Trustworthy Sensor Networks

Project Proposal

ITEC810 – Project Unit

Author	Daniel Aegerter, 41542053
Supervisor	Rajan Shankaran
Department	Department of Computing
Due date	21.08.2009
Version	1.0

Table of Contents

Summary

Due to advances in wireless communication and in the miniaturisation of electronic components, sensor network technology has grown rapidly during the last few years. The development of large scale sensor networks offers economically viable monitoring solutions for a wide range of applications. Security is of extreme importance for many sensor network applications such as battlefield surveillance and security monitoring. Because security mechanisms require a significant amount of computational and storage resources, existing security mechanisms used in traditional wireless networks are not appropriate for sensor networks. Although there have been different schemes proposed to provide encryption and authentication mechanisms for sensor networks, they generally build upon the assumption regarding trustworthiness of the participating sensors. This project identifies security constraints in sensor networks and existing schemes to establish trust by doing a literature review. Furthermore, this project examines two prominent schemes in some detail with a view to providing a critique on their limitations, problems and deficiencies.

1 Project Description

1.1 Background

During the last decade, communication technology and computer technology have increased significantly due to improvements in miniaturisation. Advances in these technologies have enabled to build small electronic components that are able to sense, process and communicate information to other nodes. These so called Sensor Nodes (SN) are capable of gathering many types of information from the environment including temperature, light, humidity and vibrations. Furthermore, wireless communication makes it possible that such nodes can exchange information with either to other nodes or to the outside world without being physically connected to another device. Wireless Sensor Networks (WSN) offer economically viable monitoring solutions for a wide variety of applications and have become popular since data gathering is becoming an important component for the success of several mission critical applications. A typical scenario of where WSN can be deployed is in the battlefield where the nodes gather information in the enemy territory. This scenario becomes very interesting because SNs could be very small in size and can even be dropped off an airplane. Then the SNs use self-configuration and self-organisation techniques to establish a WSN and send the data to a base station. In other scenarios such as environment monitoring, WSNs are used to detect bushfires or tsunamis. It is easy to see the potential benefits by using WSNs. In order to collect as much data as possible within a certain area the use of a WSN offers a cheap, viable and efficient option. Additionally, using a large number of small sensors instead of using one big sensor for sensing data in a certain area is more accurate since errors in the devices or communication can be detected easily.

WSN is a relatively new and immature technology. Building WSNs poses challenges of secure routing, node authentication, data integrity, data confidentiality and access control that are faced in conventional wireless and wired networks as well. However, WSNs are very different from traditional networks since SNs are only small devices with many electronic components such as memory, CPU, radio and sensor and each of those components consumes power. SNs have a battery and can work only as long as the battery lasts. In other words, it is very important to optimize every computation in order to increase the sensor's lifetime. These constraints make it impossible to ensure efficient use of the security mechanism used in traditional networks to establish a cryptographic based approach to build a framework of trust in a sensor network environment. Thus, providing new security features with low power and resource consumption is a significant part in WSNs. Additionally, WSNs are often used for applications such as military target tracking or fault detection and diagnosis in machinery (e.g. airplane) where security is critical. In general, wireless networks are prone to security attacks since the nature of wireless communication easily allows eavesdropping and alteration of messages. It can be seen that security becomes a major concern in WSNs.

Currently several approaches to securing sensor networks exist in the literature and many security models and encryption techniques for WSNs have been proposed. These approaches generally build upon the assumption regarding trustworthiness of the participating sensors. However, very little research been done on how trust can be established within a WSN.

1.2 Aims, Significance and Expected Outcomes

This project focuses on trust management in WSN and the aim of this project is twofold. Firstly, this project demonstrates that security mechanisms used in wired networks and Ad-Hoc networks are not appropriate in WSN by providing an introduction into WSN. This general background information identifies other potential vulnerabilities that are peculiar to the WSN environment. Secondly, the project determines how trustworthy communication can be established in a clustered WSN architecture. This is done by providing a critical analysis of existing frameworks and models in this field. This project therefore consists of a literature review where the existing approaches are identified. This is an important part in this project because it is necessary to understand how these schemes work. Next, it has to be ascertained if these approaches are applicable to the clustered environment. The clustered method is the most commonly deployed architecture used in WSN. Since the architecture is relevant to the trust management this project should also explain how the clustered architecture works. The issue of routing is also relevant for a trustworthy communication. This project examines the most common routing protocols implemented in WSNs by demonstrating their functionalities to support trust.

