Computer Communications 31 (2008) 4333–4342

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

A secure network management protocol for SmartGrid BPL networks: Design, implementation and experimental results

M.P. Anastasopoulos [a], A.C. Voulkidis [a], Athanasios V. Vasilakos [b,*], P.G. Cottis [a]

[a] Wireless & Satellite Communications Group, Division of Information Transmission Systems and Materials Technology, School of Electrical & Computer Engineering, National Technical University of Athens, GR15780, Greece
[b] School of Electrical & Computer Engineering, University of Western Macedonia, Kozani, Greece

ARTICLE INFO

Article history:
Available online 21 June 2008

Keywords:
SmartGrid
BPL
Pervasive computing
Network management
Security

ABSTRACT

This paper proposes a secure device management protocol mainly targeted to large-scale Broadband over Power Line (BPL) networks. In the context of the management patterns implied by the Smart Grid concept, the control protocol is based on the Intel Universal Plug and Play platform. To improve system scalability, a novel data aggregation algorithm has been proposed, while system security is ensured using a variation of the Rijndael algorithm and hosted in a custom Linux environment. Through appropriate simulations, the boundaries of the protocol performance have been investigated. The numerical results verified that the proposed network management protocol is secure, fast and may be used effectively to remotely manage a large-scale BPL network.

1. Introduction

Broadband over Power Line (BPL) technology has witnessed a significant growth during the last years as an alternative, cost effective last-mile-access technology. Standardization efforts on BPL networks have been undertaken by many national and international standards organizations and industrial fora [1]. Since BPL networks are installed on the existing power grid [2], they can easily be deployed in rural or remote areas where other wired connections do not exist, thus providing a variety of broadband communication services, including broadband Internet access, voice over IP (VoIP), remote metering, street light control, home security, home appliance, etc. [3,4,5,6]. Apart from their ability to provide high quality broadband services, BPL networks may be used to control power distribution, especially in emergency situations. The incorporation of BPL technology into the control and management of the power grid will gradually lead to the Smart Energy Grid, or simply Smart Grid [7].

Smart Energy is defined as the infusion of information technology to optimize the generation, delivery and end use of electrical power. The Smart Grid is the result of applying smart energy to get the most out of power delivery and generation in a systematic way [8,9]. The control of the currently existing power networks is expected to highly profit from the infusion of information technology as the actual control of the network will be carried out accurately and in real time. BPL technology provides smart grid with a robust communications platform offering also new services. For its operation, BPL requires the presence of a single device which functions differently depending on its intended operation and may be extended to perform other tasks. It is expected that large-scale implementation of smart grids will be based on the use of a unique BPL unit since the design of a cohesive smart grid control protocol will be significantly facilitated. Apart from cost reduction, two important advantages resulting from the above uniqueness are:

- Ease of protocol design and implementation, since, by and large, all hardware elements have the same hardware features.
- Easy and flexible implementation of hierarchical architectural schemes for the digital control network.

Thus, the proposed network management protocol requires the presence of a great number of distributed control devices which measure specific data concerning the power grid status. The interconnection of these control devices is based on a variation of the Universal Plug and Play (UPnP) protocol [10]. The selection of the UPnP device architecture provides a strong basis, which takes full advantage of the network oriented XML and HTTP technologies. However, to deal with a large number of dispersed devices forming a typical hierarchical pervasive computing system, traffic reduction is required making the use of information aggregation

* Corresponding author. Tel.: +30 6977449705.
E-mail addresses: mark@mail.ntua.gr (M.P. Anastasopoulos), avoulk@mail.ntua.gr (A.C. Voulkidis), vasilako@ath.forthnet.gr (A.V. Vasilakos), pcottis@central.ntua (P.G. Cottis).

0140-3664/$ - see front matter © 2008 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2008.05.046

schemes imperative [11]. This multimodal system consists of a number of computing stations, which perform simple measuring tasks upon data of interest and, then, send data to relevant master control nodes, where information processing takes place. One of the main advantages when using multimodal network architectures is their inherent ability to monitor large area networks. Extending the use of BPL devices to act as core computing stations for the pervasive system and employing the UPnP based protocol, the control of a widely dispersed BPL network becomes fast, accurate and almost fully autonomic.

The security of the proposed protocol against a variety of software attacks (data packets eavesdropping, node compromising, etc.) is provided by a customized implementation of the Rijndael algorithm, which, as the respective experimental measurements verify, is fast and resource-saving. The UNIX/Linux environment hosting the proposed protocol stack is considered among the safest in the world of computing [12].

