A Hybrid Threat Detection and Security Adaptation System for Industrial Wireless Sensor Networks

Mohammed Bahria, Alexis Olivereau, Aymen Boudguiga

A Hybrid Threat Detection & Security Adaptation System for Industrial Wireless Sensor Networks

Mohammed Bahria, Alexis Olivereau, Aymen Boudguiga

CEA, LIST, Communicating Systems Laboratory, Gif-sur-Yvette - France
{mohammed.bahria, alexis.olivereau, aymen.boudguiga}@cea.fr

Abstract. Wireless Sensor Networks (WSNs) led the way to new forms of communications, which extend today the Internet paradigm to unforeseen boundaries. The legacy industry, however, is slower to adopt this technology, mainly for security reasons. Self-managed security systems allowing a quicker detection of and better resilience to attacks, may counterbalance this reluctance. We propose in this paper a hybrid threat detection and security adaptation system, designed to run on top of industrial WSNs. We explain why this system is suitable for architectures mainly composed of constrained or sleeping devices, while being able to achieve a fair level of autonomous security.

Keywords: Threat detection, sensor network, security adaptation.

1 INTRODUCTION

The gain of maturity of WSN technologies accelerates their adoption in the industry, and this adoption is all the quicker as WSNs answer to classical needs of industrial scenarios: physical values monitoring, asset supervision and facilities surveillance are all key requirements in these scenarios, for which dedicated sensors are available. However, even though cost effective devices and energy-efficient technologies and protocols are available, the underlying security question impedes the use of WSNs in the most critical industrial scenarios. The inherent vulnerability of WSN nodes, due to their exposed location and their use of wireless communications, is such that a WSN has to mimic all security features from the legacy Internet, while also adding specific use cases and taking into account the strong shortcomings of the WSN nodes.

In this paper, we introduce a new Threat Detection (TD) system that is lightweight enough to be run on sensor nodes. We couple it with a flexible Security Adaptation (SA) system, which dynamically updates the security policies in special places in the network. We show that the use of this hybrid threat detection/reaction system greatly improves the resilience of the industrial WSN, without bringing in excessive energy consumption. The proposed solution is based on a partly centralized architecture and specifies new roles for WSN entities, in accordance with their status and capabilities.

2 PROBLEM STATEMENT

Both threat detection and security adaptation raise issues with respect to their adaptability to WSNs. Threat detection challenges the constrained nodes' limited energy resources: it involves both costly [3] passive monitoring, and heavy signature-based threat identification. Security adaptation challenges the inherent heterogeneity of a wireless sensor network: certain constrained nodes may be unable to comply with a new security policy. The sleeping/awake cycle of sensor nodes makes the operation of both security subsystems more complex, introducing desynchronization in it.

A specific factor related to the industrial scenario is the WSN real-world topology. An industrial facility is made of multiple distinct zones, such as the external perimeter, the administrative building, the workshop and the storage area. All of these zones feature different sensors and are characterized by different criticality levels. As an example, Figure 1 represents a schematized industrial network made of a production facility and an office building, both being protected by a fence. Each zone is equipped with sensors of two kinds, relevant to the concerned area.

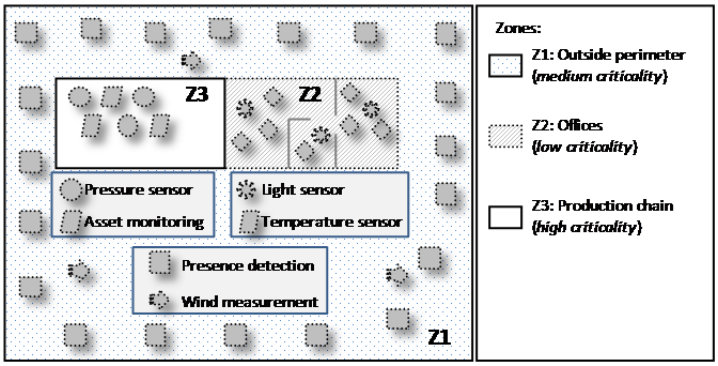

Fig. 1. Example of an industrial wireless sensor network.

