Security Framework for Wireless Sensor Networks

Stuart Stent
Department of Computing
Macquarie University
Sydney, Australia
stuart.stent@mq.edu.au

Abstract

This paper presents an overview of the various issues and requirements of Wireless Sensor Network ('WSN') deployments, and explores the unique network architecture of WSNs and the security issues involved. It is determined 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 confidentiality, key management, data integrity and data freshness in the form of a flexible and extendable framework, thereby overcoming the security issues of existing WSN protocols.

1 Introduction

Recent advances in computer hardware have allowed the development of new data collection techniques utilising wirelessly networked sensor devices to sample the environment and transmit the data back to a central location for analysis. These Wireless Sensor Networks ('WSN') are becoming an invaluable tool for collecting data in dangerous or inaccessible locations such as geologically unstable or radioactive environments. As WSNs are relied on increasingly for the collection of data, the security of that data is becoming a growing concern for those considering the deployment of this technology. In order to develop a security strategy for WSN systems, it is first necessary to understand the technical requirements, architectural limitations and security issues of WSNs. These issues are discussed in Section 2. In Section 3, an extension to the LEACH protocol is proposed. This extension aims to address the security issues of WSNs, by integrating a new extendable security framework into the existing routing protocol. Finally, the findings of the paper are outlined in section 4.

2 Technical Background

2.1 Restrictions and Requirements

The unique characteristics of WSN technologies can greatly affect the ability to provide adequate security services. To this end, it is important to have an understanding of these characteristics and their inherent limitations when designing security solutions for WSNs.

The key issues that need to be considered when developing security services for WSNs are:

Processing and Storage: The processing power and data storage capabilities of WSN nodes are very limited and require the efficient design of computational algorithms (Walters, Liang, Shi, & Chaudhary, 2006, p. 3).

Power: The energy reserves available to a WSN node are generally very limited; 2-3 AAA batteries is a common configuration. Nodes are expected to run for extended periods of time (1-2 years) on this internal energy reserve (Tilak, Abu-Ghazaleh, & Heinzelman, 2002).

Reliability: Due to the inaccessible locations in which WSNs are deployed, it is imperative that the network be reliable and not require manual intervention (Walters, Liang, Shi, & Chaudhary, 2006; Akkaya & Younis, 2005).

Cost: The cost of WSN deployments must not be adversely impacted by the inclusion of security services, as cost is often a major factor in selection of WSN technology over traditional methods (Tilak, Abu-Ghazaleh, & Heinzelman, 2002).

2.2 Network Architecture

The limitations and requirements outlined in section 2.1 above preclude the use of traditional

network technologies that are not energy-aware, or that require a large amount of configuration and maintenance. To meet these new requirements a range of new protocols have been proposed. These new protocols can be defined by both their data collection methodology (Continuous, Event-Driven, Data-Driven or Hybrid) (Tilak, Abu-Ghazaleh, & Heinzelman, 2002) or by their networking paradigm (Data-Centric, Hierarchical, Location-based or QoS-aware) (Akkaya & Younis, 2005, p. 2). Each of these models fulfils a particular usage requirement. For example, the continuous data collection or event-driven models are more suited to a security monitoring application than a query-driven model. Similarly, each network paradigm may be better suited to a particular application than another.

Some of the more prominent of these protocols are outlined below:

SPIN: The Sensor Protocols for Information via Negotiation ('SPIN') (Heinzelman, Kulik, & Balakrishnan, 1999) protocol is a Data-Centric Event-Based protocol in which an advertisement detailing the available data is generated whenever a new piece of data becomes available. Nodes that are interested in that data request the data from the node.

Directed Diffusion: Directed Diffusion is a Data-Centric Query-Based protocol developed by Intanagonwiwat *et al.* (2000). Nodes collect data and only transmit that data when they receive an 'interest' statement from the base station node. Due to the fact that data is only transmitted when required, Directed Diffusion is more energy efficient than the earlier SPIN protocol.

