Research of Trusted Network Architecture in Wireless sensor Networks

Xu Wu

Department of Computer Science, Xi’an University of Posts and Telecommunications, Xi’an, China, xrdz2005@163.com
doi: 10.4156/jcit.vol6.issue7.31

Abstract

Recently, there are many trust management solutions are proposed for wireless sensor networks. Current decentralized trust-management research focuses mainly on trust models and algorithms, whereas trust evaluation isn’t related with certainty specific application. But, in WSNs the trust management solutions should adapt to different application scenarios. In addition, potential merits of hardware-based security mechanisms to further secure application exposure have not been considered so far. Fundamentally, the secure interaction among nodes also requires to be guaranteed by hardware-based security mechanisms besides software-based ones in WSNs. This paper presents a new trust management solution towards establishing a security interacting environment for wireless sensor networks. In the solution, a trusted architecture is proposed, which is used to deal with the trust and security problem for wireless sensor networks. The proposed architecture for developers can be utilized as a foundation for their own secure wireless applications. This unique feature of the proposed architecture is that it combines software resource level security features offered by trust module and rule-engine module, with the hardware-based security mechanisms offered by Trusted Computing Platform (TCP). TCP is a platform which can be trusted by local and remote entities. TCP builds its promise of a trusted platform on the basis of some hardware – the Trusted Platform Module (TPM).

Based on analysis, we conclude that the architecture is a promising solution that can overcome many security challenges in wireless sensor networks, thus realize secure interaction among mobile sensor nodes.

Keywords: Wireless Sensor Networks, Trust, Security

1. Introduction

Wireless sensor networks (WSNs), in general, consist of a large number of inexpensive wireless devices (sensor nodes) densely distributed over the region of interest. Sensor nodes have wireless connectivity and can be tied to a backbone network such as the Internet [1]. Recently, WSNs have been used in various applications such as monitoring, disaster recovery, smart home and many others. These sensor networks are often deployed in physical environments that change overtime. For example, in a weather monitoring system, most nodes only collect temperature data, moisture date and wind date under normal situation. WSNs are vulnerable to various attacks due to dynamic topology and openness of wireless channels. Lack of trust between sensor nodes is one of main challenges that obstruct the wide adoption of WSNs, therefore both consumers and corporations are greatly concerned with the establishment of a trusted environment for WSNs.

Normally, in WSNs a number of sensor nodes need monitor physical or environmental conditions and cooperatively pass their data through the network to a main location, which can be vulnerable to attacks. There are a number of reasons why trust in such a wireless network environment is crucial for sensor nodes. Firstly, when a sensor node tries passing its data by another sensor node, it may worry about the virus or attack embedded in its data. Secondly, since sensor nodes are heterogeneous, some nodes might be benevolent in providing services. Some might be buggy or malicious and cannot provide services with the quality that they advertise. Thirdly, since there is no centralized node to serve as an authority to monitor and punish the nodes that behave badly, malicious nodes have an incentive to provide poor quality services for their benefit because they can get away. Finally, when users become more concerned about privacy, some of them may hesitate to use the wireless sensor services. They
will not accept a technology if personal information will be exposed without any control. A more trusted WSNs infrastructure is expected.

All of the above problems limit the applications build in the WSNs. The key reason is that we lack a secure and trusted management solution for WSNs. Some traditional security techniques, such as service providers requiring access authorization, or consumers requiring server authentication, are used as protection from known malicious nodes. However, they cannot prevent from sensor nodes providing variable-quality service, or nodes that are unknown. The decision making in a WSN is essential for carrying out certain tasks as it aids sensors establish collaborations. In order to assist this process, trust management systems could play a relevant role. Mechanisms for trust and reputation can be used to help sensor nodes distinguish good from bad partners. However, existing trust management solutions [5-6] are not fit in WSNs due to the power consumption constrains, dynamic network topology and heterogeneous characteristics of WSNS. In the paper, we present a new trust management solution based on a trusted architecture which is used to deal with the trust and security problem for WSNs. The proposed architecture is a layered one which combines software resource level security features offered by trust module and rule-engine module, with the hardware-based security mechanisms offered by Trusted Computing Platform (TCP). In WSNs, each cluster head are equipped with a rule-engine module and has a trusted architecture as shown in Figure 1. The device layer provide essential security services, such as authenticated booting, encryption service, secure storage, privacy support and digital rights management based on the technology of Trusted Computing Platform. The system layer ensures to establish a reliable trust relationship in different application scenarios and make security related decision between nodes. The different application services are supported at the service layer.

The remaining of this paper is organized as follows: Section 2 introduces the related works. In Section 3, a trusted architecture is elaborated and the architecture is analyzed in section 4. At last, we conclude the paper and point out the future works.

