Tilak, S., Abu-Ghazaleh, N. B., & Heinzelman, W. (2002). A taxonomy of wireless micro-sensor network models. *SIGMOBILE Mob. Comput. Commun. Rev. , 6*, 28-36.

Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2006). Wireless sensor network security: A survey. In *Security in Distributed, Grid, and Pervasive Computing.* Auerbach Publications, CRC Press.

Wang, W., & Bhargava, B. (2004). Visualization of wormholes in sensor networks. (pp. 51-60). ACM Press.

Wang, X., Chellappan, S., Gu, W., Yu, W., & Xuan, D. (2005). Search-based physical attacks in sensor networks., (pp. 489-496).

Wang, X., Gu, W., Chellappan, S., Schosek, K., & Xuan, D. (2005). Lifetime optimization of sensor networks under physical attacks., *5*, pp. 3295--3301 Vol. 5.

Watro, R., Kong, D., Cuti, S. F., Gardiner, C., Lynn, C., & Kruus, P. (2004). TinyPK: securing sensor networks with public key technology. (pp. 59-64). ACM Press New York.

Wood, A. D., & Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer , 35*, 54-62.

Yu, Y., Govindan, R., & Estrin, D. (2001). Geographical and Energy Aware Routing: A Recursive Data Dissemination Protocol for Wireless Sensor Networks.

Zhu, S., Setia, S., & Jajodia, S. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks. (pp. 62-72). ACM Press.