Computer Networks 73 (2014) 154–172

Contents lists available at ScienceDirect

Computer Networks

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

Limiting the loss of information in KNXnet/IP on congestion conditions

Salvatore Cavalieri *, Ferdinando Chiacchio

University of Catania, Department of Electrical Electronic and Computer Engineering, Viale A. Doria 6, 95125 Catania, Italy

ARTICLE INFO

Article history:
Received 16 May 2013
Received in revised form 16 August 2014
Accepted 18 August 2014
Available online 27 August 2014

Keywords:
KNXnet/IP
Congestion control
Forwarding policy
Performance evaluation
Petri net
SAN

ABSTRACT

KNXnet/IP communication system allows integration of different KNX networks through IP medium by a particular device called KNXnet/IP Router. Due to the different transmission speeds among KNX networks and the IP medium, a control mechanism to prevent the congestion of KNXnet/IP Routers has been foreseen by the KNXnet/IP standard. In this paper, the authors analyse the performance of the KNXnet/IP congestion control mechanism in terms of its impact on the loss of information exchanged between KNX devices located in different KNX networks. The main goal is to point out suitable configurations of the congestion control mechanism capable, more than others, to limit the loss of information. Performance evaluation has been realised through simulation of a Petri Net model based on Stochastic Activity Network (SAN), capable of implementing the main features of the KNXnet/IP specifications.

1. Introduction

KNX is one of the most well-known and worldwide used standards for home and building automation [1–5]. It was defined several years ago and later it was integrated into IP environment through the definition of the KNXnet/IP specification [6]. KNXnet/IP has quickly gained the attention of vendors and users; also researchers are interested in several relevant issues, like performance [7–9] and security [10].

Integration of KNX with IP is based on the use of a particular device called KNXnet/IP Router, which allows connection of several KNX networks to an IP medium used as backbone. Due to the very limited transmission speeds foreseen for certain types of KNX networks, the KNXnet/IP Router may receive more messages from IP network than it is able to sell off; in this case all or parts of the incoming messages may be lost. That condition is relevant to congestion; in order to mitigate this issue, a mechanism of congestion control has been introduced in the KNXnet/IP standard [6].

Basically, the KNXnet/IP congestion control is based on a very simple stop-and-go strategy; when a KNXnet/IP Router detects an internal congestion condition, it sends in multicast a particular datagram, causing the stop of all transmissions over IP by the other KNXnet/IP Routers. Communications are resumed when the congestion condition inside the KNXnet/IP Router has been surpassed.

It is clear that the activation of KNXnet/IP congestion control mechanism may cause loss of information exchanged by control devices located in different KNX networks and may affect the behaviour of the control applications running on KNXnet/IP communication system. For example, let us consider a control scenario featuring the presence of a controller located in a KNX network which has to receive the values generated by several sensors

* Corresponding author.
E-mail addresses: salvatore.cavalieri@dieei.unict.it (S. Cavalieri), chiacchio@dmi.unict.it (F. Chiacchio).

http://dx.doi.org/10.1016/j.comnet.2014.08.012
1389-1286/© 2014 Elsevier B.V. All rights reserved.

connected to other KNX networks. In congestion condition, after the activation of the congestion control mechanism, communication over IP between controller and sensors is paused for a certain period during which the controller may lose some values generated by sensors. In this case, the loss of information may produce undesired effects to the control algorithm executed by the controller (e.g. wrong commands to the actuators due to missed information from the sensors).

Performance of the entire KNXnet/IP system may be improved by limiting as much as possible the amount of data lost during congestion conditions. The current KNXnet/IP congestion control mechanism features several optional configurations which may impact on the loss of information in congestion condition. Among them, one of the most important is the activation rule that defines the conditions allowing a KNXnet/IP Router to detect an internal congestion. The KNXnet/IP standard draws general principles ruling the activation of the congestion control mechanism, but it does not provide exhaustive indication about their implementation; different implementations of KNXnet/IP congestion control activation rule will be proposed and then compared in terms of impact on the information loss occurring during congestion conditions.

