Design Experience with Routing SW and Related Applications

Miroslav Sveda
Faculty of Information Technology
Brno University of Technology
Brno, Czech Republic
e-mail: sveda@fit.vutbr.cz

***Abstract*—This paper deals with the current software architectures for intermediate systems for Intranet and small-range wireless interconnection using case studies founded on real-world applications. The approach demonstrates another contribution to network convergence in interconnecting software architecture development, which stems from a design experience based on industrial network applications and on metropolitan networking. The first case study focuses on IEEE 1451 family of standards that provides a design framework for creating applications based not only on IP/Ethernet profile but also on ZigBee. Next case study explores how security and safety properties of Intranets can be verified under every network configuration using model checking. The contribution of the paper consists of a new method to network convergence and network modeling in software architecture development.**

Keywords-network architecture, sensor networks, intranets, validation of network configuration

I. INTRODUCTION

This paper focuses on software architectures for intermediate system control plane in frame of Intranet and ZigBee, and then presents new contributions to network convergence and network modeling in software architecture development. To facilitate comprehensible wording, the beginnings of this section and two following subsections restate basic, standard-based terminology used in the following text.

According to the ISO Open Systems Interconnection (ISO-OSI) vocabulary, two or more sub-networks are interconnected using equipment called as intermediate system whose primary function is to relay selectively information from one sub-network to another and to perform protocol conversion where necessary. A bridge or a router provides the means for interconnecting two physically distinct networks, which differ occasionally in two or three lower layers respectively. The bridge converts frames with consistent addressing schemes at the data-link layer, or medium access and control (MAC) sub-layer, while the router deals with packets at the network layer. Lower layers of these intermediate systems are implemented according to the proper architectures of interconnected networks. When sub-networks differ in their higher layer protocols, especially in the application layer, or when the communication functions of the bottom three layers are not sufficient for coupling, the intermediate system, called in this case as gateway, contains all layers of the networks involved and converts application messages between appropriate formats.

An intermediate system represents typically a node that belongs simultaneously to two or more interconnected networks. The backbone network interconnects more intermediate systems that enable to access different sub-networks. If two segments of a network are interconnected through another network, the technique called as tunneling enables to transfer protocol data units of the end segments nested in the proper protocol data units of the interconnecting network.

The next section corroborates the basic concepts of supporting resources, namely (1) IP routers as the most important means forming the Internet, (2) industrial network couplers that enable to create hierarchical communication systems as a basis of various -- not only industrial -- applications, and (3) design experience collected by our team in this domain, which influence unsurprisingly the current research.

Section III. dealing with network convergence aims at Ethernet and IP-based industrial networking that offer an application development environment compatible with common TCP/IP setting. It stems from IEEE 1451 family of standards and provides a design framework for creating applications based not only on TCP/IP/Ethernet profile but also on ZigBee. The second part of this section reviews the first case study based on an application dealing with pressure and temperature measurement and safety and security management along gas pipes.

In section IV., the presented network modeling approach provides a unifying model suitable for description of relevant aspects of real IP computer networks including dynamic routing and filtering. The rest of this section reviews the second case study based on an application exploring how security and safety

 ISBN:978-1-61208-113-7

properties can be verified under every network configuration using model checking.

II. STATE OF THE ART

A. IP routers

Internet/Intranet router architectures have experienced three generations [7]. The *first generaion* router architecture, sometimes called also as software router, which is based on a monolitic (or centralized) routing engine, appears just as a simple PC equiped with multiple line cards.

In a cluster-based architecture, often called as the *second generation*, the Routing Engine modules are distributed on several network communication cards that share an interconnection, usually through a system bus, to operation memory and processor on the control card.

Many current Internet routers, which can provide high speed switching capacity, are built with switching fabrics based on a Banyan or analogous self-routing topology[8]. Not only pure routing, but also additional network services have enriched router functionalities in the past few years, for Internet namely packet tagging, emulating application-level proxies, application-specific packet dropping, performance monitoring, intrusion detecting, and assorted filtering and firewalling. Nevertheless, the routing engine provides the essential part of router functionality. As a software component, the routing engine is used to control the router activities and to build the data forwarding table.