2. Related work

The reputation and trust systems have been proved useful mechanism to address the threat of compromised or faulted entities in sensor networks. There is some related work conducted in the literature. They operated by identifying selfish nodes and excluding these entities from the network. Most of existing work follows the research steps that, what is trust referent, what are factors or aspects related to trust, and evaluate or assess trust based on those factors and aspects and try to manage trust.

Some reputation-based frameworks based on the approach of trust management have been extensively studied in many contexts and equally diverse domains such as human social networks, e-commerce, 802.11 networks, node-to-node networks etc. A collaborative filtering recommendation algorithm based on user interest change and trust evaluation is proposed by Zhimin Chen etc [2]. The user’s trust rating is given a weight by a gradual time decrease and credit assessment in the course of user similarity measurement and then several users highly similar with active user are selected as his neighbor. Experimental results show that the algorithm can make the neighbor recognition more accurately and enhance the quality of recommendation system effectively. Qing Ding, et al. proposes a reputation framework for trust management in the P2P Grid. To validate their system, a context-related reputation function is designed to facilitate an efficient mechanism for service provider selection in this P2P Grid environment. Network simulation experiments show that significant performance gains can be gotten using this framework [3]. A study conducted by Kim and Seo [4] proposes a trust model using fuzzy logic based on the data exchange among nodes. The paper focused on the trustworthy of sensor node which participating the wireless network. If the sensor node has high trust value, other node can trust the sensor node and sending and receiving a data safely with it. The trust model is very much similar to collecting trust votes and establishing reputation of nodes in the network. The reputation is then used to determine the degree of trust.
DRBTS [5] is a special case to build a distributed model in location-beacon sensor networks using both first-hand and second-hand information. But the trust building in this kind of WSNs depends on a distributed trust management model, not on a Trusted Computing Platform.

Haiguang Chen proposes a task-based trust management solution for WSNs [6]. In this paper, the scheme is distributed and the sensor node builds trust rating by their own observation in different task. But, their scheme is more suitable for trust system in WSNs due to its trust system build on different task.

Jianguo Chen and Stefan D. Bruda propose an efficient trust model based on the incremental Proportional-Integral-Derivative (PID) controller and the efficiency of our model is O(1) that uses only four data and needs four multiplications, four additions and two subtractions. Besides, this paper reviews some trust models and discusses the robust effects for some important issues such as consistent node behavior, sudden fluctuations in node behavior and unintentional errors [7].

Ganeriwal et al. [8] make a trust evaluation model and uncertainty analysis based on Bayes theory. Because the lack of prior knowledge about wireless sensor networks, the model’s subjective assumptions of prior distribution aggravates the uncertainty of trust. These two models both regard the subject fuzziness of trust as the randomness and use pure probability statistic method to assess trustworthiness, which is difficult to obtain prior knowledge from practical application and inevitably result in something unreasonable. Song et al. [9] add trust component to the LEACH algorithm, where nodes select the highest trust value one from their neighbors as cluster head. Although the distributed algorithm in this scheme has high convergent speed, reputation-based trust management may be vulnerable to collusion attacking.

In summary, the proposed solution does borrow some design features from several existing works in literature but as a complete system differs from all the existing solutions. Existing work only provides software resource level security schemes, but potential merits of environment-based security mechanisms to further secure application exposure have not been considered so far. In our solution the device layer provides essential security services, such as authenticated booting, encryption service, secure storage, privacy support and digital rights management based on the technology of Trusted Computing Platform. The system layer ensures to establish a reliable trust relationship and make security related decision between nodes, so the risks raised by malicious nodes is reduced. This is more feasible in practice, especially in mobile domains because managing heterogeneous hardware and software components with dynamic capability is a challenge in the mobile sensor scenarios.

3. Trusted architecture

To guard against malicious nodes, wireless sensor applications must incorporate suitable trust mechanisms. Current decentralized trust-management research focuses mainly on producing trust models and algorithms, but few consider the relationship of trust evaluation and application requirement changes. In addition, potential merits of hardware-based security mechanisms to further secure application exposure have not been considered so far. In the paper we present a new trust management solution based on a trusted architecture which is used to deal with the trust and security problem for WSNs.

The proposed architecture combines software resource level security features offered by trust module and rule-engine module, with the hardware-based security mechanisms offered by Trusted Computing Platform. In WSNs, each node device is TCP compatible and has such a secure architecture as shown in Figure 1. The trusted architecture is elaborated in the section. There are three layers in this architecture which includes the device layer, the system layer and the service layer.
3.1. Device layer

The mobile P2P device layer contains Trusted Computing Platform (TCP) components. These components ensure the OS of mobile node is implemented in a trusted fashion. Trusted computing platform (TCP) is a platform which can be trusted by local and remote entities. Trusted Computing Group is an industry standardization body to develop standards for Trusted Computing Platforms. TCG aims to enhance the overall security, privacy and trustworthiness of a variety of computing devices. TCG's Trusted Computing Platform (TCP) builds its promise of a trusted platform on the basis of some hardware – the Trusted Platform Module (TPM). TPM is the root of trust. It is designed and manufactured in specific way such that all other remote parties trust some cryptographic computing results from this TPM.