The analysis presented in the paper uses a KNXnet/IP model based on Stochastic Activity Network (SAN) formalism [11]; results presented in the following have been obtained through simulation of the SAN model.

Current literature presents few works dealing with KNXnet/IP Router congestion; to the best of authors' knowledge, only the papers [7–9,12,13] cover this subject. The paper [7] presents an overview of the congestion problem in KNXnet/IP environment; [8] highlights also some possible countermeasures able to reduce congestion in the KNXnet/IP Router and improve communication bandwidth. In [9] a study about the influence of congestion in the loss of information for KNXnet/IP network communication is presented; but that analysis does not take into account the current KNXnet/IP congestion control mechanism, under definition when the paper was written. Finally, in [12,13] the same authors present an analysis of the current KNXnet/IP congestion control mechanism; the analysis is also based on the use of SAN. The results shown in these last two papers must be considered preliminary to the ones here presented, which refer to a more general KNXnet/IP communication scenario and take into account the influence of a wider set of parameters featured by the KNXnet/IP congestion control mechanism (e.g. KNXnet/IP Router internal queue sizes). For these reasons, conclusions here presented include and extend the ones given in [12,13].

After a brief overview of KNX and KNXnet/IP communication systems, the paper will present the current KNXnet/IP congestion control mechanism; then, the main assumptions made for the relevant analysis will be pointed out. The SAN model adopted for this analysis will be presented after a brief introduction of Stochastic Activity Network formalism. Finally, the main results achieved by the authors will be shown and the relevant comments will be given.

2. Overview of KNX and KNXnet/IP

The aim of this section is to give basic information about KNX specifications, for both KNX basic communication system and for its IP extension.

2.1. KNX communication system

KNX communication stack allows exchange of KNX telegrams through the Physical, Data Link, Network, Transport and Application layers.

Several physical media have been foreseen for the KNX Physical layer: power line, radio frequency and twisted pair (TP0 and TP1). In this paper only the twisted pair 1, TP1, running at 9600 bps, will be considered [14]. KNX TP1 specification features a Medium Access Control based on CSMA/CA, Carrier Sense Multiple Access with Collision Avoidance. In order to avoid saturation of the TP1 medium, each KNX TP1 device can transmit, at most, a load corresponding to 50 telegrams/s, with each telegram containing up to 23 bytes of data.

KNX TP1 devices are connected to a physical Segment, which may feature a linear, star, tree or mixed topology. Two different versions of TP1 exist: TP1-64 and TP1-256; the main difference is the maximum number of connectable KNX devices to a physical Segment: up to 64 in TP1-64 and up to 256 in TP1-256. The maximum cable length of a physical Segment is 1000 m. Bridges can be used to connect up to four physical Segments allowing up to 255 KNX TP1-64 devices to be connected on a so-called Line. In the case of TP1-256, a Line is made up of only one physical Segment and up to 256 devices can be connected. For larger networks, up to 16 Lines can be combined to an Area using 15 Line Coupler; the inner Line of an Area is called Main Line and the outer Lines of an Area are called Lines. An Area may therefore have a maximum number of 256 × 16 = 4.096 devices and an extension of 4000 m × 16 = 64 km. Multiple Areas may be connected by Backbone Couplers; up to 16 Areas can be connected using 15 Backbone Couplers. The Main Line of the inner Area is called Backbone Line. A maximum size network may therefore have up to 4.096 × 16 = 65.536 devices and a total network extension of 64 km × 16 = 1.024 km. Fig. 1 shows an example of a KNX communication system made up of Lines and Areas.

KNX Data Link Layer (DLL) offers services to transmit and receive user data, using three telegram priority levels (low, normal and urgent) [15].

According to KNX Application layer [16], particular objects, Group Objects, allow communication between devices; they are abstract data structures giving access to internal objects in a device, which can store any type of information and can be writeable and readable by a generic device. Several Group Objects may be bound together by assigning them the same Group Address; in this way the values of the Group Objects may be kept in sync.

2.2. KNXnet/IP communication system

A KNXnet/IP system is defined as a set of KNXnet/IP Routers communicating over a one-to-many communication