3 RELATED WORK

Roman et al. [4], define a threat detection system based on monitoring agents. They distinguish between local agents (able to process only the packet they actively forward or to act as spontaneous watchdogs with a one-in-*n* probability, *n* being the number of neighbors) and global agents. Loannis et al. [5] also apply the watchdog behavior, with a higher emphasis on countering malicious monitoring nodes. Huang and Lee [6] propose an energy-efficient monitoring system. They select a single node, designated through a fair election process, to perform monitoring at a given time within a given cluster. Though, the election process is heavy for constrained nodes.

To summarize, [4] and [5] misuse the watchdog behavior while [6] uses a costly election process, leading to expensive message exchange.

Ma et al. [7] propose a Self-Adaptive Intrusion Detection System in WSN (SAID). Their approach does not take into the account the global view of the network, which may lead to incoherence. In addition, they propose to apply a new policy without checking if the nodes can handle it, which may be harmful to the network. Lacoste et al. [8] propose an approach that uses context-awareness for adaptive security. The context knowledge is combined with confidence and reputation metadata. The disadvantage of this approach is the expensive exchange of messages to maintain the coherence of the metadata. Younis et al. [9] suggest an Adaptive Security Provision (ASP), which adjusts security packet security processing based on trust and threats associated to routes. This solution is however too heavy for WSN. In addition, if a node that belongs to a route crashes, the route must be removed and new one will have to be computed. Finally, this solution is only suitable for routing security. Taddeo et al. [10] propose a method that permits the self-adaptation of security mechanisms. However, they always start with the highest security level, which could be costly for WSN nodes. Adaptive Security System (ADAPSEC) is reconfigurable security architecture for WSNs that has been developed by Shi et al. [11]. However it assumes both constant monitoring by each node and local inferring of new policies that the node should apply upon attack detection. Both would lead to high resource consumption. M.-Y. Hsieh et al. [12] base the WSN security on a trust management system. This approach delays the threat identification, though.

In addition to the identified shortcomings, neither of the previous security adaptation systems takes into consideration the sleep mode, although it is of paramount importance in WSN: a sensor node spends most of the time in sleep mode, wakes up to collect information and push it towards a sink or server, and reverts back to sleep.

4 SOLUTION DESCRIPTION

4.1 Assumptions, Components and Roles

The network is supposed to be divided into zones, each containing one or more sensor clusters. Zones and clusters have different criticalities, security levels and security policies. It is also assumed that the sensors in one cluster can communicate with each other. In addition, we assume that the awake time is negligible compared to the sleep time. Finally, we exclude any form of synchronization between nodes.

The security system we present in this paper is made up of the following elements:

- *Threat Detection Client*, which identifies threats and notifies the TD server.
- *Threat Detection Server*, which chooses which sensor(s) will be in monitoring mode for each cluster by taking into account status parameters such as batteries level and available resources, updates the global network database, receives the alarms from TD clients and transfers them to the SA Server.
- *Security Adaptation Server*, which decides upon threat identification which is the best policy to apply and stores the new policy in the security policy mailbox.

- *Security Adaptation Client*, which regularly prompts the SA Server for new policies, and either applies them or generates new affordable security policies.
- *Inference engine*, which deals with reasoning and allows for easy rule changes.
- *Security Policy mailbox*, which stores the generated policies and delivers them at nodes request. The use of this module is required since the nodes are not synchronized. It also reduces the overall bandwidth consumption.
- *Global Network Database*, which contains a global view of the network and the threats detected in the past.