B. Industrial networks coupling

Contemporary industrial distributed computer-based systems encompass, at their lowest level, various wired or wireless digital actuator/sensor to controller connections. Those connections usually constitute the bottom segments of hierarchical communication systems that typically include higher-level fieldbus or Intranet backbones. Hence, the systems must comprise suitable interconnections of incident higher and lower fieldbus segments, which mediate top-down commands and bottom-up responses. While interconnecting devices for such wide-spread fieldbuses as CAN, Profibus, or WorldFIP are currently commercially available, some real-world applications can demand also to develop various couplers either dedicated to special-purpose protocols or fitting particular operational requirements, see [12].

The following taxonomy of industrial communication and/or control network (ICN) interconnections covers both the network topology of an interconnected system and the structure of its intermediate system, which is often called in the industrial domain as *coupler*. On the other hand, the term gateway sometimes denotes an accessory connecting PC or a terminal to an ICN. For this paper, the expression "gateway" preserves its original meaning according to ISO-OSI terminology as discussed above.

The first item to be classed appears the level ordering of interconnected networks. A peer-to-peer structure occurs when two or more interconnected networks interchange commands and responses through a bus coupler in both directions so that no one of the ICNs can be distinguished as a higher level. If two interconnected ICNs arise hierarchically ordered, the master/slaves configuration appears usual at least for the lower-level network.

The second classification viewpoint stems from the protocol profiles involved. In this case, the standard taxonomy using the general terminology mentioned above can be employed: bridge, router, and gateway. Also, the tunneling and backbone networks can be distinguished in a standard manner.

The next, refining items to be classed include internal logical architectures of the coupler, such as source or adaptive routing scheme, routing and relaying algorithms, and operating system services deployed.

C. Design backgrounds

We launched our coupling development initiatives in the Fieldbus and Internet domains almost concurrently, see [10] and [3]. Fieldbus coupling was studied by our research team originally from the viewpoint of network architecture of low-level fieldbuses [10][11]. Next interest was focused on real-world applications based on network coupling, such as data acquissition appliance [9], or wireless smart sensors [14]. And also, the role of Ethernet and TCP/IP attracted our attention as a means of network convergence [2][12].

The other branch of our network interconnection initiative covers IP routing. In this case we launched with software router design based on a simple Unix machine [3] and with creation of a routing domain for academic metropolitan networking [5]. The current research initiatives deal with the high-speed IP6 router for optical networks [16], and with modeling of dynamically routed IP networks and exploration of their properties such as reachability-based safety and security [6].

III. NETWORK CONVERGENCE

This section deals with network convergence aiming at Ethernet and IP-based industrial networking that offer an application development environment compatible with the common TCP/IP setting. It stems

 ISBN:978-1-61208-113-7

from IEEE 1451 family of standards, mentioned in the subsection 3.2 and provides a design framework for creating applications based not only on TCP/IP/Ethernet profile but also on ZigBee. The last part of this section reviews the first case study based on an appication dealing with pressure and temperature measurement and safety and security management along gas pipes.

A. IP over Ethernet profile

The attractiveness of Ethernet as an industrial communication bus is constantly increasing. However the original concept of the Ethernet, which was developed during seventies of the last century as communication technology for office applications, has to face some issues specific for industrial applications. The concept of the Ethernet proved to be very successful and encountered issues are being addressed by modifications and extensions of the most popular 10/100 BaseT standard. In fact, the switched Ethernet with constraint collision domains proved to be efficient real-time networking environment also for time-critical applications.

Similarly, IP networking support appears as a rapidly dominating tendency in current industrial system designs. Namely, when layered over a real-time concerning data-link protocol, it seams as a best choice for future applications because of a simple interfacing within the Internet.

B. IEEE 1451 profile

The design framework, presented in this paper as a flexible design environment kernel, is rooted in the IEEE 1451.1 standard specifying smart transducer interface architecture. That standard provides an object-oriented information model targeting software-based, network independent, transducer application environments. The framework enables to unify interconnections of embedded system components through wireless networks and Ethernet-based intranets, which are replacing various special-purpose Fieldbuses in industrial applications [12].