LEACH: One of the first hierarchical routing protocols developed was the Low-Energy Adaptive Clustering Hierarchy ('LEACH') protocol, proposed by Heinzelman *et al.* (2000). LEACH divides the network up into smaller networks called clusters. Each cluster elects a 'cluster head' node which is responsible for aggregating all of the data from that cluster and forwarding it to the sink node. This clustering allows for much larger networks and is far more energy efficient than either SPIN or Directed Diffusion.

2.3 Security Issues

The development of new routing protocols and techniques has led to the inevitable development of new security issues and attacks. Some of the possible types of attacks are outlined below:

Denial of Service: Wood *et al.* (2002) define a Denial of Service ('DoS') attack as "any event that diminishes or eliminates a network's capacity to perform its expected function". These attacks range from radio jamming to flooding the network with data (Walters, Liang, Shi, & Chaudhary, 2006, pp. 10-15).

Routing Protocol Attacks: These attacks misuse the routing protocol to redirect traffic to a malicious node, alter the transmitted data or selectively forward data (Karlof & Wagner, 2003).

SYBIL Attack: This attack involves a malicious node masquerading as multiple other nodes in order to disrupt routing, cluster formation or data aggregation (Newsome, Shi, Song, & Perrig, 2004).

Node Replication: This attack is similar to the SYBIL attack above; however, the malicious node only masquerades as a single already existing node.

Traffic Analysis: This attack involves the analysis of data transmission patterns to determine the location of a particular node, in order to destroy or compromise the node. This attack can be performed even if the data is encrypted (Deng, Han, & Mishra, 2005).

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.

All of the afore-mentioned attacks can be categorised as either 'information-gathering' or 'disruptive'. Techniques such as the SYBIL and Node Replication attacks, which allow one node to masquerade as another node(s), may fall into either category, while others such as the DoS attacks are explicitly disruptive.

While classical security techniques are capable of defending against these attacks, they are rarely designed with energy efficiency in mind and are therefore inappropriate for use in a WSN environment.

2.4 Security Requirements

Walters *et al.* (2006, pp. 5-10) define eight requirements that are necessary to ensure a secure sensor network environment. These requirements are:

Data Confidentiality: The data being transferred should not be readable by an unauthorised party.

Data Integrity: The receiver of transmitted data should be able to verify that the data has not been tampered with or corrupted.

Data Freshness: The receiver should be able to verify that the message has not been resent. This is used to mitigate the replay attack given in section 2.3.

Authentication: The receiver should be able to verify the identity of the sender.

Availability: The implementation of security services should not adversely affect the ability of the network to function.

Self-Organisation: Due to the unmanaged nature of WSN deployments, the security services should be self-initialising once in the field and self-healing.

Time-Synchronisation: The ability to securely and accurately synchronise times between nodes is a requirement of other security services and applications.

Secure Localisation: To support applications that are based on accurate location data, it should be possible to verify that a node's location is accurate and is not being faked.

It is important to note that this list of services is neither exhaustive nor mandatory, and the security services used should be tailored to the particular requirements of a deployment. For example, an application for tracking shipping containers and their cargos is likely to require a data confidentiality service, whereas one tracking less sensitive data will not. This ability to tailor services is of the utmost importance. Each service has its own unique overheads in terms of energy and bandwidth consumption, thus reducing the operating life of the network.

3 SE-LEACH

There has been significant research into techniques to counter the attacks outlined in section 2.3; however, there has been less investigation into the integration of these services with the routing protocols outlined in section 2.2 above. This paper proposes a theoretical protocol, Security Enabled - Low-Energy Adaptive Clustering Hierarchy ('SE-LEACH'). SE-LEACH is designed to extend the popular LEACH routing protocol by integrating several security features into the protocol using a modular framework.

The LEACH protocol is a hierarchical protocol that uses radio strength measurements to divide the network into smaller networks called 'clusters'. Each cluster elects a 'cluster head' node, which is responsible for aggregating all of the data from that cluster and transmitting it back to the sink node. In order to spread the energy consumption evenly over the network, the cluster head role is rotated around all nodes in a cluster.

3.1 Assumptions

The following assumptions have been made in the formulation of the SE-LEACH protocol:

- All devices are statically located;
- Sensor nodes all use the same hardware;
- Some pre-configuration of the nodes will be undertaken; and
- Additional pre-configuration is acceptable.