4.2 Operation

A node joining the network is in **Bootstrapping** mode. The newly joining node first sends a registration request to the TD server, informing this latter about its potential monitoring abilities. The TD server then registers the node and responds with a configuration message specifying whether it should remain in normal mode or temporarily switch to monitoring mode. The decision by the TD is based on its knowledge of current and, in some cases, foreseen contexts of the candidate monitoring nodes. This contextual information includes data related to the nodes resources (e.g. battery level), locations, and capabilities (e.g. number of observables neighbours). With this information, the TD server can identify the best node in the cluster for acting as a monitoring entity, and configure it with this role for a certain period of time. Once the monitoring delay expires, the TD server designates a new cluster monitoring node.

A node switches to **Monitoring Mode** when ordered to do so by the TD server. The sequence of actions performed when in monitoring node is:

1. When the TD Client detects a threat, it sends an alarm to the TD server that includes information about the threat. This information contains at least the IP addresses of the attacker and target(s) and the type of attack.
2. Upon receiving the alarm, the TD Server reports it to the SA server, optionally after having aggregated multiple alarm messages and/or having assessed the quality of the evaluator. The SA Server then uses the inference engine to determine which policies have to be applied to counter the detected threat. Next, it stores the new policies in the security policy mailbox. Depending on the global state of the network and type of the threat, a new policy may be wide-scale or local.
3. In monitoring mode, the TD client on the sensor regularly polls the security policy mailbox by sending a dedicated inquiry message to the SA server.
4. The SA server sends the requested new policy if it exists. Otherwise it replies with a message telling the node that it is not to enforce a new policy.
5. If a new policy is received, the SA Client checks whether it can be enforced by checking the available resources and safety constraints. If it finds out that applying the policy would be too costly or would put the safety or workers/facilities at risk, it tries to find a trade off in the form of a less demanding security policy.
6. The SA client configures the security services in accordance with the received or self-determined security policy. It then sends an ACK if the received policy was applied without change, or sends a descriptor of the locally generated policy.

7. The SA Server receives the ACK or locally generated policy descriptor and updates the global network database accordingly.

The **Normal Mode** is the default mode for a bootstrapped sensor that has not been designated as a monitoring node. In this mode, the sensors alternate between active and sleeping states. Upon leaving sleeping state, the node interrogates the SA server about an eventual new policy to enforce. It then performs the task(s) for which it has left the sleeping state. An alarm may be raised by a node in Normal Mode only if one of the run tasks detects a threat and notifies the TD Client through an API call.

The overall process of our solution, depicting its state machines and internal/network message exchanges, is depicted in Figure 6.

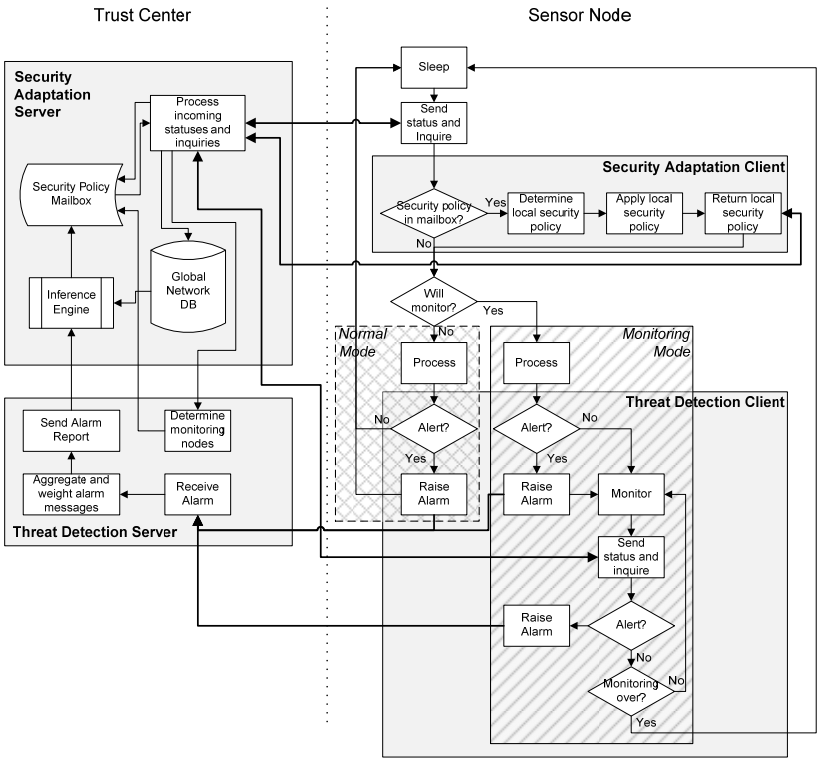

Fig. 2. Overall logical architecture and state machines.