The IEEE 1451 package consists of the family of standards for a networked smart transducer interface. The 1451.1 software architecture provides three models of the transducer device environment: (i) the object model of a network capable application processor (NCAP), which is the object-oriented embodiment of a smart networked device; (ii) the data model, which specifies information encoding rules for transmitting information across both local and remote object interfaces; and (iii) the network communication model, which supports client/server and publish/subscribe paradigms for communicating information between NCAPs. The standard defines a network and transducer hardware neutral environment in which a concrete sensor/actuator application can be developed.

The object model definition encompasses the set of object classes, attributes, methods, and behaviors that specify a transducer and a network environment to which it may connect. This model uses block and base classes offering patterns for one Physical Block, one or more Transducer Blocks, Function Blocks, and Network Blocks. Each block class may include specific base classes from the model. The base classes include Parameters, Actions, Events, and Files, and provide component classes.

The Transducer Block abstracts all the capabilities of each transducer that is physically connected to the NCAP I/O system. During the device configuration phase, the description of what kind of sensors and actuators are connected to the system is read from the hardware device. The Transducer Block includes an I/O device driver style interface for communication with the hardware. The I/O interface includes methods for reading and writing to the transducer from the application-based Function Block using a standardized interface.

The Function Block provides a skeletal area in which to place application-specific code. The interface does not specify any restrictions on how an application is developed.

The Network Block abstracts all access to a network employing network-neutral, object-based programming interface supporting both client-server and publisher-subscriber patterns for configuration and data distribution.

C. ZigBee profile

The ZigBee/IEEE 802.15.4 protocol profile [1][15] is intended as a specification for low-powered wireless networks. ZigBee is a published specification set of higher level communication protocols designed to use small low power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks. The document 802.15.4 specifies two lower layers: physical layer and medium access control sub-layer. The ZigBee Alliance builds on this foundation by providing a network layer and a framework for application layer, which includes application support sub-layer covering ZigBee device objects and manufacturer-defined application objects.

Responsibilities of the ZigBee network layer include mechanisms used to join and leave a network, to apply security to frames and to route frames to their intended destinations. In addition to discovery and maintenance of routes between devices including

 ISBN:978-1-61208-113-7

discovery of one-hop neighbors, it stores pertinent neighbor information. The ZigBee network layer supports star, tree and mesh topologies

The ZigBee application layer includes application support sub-layer, ZigBee device objects and manufacturer-defined application objects. The application support sub-layer maintains tables for binding, which is the ability to match two devices together based on their services and their needs, and forwards messages between bound devices.

D. Sensor network case study

This section describes a case study that demonstrates deployment of the introduced design concepts. The application deals with pressure and temperature measurement and safety and security management along gas pipes. The related implementation stems from the IEEE 1451.1 model with Internet and the IEEE 1451.5 wireless communication based on ZigBee running over the IEEE 802.15.4.

The interconnection of TCP/IP and ZigBee is depicted on Figure 1. It provides an interface between ZigBee and IP devices through an abstracted interface on IP side. Each wireless sensor group is supported by its controller providing Internet-based clients with secure and efficient access to application-related services over the associated part of gas pipes. In this case, clients communi-cate to controllers using a messaging protocol based on client-server and subscribe-publish patterns employing 1451.1 Network Block functions. A typical configuration includes a set of sensors generating pressure and temperature values for the related controller that computes profiles and checks limits for users of those or derived values. When a limit is reached, the safety procedure closes valves in charge depending on safety service specifications.

Security configurations can follow in this case the tiered network architecture: (1) To keep the system maintenance simple, all wireless communication uses standard ZigBee hop-by-hop encryption based on single network-wide key because separate pressure and/or temperature values, which can be even-dropped, appear useless without the overall context; (2) Security in frame of Intranet subnets stems from current virtual private network concepts such that the communicating couples utilize ciphered channels based on tunneling between each client and a group of safety valve controllers -- the tunnels are created with the support of associated authentications of each client.

The example network configuration, see Figure 2., comprises several groups of wireless pressure and temperature sensors with safety valve controllers as base stations connected to wired intranets that dedicated clients can access effectively through Internet. The WWW server supports each sensor group by an active web page with Java applets that, after downloading, provide clients with transparent and efficient access to pressure and temperature measurement services through controllers. Controllers offer clients not only secure access to measurement services over systems of gas pipes, but also communicate to each other and cooperate so that the system can resolve safety and security-critical situati ons by shutting off some of the valves.

