SEC-SNMP: POLICY-BASED SECURITY MANAGEMENT FOR SENSOR NETWORKS

Qinghua Wang and Tingting Zhang
Department of Information Technology and Media, Mid Sweden University, Sundsvall, Sweden

Keywords: Security management, security policy, sensor network.

Abstract: In this paper, we present a sensor network security management framework called Sec-SNMP, which organizes and manages security related behaviors in sensor networks based on security policies. There are three main components in Sec-SNMP: Sec-SNMP manager, Sec-SNMP agent and a policy control and deployment protocol. Sec-SNMP manager provides the interface between human administrator and the managed mesh network. Sec-SNMP agent represents Sec-SNMP manager to enforce security policies within the managed mesh network. The policy control and deployment protocol allows the communication between Sec-SNMP manager and Sec-SNMP agents. The security management for sensor networks is still in its germinal stage, and this paper provides a good guideline for future research.

1 INTRODUCTION

Sensor networks deployed in human-unattended enviroments for critical applications suffer from a magnificent number of threats. Countermeasures including key management, authentication, intrusion detection, intrusion/fault tolerance, privacy protection, etc., have been proposed for conquering sensor network threats. Unfortunately, these countermeasures are so diversified and there is no easy in incorporating all these countermeasures in one network. To provide the possibility of coorporatively exploiting the benefits of different kinds of security measures, efficient security management must be implemented. However, security management as the mostly used way for security situation to be awared and security operations to be executed is left among those few untacted areas in sensor network related research.

In this paper, we present a policy-based sensor network security management framework called Sec-SNMP. With this security management framework, the administrator can monitor the dynamic security situation of the sensor network, and then update the security configuration according to the changed security situation.

In the remainder of this paper, we firstly elaborate the proposed policy-based sensor network security management framework Sec-SNMP by seperately introducing its architecture, three main components (Sec-SNMP manager, Sec-SNMP agent, and Policy Control and Deployment Protocol) and the flow of security policy enforcement. After that, we summarize some nice features of the proposed Sec-SNMP framework in Section 3. A short introduction of the related work is given in Section 4. The conclusion is finally given in Section 5.

2 POLICY-BASED SENSOR NETWORK SECURITY MANAGEMENT FRAMEWORK (SEC-SNMP)

In this section, we propose a security management framework called Sec-SNMP, which organizes and manages security related behaviors in WSNs based on security policies. As for security policy, it is a high level definition of what it means to be secure for a system. In Sec-SNMP, the top security policy is that the managed sensor network should fulfill security requirements including Availability, Authentication, Confidentiality, Integrity, Non-repudation, Freshness, and Survivability. When it comes to implementation in Sec-SNMP, this top security policy is divided into many policy items which concretely specify security operations when some pre-defined security situation appears.

Wang Q. and Zhang T. (2008).
SEC-SNMP: POLICY-BASED SECURITY MANAGEMENT FOR SENSOR NETWORKS.
In *Proceedings of the International Conference on Security and Cryptography*, pages 222-226
DOI: 10.5220/0001928602220226

2.1 Architecture

Figure 1 shows the Sec-SNMP architecture. The considered sensor network system consists of two parts: infrastructure servers and mesh network. Infrastructure servers provide remote data acquisition and query service, strong authentication service, and network management service. Mesh network provides data collection, event detection, and authenticated in-field query service. In Sec-SNMP, the security management service is collaboratedly provided by the Sec-SNMP manager standing on the infrastructure server side and the Sec-SNMP agents distributedly installed on the sensor side.

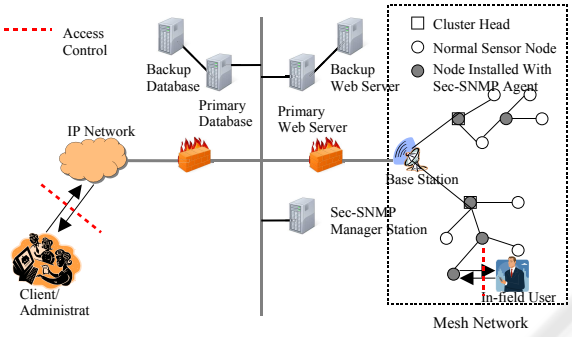

Figure 1: Sec-SNMP architecture.

2.2 Sec-SNMP Manager

The Sec-SNMP manager provides the interface between the human network administrator and the managed sensor network system. It consists of a Security Policy Base, a Security Management Information Base (Security MIB), a Security State Base, and a Security Event Processing Module.