A trusted computing platform implements many security related features based on TPM, for example secure boot, privacy support, sealed storage, software integrity attestation, etc. Every time the computer is reset, the TPM steps in, checks itself and then verifies the OS loader before letting boot-up continue. The OS loader is assumed to verify the operating system (OS), the operating system is assumed to verify every bit of software that it can find in the computer, and so on. Figure 2 illustrates the process of authenticated booting and trust challenge on remote platform or data. A TPM chip is responsible to examine the OS loader. Once it is proven safe, then OS kernel is examined.

In short, the TPM certifies an OS version, and then the OS can check the applications’ precise configuration. If they aren’t executed in trusted states, these applications should be stopped working.

![Figure 1. Trusted architecture of mobile P2P node device](image1)

![Figure 2. Authenticated booting and trust challenge](image2)
3.2. System layer

The system layer represents the bulk of trusted architecture. It contains the core functionality for providing a secure mobile framework, on which applications can then be built. The system layer has been broken down into a modular structure. The use of a modular approach provides expandability for the system layer. New modules can be added at a later date. Interaction manager is responsible for various interactions (e.g., sensor nodes joining and leaving). Device information lookup module allows the application to discover information about the device it is running on (e.g., resources, geographical location, etc). When used in conjunction with the trust evaluation module, this could be extended to discovering information about other devices within the node group. Obviously what information is made available will be dependent on the security settings of the device.

The rule-engine module takes responsibility of the awareness of the varieties of application and notify trust evaluation module. Reconfiguration of trust evaluation is triggered by the changes of application requirements and is performed by transitioning to a new evaluation configuration. A cluster head can be equipped with a rule-engine module. It is composed of three components: conversion component, sample value base and reconfiguration trigger. During a monitoring system initialization, the regular sample values of environmental changes are deployed in rule-engines. When a cluster head is aware to a requirement change of its member nodes, it dynamically makes a trust evaluation reconfiguration decision following sample values of environmental data in a rule-engine. For instance data fusion process, should some selfish nodes need to be indentified adaptively? The requirement information is converted to logic expressions by a conversion component in a rule-engine. The rule-engine analyzes the logic expressions, and matches them with sample values of requirement change, and then determines whether trust evaluation reconfiguration or not. If yes, it will send message to trust evaluation module. The rule-engines are used to guide the evaluation reconfiguration decision-making process to adapt to new application requirement. The rule-engine module is described in figure 3.

Sample value base stores sample values of environmental change defined by system. Sample values express the relationship between requirement change and corresponding applications. We denote sample value as the following formula: \( (C_1, C_2, C_3, \ldots, C_n) \rightarrow A \), where

1) \( C \) is a logic expression, which represents change of certain application parameter. 2) \( A \) is an application requirement, which denotes an application requirement in certain current application condition.

![Figure 3. The rule-engine module](image)

Utilizing the sample value and the requirement data from sensor nodes, rule-engine can make a reconfiguration decision-making, and send the reconfiguration request to trust evaluation module to adapt to new situation. If requirement data cannot match with sample values in a rule-engine, the cluster head will send them to other cluster head. If no any result, it will send
them to user, then user will decide whether reconfiguration or not. If yes, the new evaluation configuration is uploaded to trust evaluation module by user. The reconfiguration is triggered, and the cluster head will add the record of requirement change into sample value base. Trust evaluation module is applied to evaluate trust relationship between mobile nodes, before any security related decision is made. It is needed to identify trustworthiness of mobile nodes in order to distinguish between malicious nodes and innocuous nodes, and to strengthen reliable nodes and weaken suspicious nodes. Risk is one of the important factors that affect the decision making process. The trust evaluation module may receive the messages of application requirement changes from rule-engine module and adaptively adjust the trust evaluation process. In the module we use a power node-based reputation scheme proposed by us [10]. We classify sensor nodes into two groups, power nodes (cluster heads) and member nodes. The purpose of maintaining power nodes is to manage their member nodes that are connected to their power node and allow the power node to have their reputation information.

Trust decision module analyses the relationship of trust and risk and makes an interaction decision. In fact, higher risk brings lower success rate of interaction. The interaction manager deals with different sensor node interactions and cooperates with Trust decision module. The main idea is that we use utility function to express the relationship between benefits and costs as perceived by each sensor node by being connected to the WSNs and particular events that occur within the WSNs, and then make the interaction decision based on expected utility as well as risk attitude. Similarly, a rational attacker would not find it beneficial to attack the node if its MaliciousBenefit for the attack was less than what it expects based on the relationships between benefits and costs. Moreover if the malicious node knows that the decision mechanism is being used, then it will have to probabilistically increase its benign service in order to not be discovered, which increases resource availability in the system and benefiting all benign nodes.

