6.1 introductionwe have previously proposed a node-level mitigation

Business, Strategy

6. 1IntroductionWe have previously proposed a node-level mitigation approach to address the DAG inconsistency attack. While we have demonstrated that the cost of this solution was reasonable, in some cases, attacks, such as the version number attack, have specic characteristics such that similar local-node methods cannot be ecient nor feasible in that context.

We therefore propose to extend our solution to these cases with a passive distributed monitoring architecture designed for security. The originality of our approach comes in particular from the fact that the architecture exploits the RPL protocol to eciently organize monitoring nodes. Node-level security strategy and distributed strategy are complementary according to network characteristics. Indeed, on one hand, the distributed strategy allows providing a global view and raising alarms to a network administrator, while, on the other hand, the node-level strategy permits to limit the impact of ongoing attacks. Thanks to this architecture, we can also handle cases where specic code, such as the node-level mitigation, cannot be deployed on nodes (no physical access, proprietary motes, no more capacity, etc.). 79 80Chapter 6. Security-oriented Distributed Monitoring ArchitectureFigure 6.

1: Typical AMI network 19. In order to preserve node resources, we exploit typical deployments of IoT infras-tructures relying on higher-order devices. This is the case for advanced measurement infrastructures (AMI) which is expected to be organized as showed in Figure 6. 1 19. This network can be divided into two tiers, i.

e., the Neighborhood Area Network (NAN) and the Wide Area Network (WAN). The NAN consists of the smart meters that are deployed at (1) residential premises, (2) commercial and industrial buildings and (3) electricity transformer and feeder points in a specic neighborhood. These smart meters typically communicate by forming an IEEE 802.

15. 4 based mesh net-work that uses IPv6 for addressing individual devices. The RPL routing protocol is likely to be used to form the routing topology in the NAN tier. The WAN tier usually consists of the utility providers head end systems where metering data is typically collected. Unlike the NAN tier, systems in the WAN tier communicate using high-speed wireless or xed-line access technologies. Field routers controlled by the utility providers, deployed on supply poles in a neighborhood, act as a bridge between the NAN and WAN tiers. These eld routers have two interfaces, one that allows it to communicate with the low-power lossy network (typically IEEE 802.

15. 4) on the NAN side and another one that provides access to the high-speed wireless or xed-line networks on the WAN side. It is also possible for these eld routers to par-ticipate in a NAN-to-NAN mesh, such that the nal interconnection of smart meters with head end systems occurs only via the low-power lossy communication channel. We therefore want to outsource monitoring and anomaly detection activities on these higher-order devices that are eld routers. These ones can be interconnected to form an independent network from the LLN network in order to share their information which constitute our monitoring architecture.

This chapter presents our monitoring architecture concepts and details detection algorithms which can be integrated in our solution to address attacks. Section 6. 2 introduces our solution, describes its main components and mechanisms based on the RPL protocol.

We then propose in Section 6. 3 to formalize the placement of 6. 2. Proposed Architecture81monitoring nodes through an optimization problem. Finally, Section 6. 4 presents algorithms deployed on monitoring nodes in order to detect DAG inconsistency and version number attacks. 6. 2Proposed ArchitectureWe propose a security-oriented distributed monitoring architecture for the Internet of Things that passively observes the network.

This one allows us to detect threats complementary to the local-node approach, for specic complex attacks which cannot be detected locally or even when dedicated code cannot be implemented on nodes. It is based on dedicated nodes and relies on the RPL protocol mechanisms to perform monitoring operations, so the target nodes do not have the charge of this activity. We describe both the main components of this architecture and the RPL-oriented features that are exploited to support it on an IoT network. (a)Monitoring nodes snooping packets transmitted by nodes in radio range. (b) Building of two RPL instances.

Figure 6. 2: Example of our passive monitoring architecture exploiting the RPL multi-instance feature. 6. 2. 1Overview and ComponentsOur monitoring architecture described in Figure 6. 2 is composed of two types of nodes participating in the network, regular nodes also called target nodes which

are monitored, plotted in white, and monitoring nodes plotted in blue. The sink plotted in green is also a monitoring node.

The regular nodes are typically lower order devices that t into the C0 or C1 class of constrained devices. Their primary function is to carry out their assigned sensing 82Chapter 6. Security-oriented Distributed Monitoring Architectureor actuation task.

They form the so called regular network. They communicate with a sink/controller, where all collected sensing data is forwarded or from where actuation commands might be periodically received. This communication occurs over low-power lossy channels and a multi-hop mesh network might be formed in order to enable interconnection between all nodes. The monitoring nodes are higher-order devices that should be at least C2 or better. As such, their monitoring activities might not have an eect upon their ability to serve their primary purpose of routing information in the regular network. These monitoring nodes are capable of passively listening to the regular nodes in their radio communication range, while also recording required information. Since the higher-order devices, instrumented as monitoring nodes, are expected to be deployed in many IoT applications, those nodes participate in the regular net-work. As such, they are able to intercept and analyze packets sent by regular nodes.

A monitoring node can only monitor its own low-power lossy network neighbo