5 Conclusion

This paper presents an adaptive autonomous security system for industrial wireless sensor networks that features both threat detection and adaptive security. Both of these subsystems involve semi-centralized processes. The switch from normal threat detection mode to monitoring mode is triggered by the threat detection server, which bases on regular reports from nodes and updates its decision accordingly. The security

adaptation system relies on server-issued policies, but the last word on how to enforce these policies remains with the sensor nodes. This system is currently being implemented for multiple industrial scenarios.

6 Acknowledgement

This work was financially supported by the EC under grant agreement FP7-ICT-258280 TWISNet project.

7 References

1. Refaei, M.T.; Vivek Srivastava; DaSilva, L.; Eltoweissy, M.; , "A reputation-based mechanism for isolating selfish nodes in ad hoc networks," Mobile and Ubiquitous Systems: Networking and Services, 2005 (MobiQuitous 2005), July 2005.
2. H. Debar, Y. Thomas, F. Cuppens, and N. Cuppens-Boulahia. Enabling automated threat response through theuse of a dynamic security policy. Journal in Computer Virology (JCV), 3, August 2007.
3. A. Wander, N. Gura, H. Eberle, V. Gupta, and S. C. Shantz, “Energy analysis of public-key cryptography for wireless sensor networks,” In Pervasive Computing and Communications, Third IEEE International Conference on, pages 324–328, 2005.
4. R. Roman, J. Zhou, and J. Lopez. “Applying intrusion detection systems to wireless sensor networks,” In Proceedings of IEEE Consumer Communications and Networking Conference (CCNC'06), pages-640-644, Las Vegas, USA, January 2006.
5. K. Ioannis et al, “Toward Intrusion Detection in Sensor Networks,” 13th European Wireless Conference, Paris, 2007.
6. Yi-an Huang, Wenke Lee, “A cooperative intrusion detection system for ad hoc networks, ” Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, October 31, 2003, Fairfax, Virginia.
7. Jianqing Ma , Shiyong Zhang , Yiping Zhong , Xiaowen Tong, SAID: a self-adaptive intrusion detection system in wireless sensor networks, Proceedings of the 7th international conference on Information security applications: PartI, August 28-30, 2006, Jeju Island, Korea
8. M. Lacoste, G. Privat, and F. Ramparany, “Evaluating confidence in context for context-aware security,”Proceedings of the 2007 European conference on Ambient intelligence, Berlin, Heidelberg: Springer-Verlag, 2007, pp. 211-229.
9. M. Younis, N. Krajewski, and O. Farrag, “Adaptive security provision for increased energy efficiency in Wireless Sensor Networks,”2009 IEEE 34th Conference on Local Computer Networks, Oct. 2009, pp. 999-1005.
10. A.V. Taddeo, L. Micconi, and A. Ferrante, “Gradual adaptation of security for sensor networks,” Proceedings of the IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, IEEE, 2010, pp. 1-9.
11. K. Shi, X. Qin, Q. Cheng, and Y. Cheng, “Designing a Reconfigurable Security Architecture for Wireless Sensor Networks,” World Congress on Software Engineering, IEEE, 2009, pp. 154-158
12. Meng-Yen Hsieh, Yueh-Min Huang, Han-Chieh Chao, Adaptive security design with malicious node detection in cluster-based sensor networks, Computer Communications, v.30 n.11-12, p.2385-2400, September, 2007.