3.2 Goals

This theoretical model has been designed to meet the following set of requirements as defined in section 2.4:

- Data Confidentiality;
- Data Integrity;
- Data Freshness;
- Network Availability; and
- Self organisation.

The LEACH routing protocol was chosen as the basis for this proposal due 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 (Manjeshwar & Agrawal, 2001) and AP-TEEN (Manjeshwar & Agrawal, 2002).

Further design goals for SE-LEACH are that it should be both application and hardware agnostic, and allow for flexibility during configuration to take into account WSN 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.

3.3 Design Principles

The issue of ensuring that network availability is not adversely affected by the security protocol implementation is a difficult issue 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:

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.

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.

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.

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.

3.4 Placement of Security 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 1 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 protocols, resides in this layer. This layer corresponds to layers 3-5 of the OSI model (refer to Figure 1below).

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 1 below).

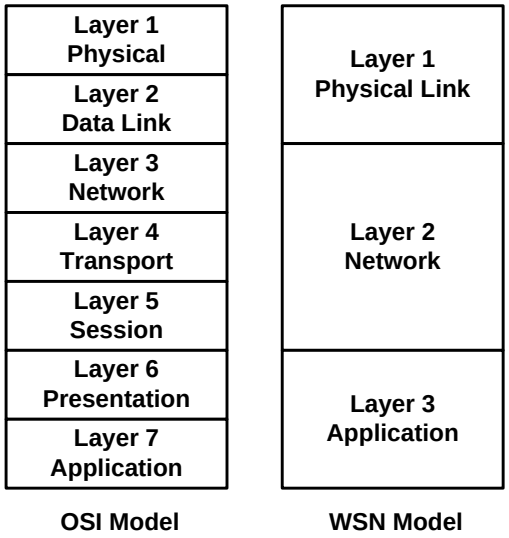

Figure 1- A Comparison of the OSI and WSN Network Models

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 data confidentiality mechanism be placed between layer 1 and layer 2, with heavy interaction with layer 2 for key management etc.

3.5 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.

3.6 Data Confidentiality

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.

In order to meet the design principles outlined in section 3.3, 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.

3.7 Key Management

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. 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 2 reproduced from (Bongartz, Ginzler, Bachran, & Tuset, 2008)). 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.

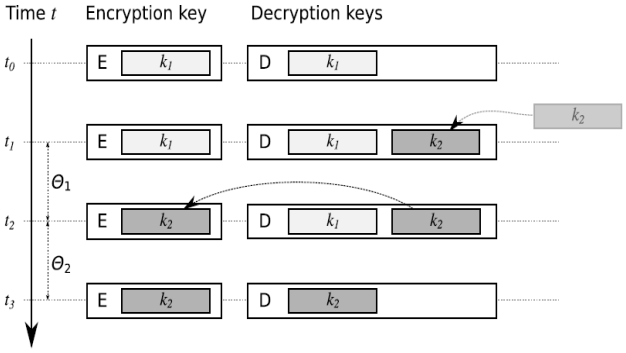

Figure 2 - Key Update Sequence

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:

$$(Message)_{k_1}$$

3.8 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.

3.9 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.

3.10 Critical Analysis

The primary purpose of the proposed SE-LEACH protocol is to highlight the ability to successfully integrate security services into an existing WSN routing protocol, in this case LEACH.

The modules defined in SE-LEACH provide a framework and a basic set of security services. The data confidentiality, key management, integrity and freshness mechanisms used in this protocol are designed to be selectable and replaceable based on the specific implementation requirements. Moreover, owing to the flexibility of the modular design, if further protection is required against advanced attacks, such as the SYBIL attack, an authentication service could easily be integrated.

4 Conclusion

This paper has presented an overview of the current state of WSN network and security technology. 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, techniques and security services have been developed; however, little there has been little investigation into the integration of these security services with the existing network protocols. An extension to the LEACH protocol, SE-LEACH, is proposed to demonstrate one method of implementing these security services, and overcome many of the security issues with current WSN protocols.

5 References

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

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

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

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.

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).

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).

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

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.

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