There are many reasons for doing this project. First of all, the range where WSNs can be used has grown rapidly during the last years. As mentioned above WSNs are often used where security is critical (e.g. enemy tracking in battlefield environments and habitat monitoring in the nature preserves). This poses challenges of secure routing, node authentication, data integrity, data confidentiality and access control. Even though, in some situations, the

security requirements in WSNs may be similar to those that are there in wired networks and wireless networks; however, the applicable security solutions are different due to the specific characteristics of the devices. As a result, a number of new security mechanisms based on cryptography and authentication have been developed. Nonetheless, these mechanisms alone are not sufficient for the unique threats and novel misbehaviours encountered in WSNs. Dealing with issues such as these require that the sensors themselves are trustworthy. Different schemes to build trust in WSN have been proposed. Some schemes use probability theory, some use formal methods and logic, some use statistical weighting techniques while others use Bayesian techniques. However, not all of those proposals are applicable in a clustered architecture and they may have different limitations and constraints.
The intended outcome of this project is a report on trustworthiness in sensor networks. To be more precise, it contains general information about sensors, sensor networks and trust management as well as information about specific security challenges in WSN. This information helps to identify constraints that are peculiar only to sensor networks and highlights critical issues in the provisioning of trustworthy sensors. Moreover, the report briefly describes existing trust models used in sensor networks. Because many schemes are very complex and require a background in sensor techniques and mathematics as well, this paper focuses on the general principles that govern these schemes. A comparison between prominent models of trust in clustered environment with a critique will be provided. In fact, based on the outcome of this critical analysis, I will aim to provide some recommendations that will help researchers to build more coherent and complete trust framework in the future.

2 Research Methodology and Plan

2.1 Approach

The objective of this project is to study the problem of trust in sensor networks. Although this project combines the two related fields network communication and network security, I have to do a lot of literature research. Due to the specific characteristics, WSNs are very different from conventional networks and the applicable security solutions are unique when compared to other related technologies such as Mobile Ad Hoc Networks (MANETs) and mobile networks. These issues make it impossible to adopt existing schemes to secure these networks. In a first stage, I intend to collect reading material from different sources. As mentioned earlier, research has already been done in this field and several approaches have been proposed. Many proposals and papers about security issues related to WSNs are published by the Institute of Electrical and Electronics Engineers (IEEE) association. The trust models used in my project will be based on those proposals because IEEE is a well known and trusted organisation in the field of engineering, computing and information technology. Furthermore, IEEE is in charge of the 802.11 wireless standards. General explanations about sensors and sensor networks are stated in Mahgoub 2006 and De Morais Cordeiro 2006.

The second stage of the project concerns the data processing. Here, I intend to use the knowledge that I had acquired in the first stage to build a general understanding in WSNs.

This stage also includes also the literature review in which the collected material about existing trust schemes is compared and analysed. In order to fulfil the project aims, I need to choose two existing trust schemes which are applicable for the clustered architecture.

I will examine and critically analyse those two approaches in more detail. To be more precise, I will identify the requirements and constraints of both schemes. After that, I expect to combine my already existing knowledge in security and networking with the outcome of the analysis. This helps me to identify the constraints and will lead me to my recommendations.

2.2 Task Plan

This section lays out the sequences of steps that are involved in this project. Each of the following tasks is defined by an activity with an explicit outcome. This task plan corresponds to the project plan that can be found in the appendix. Since this project is an analysis project, it requires a lot of reading, thinking and writing. From my own experience, I can state that reading as well as writing for an analysis requires much more time than for a development project. This was taken into account when the task plan was created.

Task 1: Gain general understanding of Wireless Sensor Networks – 20 hours
Since WSN is an unfamiliar topic to me, I first of all have to understand how it works. This task involves the reading and understanding of chapters one and two in Mahgoub 2006 and chapter nine in De Morais 2006. This understanding is necessary for two reasons. First, it helps to examine the significance and the aim of the project. Second, the gained knowledge is used to determine the project scope. This task is completed by the end of week 3 by writing the project proposal.

Task 2: Identify architectures, security challenges and routing protocols – 40 hours
In order to identify the constraints and security challenges in WSNs it is important to understand the architectures and routing protocols that are used in WSN. In Qiangfeng 2004 routing protocols for WSNs are proposed and chapter eight in Mahgoub 2006 explains the different architectures. Although the mentioned literature contains the information about architectures and routing protocols, it may not contain specific security challenges. Thus, this task includes also research in other resources. By writing the introduction for the project paper this task is finished by the end of week 7.

Task 3: Understand existing models of trust in WSN- 30 hours
After having a deeper understanding on WSNs, I will focus on trust establishment and trust management in WSNs. First, I identify and understand existing schemes and then I do a literature review. As this project focuses on the clustered architecture only, I will choose two schemes that are applicable to this architecture. This task should be finished in week 10 when the literature review is done and the two schemes for doing the critical analysis are chosen.

Task 4: Critical analysis of existing models – 20 hours
The aim of this task is a critical analysis on the two chosen schemes that helps to provide a critique on their limitations, problems and deficiencies. Therefore, I will examine the two trust schemes in more detail and demonstrate how they work in a clustered architecture. The

outcome of this task is a significant part for the project paper and should be done by the end of week 12.

Task 5: Provide some recommendations – 10 hours
Finally, after understanding the concept of trustworthy communication and having identified the requirements and constraints, I will give my own recommendations. This includes a recommendation about where services that support trustworthy sensor communications must be located. Additionally, this task shows where further studies in this field are to be done. This task is completed by writing the conclusion part in the project report (week 13).