- Security Policy Base stores all available security policy rules configured by the network administrator.
- Security MIB provides static security management information, including both network and network component security configuration. In a policy-based security management, a security MIB tells what object (an object can be a node component, a group of node components, a node, or a group of nodes) is imposed with what kind of security policy.
- Security State Base keeps the up-to-date network and component dynamic states and the states are stored according to sensor network security models. Examples of sensor network security models include network topology map, network connectivity map, network routing path map, and network behavioral history, etc. The Security State Base is dynamically updated according to the alerts and query results coming from Sec-SNMP agents, and it provides necessary information when the administrator decides to update network security configuration.
- Security Event Processing Module consists of key managemnet engine, authentication engine, intrusion detection engine, fault detection engine, etc. It is responsible for security event detecting, identification, and processing. It also provides the input for security policy matching and enforcement.

The Sec-SNMP manager runs an application that provides an interface for the administrator to edit the Security MIB and the Security Policy Base. It also runs a Policy Control and Deployment Protocol for its communication with Sec-SNMP agents.

2.3 Sec-SNMP Agent

The Sec-SNMP agent is a piece of software located in the managed device and provides the interface between the Sec-SNMP manager and the physical devices or software applications being managed. Each Sec-SNMP agent is a mini Sec-SNMP manager, and is responsible for accepting the security policy configuration from the Sec-SNMP manager, for enforcing configured local security policies, and for reporting local security states to the Sec-SNMP manager. To fulfill these functions, it needs to keep a local Security MIB, a local Security Policy Base, a local Security State Base, and a local Security Event Processing Module.

As for the implementation of Sec-SNMP agent, we use the way that Almajali and Elrad proposed in their Remote Dynamic Policy Deployment Framework (RDPD) (Almajali and Elrad, 2006). Simply speaking, Sec-SNMP agent is run as an agent service application on the host sensor node, and the agent application relies on a underlying filter driver called Network Driver Component to control the traffic that flows in and out through sensors. Sec-SNMP agent stays in contact with Sec-SNMP manager using the Policy Control and Deployment Protocol. Sec-SNMP agent communicates with the Network Driver Component in order to enforce the policies configured by Sec-SNMP manager.

2.4 Policy Control and Deployment Protocol

The Policy Control and Deployment Protocol (PCDP) allows the different components (Sec-SNMP manager

and Sec-SNMP agents) to communicate with each other and perform their various functions. The PCDP protocol used in Sec-SNMP framework is a revised version of a cognominal protocol proposed in ref. (Almajali and Elrad, 2006), where Almajali and Elrad define the following message types that can be implemented in the PCDP protocol:

- New network policy deployment request
- Check for new policies deployment/ undeployment request
- Check for new policies deployment/ undeployment reply
- Policy request
- Policy reply
- Network policy deactivation request

We enlarge this message group to make it fit for security management by adding the following message types:

- *MIB update*. In Sec-SNMP, the security configuration is organized by MIB. Sec-SNMP manager needs to update the local MIB information on the place of each Sec-SNMP agent when there is updated security strategy.
- *Security state query*. Global security state at the place of Sec-SNMP manager is regularly updated by sending a security state query message to every Sec-SNMP agents distributed in the mesh network.
- *Security state reply*. Sec-SNMP agents check the local security state and reply this message to Sec-SNMP manager on receiving a security state query message.
- *Security state alert*. This message is sent from Sec-SNMP agents to Sec-SNMP manager when there is some emergent security state change.

2.5 Security Policy Enforcement

In Sec-SNMP, an individual security policy item tells what kind of operation needs to be executed when a corresponding security event happens. Examples of defined security events include: authentication failed/succeeded, node failure detected, malicious node detected, etc. Examples of adoptable operations include: sending alert to manager, accouting, re-establishing routing, going to sleep, droping packets, etc.

Security policies must be enforced after their configuration. Figure 2 shows the flow of policy enforcement. When a general event (e.g. sensing event, radio event, time event, etc.) is captured by the system, it is firstly forwarded to the Security Event Processing Module for security analysis. The Security Event Processing Module consists of key management engine, authentication engine, intrusion detection engine, fault detection engine, etc. Thus, it has the ability to translate a general input event into a predefined security event. The identified security event is further forwarded to the policy matching engine for the extracting of the applicable policy on the applicable object. Finally, the extracted applicable policy is enforced by the system according to the operation defined in this policy.

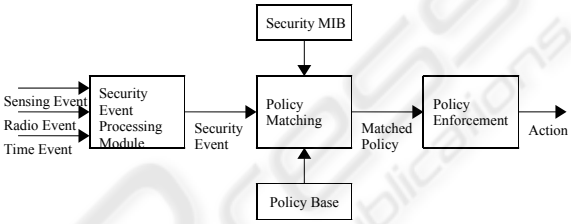

Figure 2: Security policy enforcement.