The main contribution of this paper is the implementation of a secure network management protocol for large-scale BPL Networks based on the UPnP platform. Its experimental application in a real BPL Pilot network located in Lavrion, Greece is also examined. The optimum cluster size and topology as well as the optimization of the algorithmic implementation of the aggregation process are subjects to be investigated in a future work.

The rest of the paper is organized as follows. Section 2 presents the core of the implemented protocol and provides some relevant information about UPnP technology and its perspective. The aggregation scheme along with critical parameters expected to affect the overall system performance are outlined in Section 3. In Section 4, the various security risks related to system coherence and stability are discussed. Then, a solution is proposed to deal with these risks. In Section 5, the architecture of the simulated BPL environment is presented along with relevant experimental results. Finally, in Section 6 conclusions are given.

2. Description of the network management protocol

UPnP technology defines a platform for pervasive peer-to-peer network connectivity of various types of computing stations or even embedded systems [10]. UPnP technology provides a distributed, open networking architecture based on TCP/IP and various Web technologies to enable seamless proximity networking in addition to control and data transfer among connected devices. Based on UPnP technology, a device is able to dynamically join a network, obtain an IP address, convey its abilities and services, and learn about the presence and capabilities of other similar devices. A device may also leave a network smoothly and automatically without leaving any unwanted state information behind.

The devices employed in the UPnP architecture are classified in two categories: controlled devices (or simply devices) and control points [10]. A controlled device functions as a server responding to requests from the control points. Both control points and controlled devices may be implemented on a variety of platforms including embedded systems. Both multiple devices and control points may be operational on the same network endpoint simultaneously.

The operational life cycle of UPnP enabled devices is described algorithmically through four basic stages, which allow control points to automatically detect and configure the devices of interest [10]. During the first stage – called *Discovery stage* – the control points search for devices and services. Similarly, the various devices multicast announcements of the services they offer. Once a control point finds a device or service of interest, it requests a more detailed description of its component devices (if any) and services (*Description phase*). The third phase is the *Control phase*, when, by enabling changes to a device state, the control points take control of one or more of its potential services. Then, the control points may keep synchronized with the service state of interest. The control points may subscribe to the event server of a particular service and receive event notifications when the related device state changes (*Eventing phase*). The Discovery, Description, Control and Eventing phases provide UPnP with all the necessary functionalities to discover new devices, acknowledge their capabilities and services, control them and establish subscription-like connections with them, respectively.

For the discovery of the devices, UPnP uses the Simple Service Discovery Protocol (SSDP) over UDP. Due to the nature of SSDP and to the lack of data integrity check of UDP, a large number of broadcast packets are sent during the discovery procedure. The rest of the UPnP functional blocks are supported by TCP. The Description phase occurs through HTTP GET messages which cause responses from the devices containing the relevant device description files. For the Control phase, SOAP remote procedure calls (RPC) are used. Method names, arguments and possible return values are thus hosted in predefined XML structures. The Eventing phase is accomplished through the generic event notification architecture (GENA) mechanism. In UPnP, a per-service rather than a per-variable subscription is supported. If a UPnP control point is to be notified about a single variable change, the corresponding device sends notification messages, not only when this variable is modified, but also each time another (notification-enabled) state variable belonging to the same service is changed upon request.

The implemented protocol is based on the same philosophy UPnP is based, using two basic device types, the control point and the (controlled) device. The devices control the overall network state, measuring crucial operational parameters such as current and voltage along the power line, the BPL signal strength, as well as their ripple, which is a critical in estimating quality of service. By controlling the devices, the control points act as managers upon managed resources, constantly supervising the network state and optimally configuring the devices. Other check parameters may easily be implemented with regard to the control application, making it flexible and highly customizable. Besides controlling the core UPnP part, the control points have the ability to automatically detect which parameters exceed their predefined limits and command the devices to restore the network status. Thus, the network practically becomes autonomic and self-optimizing. The control points function as forecasting agents protecting the system from being disrupted or eroded.

Through the UPnP-based implementation the installation of a new network controller (the UPnP “device”) becomes automatic with no need for extra specific configuration. Thus, the whole installation procedure is rendered quite faster and less susceptible to errors.

3. Providing large-scale services: The data aggregation mechanism

UPnP was originally designed to work in proximity networks, where traffic load and management issues are of secondary importance due to the relatively high bandwidth available and to the limited number of managed devices and services. However, in an open, large-scale network consisting of hundreds or even thousands of device nodes the repeated information overhead, such as information concerning the manufacturer or the complete WWW URL address of the device specifications, may cause the partial loss of the real-time character of the application.

The necessity to suppress redundancy is more frequent in Wireless Sensor Networks (WSN). The application of several aggregation algorithms onto WSNs has been intensively studied and it