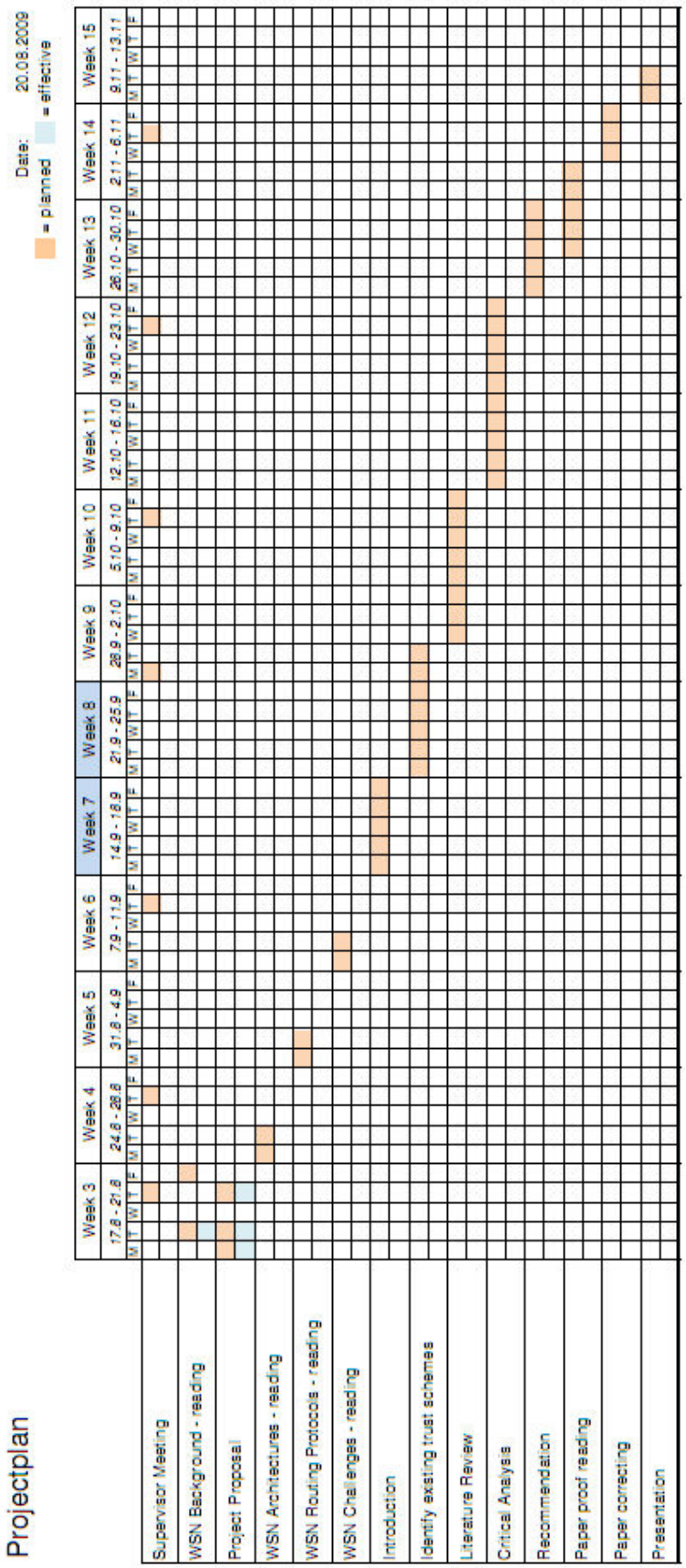
3 Bibliography

De Morais Cordeiro, C 2006, 'Ad Hoc & sensor networks: theory and applications', World Scientific Publishing Co, Hackensack, New Jersey.

Mahgoub, M and Ilyas, M 2006, 'Smart Dust: Sensor Network Applications, Architecture, and Design', Taylor & Francis, Boca Raton, Florida.

Qiangfeng, J 2004, 'Routing Protocols for Sensor Networks', IEEE Communications Magazine.

Appendix


Projectplan
Date: 20.08.2009
= planned
= effective
Week 3
17.8 - 21.8
Week 4
24.8 - 28.8
Week 5
31.8 - 4.9
Week 6
7.9 - 11.9
Week 7
14.9 - 18.9
Week 8
21.9 - 25.9
Week 9
28.9 - 2.10
Week 10
5.10 - 9.10
Week 11
12.10 - 16.10
Week 12
19.10 - 23.10
Week 13
26.10 - 30.10
Week 14
2.11 - 6.11
Week 15
9.11 - 13.11
Supervisor Meeting
WSN Background - reading
Project Proposal
WSN Architectures - reading
WSN Routing Protocols - reading
WSN Challenges - reading
Introduction
Identify existing trust schemas
Literature Review
Critical Analysis
Recommendation
Paper proof reading
Paper correcting
Presentation