3 DESIGN FEATURES OF SEC-SNMP

Sec-SNMP is designed to provide convenient security management service for resource-constrained sensor networks. It possesses the following nice features:

- *Energy efficiency* The main computation, communication and storage tasks related to security management are put on the infrastructure server side. The concept of agent allows most of security related events to be processed locally. The main communication overheads in Sec-SNMP are security configuration updates and the on-demand local security state reports, which shouldn't happen too often.
- *Compatibility* The three main components (Sec-SNMP manager, Sec-SNMP agent, Policy Control and Deployment Protocol) in Sec-SNMP framework can also be used in other network management services, such as fault management, power management, etc. Besides, the concepts of Security MIB, Security Policy Base and Security State Base can also be generalized for the use in a general purpose policy-based network management structure.
- *Seamless Integration* Independently implementing different available security mechanisms in sensor networks can cause unnecessary overheads, and possibly even a mess. Sec-SNMP organizes available security mechanisms according

to their mutual dependency relations, and makes them act under the common defined security policies. Thus, the security related information can be presented to the security administrator by a single interface.

- *Local Response & Global Awareness* Sec-SNMP agents respond to security events locally and in time, while collaborations among these distributed agents are still possible through Sec-SNMP manager, which can be accessed by all agents and is globally situation aware.

4 RELATED WORK

Louis Lee *et al.* (Lee *et al.*, 2006) propose an adaptive policy-based management system for sensor networks, called Wireless Sensor Network Management System (WinMS). The end user predefines management parameter thresholds on sensor nodes that are used as event triggers, and specifies management tasks to be executed when the events occur. WinMS uses its underlying MAC and routing protocol FlexiMAC, which is a TDMA-based protocol that provides synchronized communication, to support resource (time slots) transfer from the rest of the network to areas where important sensing events are detected. MANNA (a Management Architecture for Wireless Sensor Networks) (Ruiz *et al.*, 2003), is another policy-based management system that collects dynamic management information, maps this into WSN models, and executes management functions and services based on WSN models. WSN models maintain the information about the state of the network. MANNA defines the relationship among WSN models in a Management Information Base (MIB). It has been shown (Ruiz *et al.*, 2004) that fault management aiming to detect failures in WSNs can be easily performed by analyzing WSN models within the architecture of MANNA. Unfortunately, both WinMS and MANNA are proposed for general network management, and the solution of security management cannot be provided by WinMS and MANNA in a straight-forward way. However, we found that Sec-SNMP has a good compatibility with them, thus Sec-SNMP can be integrated into the existing network mangement frameworks for security management purpose.

Coming to the research attempts in the special area of security management, ref. (Misic *et al.*, 2007) addresses the networking and security architecture of a healthcare information system which includes a wireless hop. This hop includes wireless sensor networks and, possibly, wireless local area or mesh networks to connect to the main wired hospital network. The authors discuss confidentiality and integrity policies for clinical information systems and propose the feasible enforcement mechanisms over the wireless hop. They also compare two candidate MAC technologies, IEEE 802.15.4 and IEEE 802.15.1, from the aspect of resilience to jamming and denial-of-service attacks. Compared to Sec-SNMP proposed in this paper, the solution proposed in (Misic *et al.*, 2007) is too specialized and not appropriate for the security management of a general purpose wireless sensor network.

5 CONCLUSIONS AND FUTURE WORK

Security management is the process of managing, monitoring, and controlling the security related behaviors of a network, and it plays a vital important role in network management. Currently, a few attentions have been paid on general network management for sensor networks, with fewer papers specifically discussing security management. This paper presents a policy-based sensor network security management framework called Sec-SNMP, which specifies the necessary important components and functionalities in a sensor network security management system. To the best knowledge of the authors, this paper is within the earliest works in the important sensor network security management area.

Although the framework of sensor network security management has been presented in this paper, there exist open problems to implement it. One challenge is to make clear the dependency relations among different proposed security technologies and design appropriate interfaces among them. Another challenge could be the development of expressive languages or metadata for representing management policies and for representing the MIBs that can be understood by the security agent application, the security manager application, and the security administrator.

REFERENCES

Almajali, S., Elrad, T., 2006. Remote dynamic policy deployment for sensor networks using application transparent approach. In *OOPSLA '06, Workshop on Building Software for Sensor Networks.*

Lee, W.L., Datta, A., Cardell-Oliver, R., 2006. WinMS: wireless sensor network-management system, an adaptive policy-based management for wireless sen-

sor networks. In *Technical Report UWA-CSSE-06-001*. The University of Western Australia.

Misic, J., Misic, V.B., 2007. Implementation of security policy for clinical information systems over wireless sensor networks. In *Ad Hoc Networks*. Elsevier, 5(1), pp. 134-144.

Ruiz, L.B., Nogueira, J.M. and Loureiro, A.A.F., 2003. MANNA: a management architecture for wireless sensor networks. In *IEEE Communications Magazine*. 41(2), pp. 116-125.

Ruiz, L.B., Siqueira, I.G., etc., 2004. Fault management in event-driven wireless sensor networks. In *MSWiM'04, 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. ACM Press.