3.3. Service layer

Service layer contains components for application services. All the components in service layer are certified by the device layer. Any distrust behavior could be found and turned down by the device layer. Taking resource sharing as an example, this layer should contain components like resource-find module, resource-provide module and resource-download module. The resource-find module is responsible for finding demanded resources in WSNs. The resource-provide module provides shared resources according to their copyright and usage rights. The provided resources could be encrypted through the TCP. The resource-download manager handles remote resource accessing and downloading. If the resources are examined without potential risk, they will be stored at the node.

4. Analysis of architecture

The trust between mobile nodes is deal with by the proposed trusted architecture. Each mobile node can evaluate whether another mobile node is running in its expected status. The process is shown in figure 3 (step1-4). This is done through digitally certificating the device configuration. The OS’ executing environment is ensured by the TPM. The OS then can estimate the configuration of application. The configuration information of application is contained in a certificate signed by a private key. It is only known by the system. In order to confirm the configuration information of node’s OS, the system will verify the validity of the certificate by generating the value of random challenge. The proposed trusted architecture can ensure the node to work in a trustworthy way through the TCP technology.

A mobile node can guarantee the trusted status based on predefined conditions in the step 5-6. The conditions are approved by two interacting nodes when trust is established between them. The secure hardware chip is used to build the TCP components. The hardware chip has higher security than software. In the step 7 any distrust behavior of the other node is automatically notified to the mobile node based the predefined conditions. Therefore, the mobile node can deal with any changes that may affect the trust. In system layer based on the trust evaluation
mechanisms embedded in the trust evaluation module, each node can anticipate potential risks and make the best decision on any security related issues in the wireless communications. The trust evaluation results can help generating feasible conditions for sustaining the trust relationship. The risk raised by malicious nodes could be greatly reduced based on the trust evaluation mechanism. The evaluation is conducted based on past experience and other nodes’ recommendations, as well as risk analysis. In particular, the TCP components in the proposed architecture provide a secure running environment and further ensure the integrity of this environment for the trust evaluation. Therefore the trust evaluation is conducted in the expected trust environment, thus the evaluation results are generated through correct processing. This mechanism is very helpful in fighting against attacks raised by internal malicious nodes that hold a correct platform certificate and valid data for trusted platform attestation. With the TCP components in the architecture, any device component in service layer can only execute as expected and process resources in the expected way. Furthermore, with the support of trust evaluation, the nodes could interact in the most trusted way.

![Figure 4. Trusted interactions in WSNs](image)

5. Implement and development

The previous sections have provided an overview of the trusted architecture. Our work has provided some detailed design of the architecture. In order to deploy the architecture, the node device is required TCP compatible. When it is deployed in the mobile devices of WSNs, it can help the devices to interact in a secure fashion through the components and mechanisms provided by the architecture.

The architecture is to be implemented to work with Linux platform and will be evaluated based mobile devices. That being said, the architecture is implemented in a platform independent manner and can be applied to other platforms in the future. Where possible, existing technologies and developments will be utilized, with the mobile version of JXTA being used as a basis for wireless communication. Linux also provides a powerful set of security features and these will be exploited by the architecture. Therefore the architecture can be
Research of Trusted Network Architecture in Wireless sensor Networks
Xu Wu
Journal of Convergence Information Technology, Volume 6, Number 7, July 2011

flexibly integrated into any distributed system, such as Pervasive computing system. It can provide secure interaction environment for dynamically decentralized systems. For application developer with different intents, they may install different components into the service layer. The architecture is a component-based one which provides trustworthy mechanisms to support mobile application. As we have already mentioned, the intention is for developers to utilize the architecture as a foundation for their own secure applications of WSNs.

6. Conclusion and future work

Wireless sensor networks (WSNs), in general, consist of a large number of inexpensive wireless devices (sensor nodes) densely distributed over the region of interest. Existing trust management solutions are not fit in WSNs due to the dynamic and heterogeneous characteristics of a mobile system. This paper presents a new trust management solution based on a trusted architecture towards establishing a security mobile environment for WSNs. The proposed architecture for developers can be utilized as a foundation for their own secure applications of WSNs. The proposed architecture can be flexibly integrated into any distributed system, such as Pervasive computing system. In the future work, the core aspects of the architecture will be implemented in a platform independent manner allowing for their transference to other platforms.

7. Acknowledgements

The work in this paper has been supported by Scientific Research Program Funded by Natural Science Basis Research Plan in Shaanxi Province of China (Program No.2011JQ8006) and Shanxi Provincial Education Department (Program No.11JK1060).

8. References