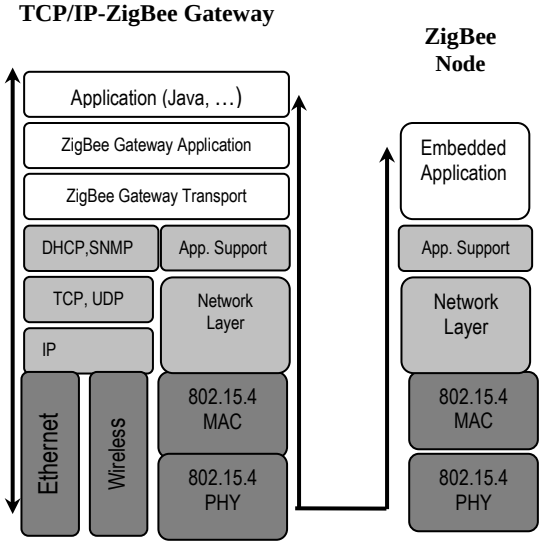

Figure 1: Network gateway.

Each controller communicates wirelessly with its sensors through 1451.5 interfaces by proper communication protocol. In the discussed case the proposed P1451.5-ZigBee, which means ZigBee over IEEE 802.15.4, protocol was selected because it fits application requirements, namely those dealing with power consumption, response timing, and management. The subscriber-publisher style of communication, which in this applica-tion covers primarily distribution of measured data, but also distribution of group configuration commands, employs IP multicasting. All regular clients wishing to receive messages from a controller, which is joined with an IP multicast address of class D, register themselves to this group using IGMP. After that, when this controller generates a message by Block function publish, this message is delivered to all members of this class D group, without unnecessary replications.

The WWW server supports each sensor group by an active web page with Java applets that, after downloading, provide clients with transparent and efficient access to pressure and temperature

 ISBN:978-1-61208-113-7

measurement services through controllers. Controllers provide clients not only with secure access to measurement services over systems of gas pipes, but also communicate to each other and cooperate so that the system can resolve safety and security-critical situations by shutting off some of the valves.

Each wireless sensor group is supported by its controller providing Internet-based clients with secure and efficient access to application-related services over the associated part of gas pipes. In this case, clients communicate to controllers using a messaging protocol based on client-server and subscriber-publisher patterns employing 1451.1 Network Block functions. A typical configuration includes a set of sensors generating pressure and temperature values for the related controller that computes profiles and checks limits for users of those or derived values. When a limit is reached, the safety procedure, which is derived from the fail-stop model, closes valves in charge depending on safety service specifications.

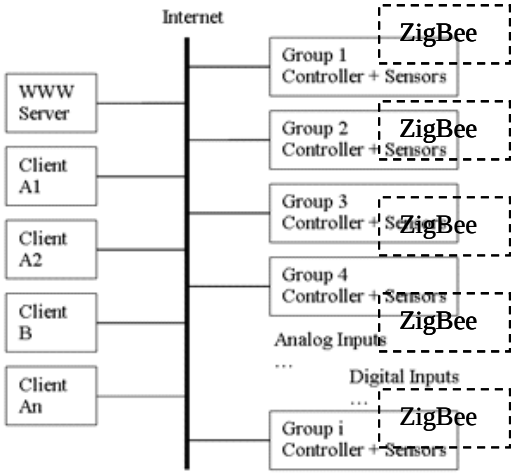

Figure 2: Example network configuration.

IV. DYNAMIC NETWORK BEHAVIOR

The current goals of our research in frame of Internet-level routed networks consist of i) creation of a unifying model suitable for description of relevant aspects of real computer networks including routing information, ACLs (access control lists), NAT (network address translation), dynamic routing policy; and ii) delivering methods for automated verification of dependable properties (e.g., availability, security, survivability). The unique added value of the project is to specifically merge the research on formal methods with the research on network security to devise a new method for network security verification.

A. *Dynamic network model*

The recent work has focused on studying models and analysis techniques based on simulation and network monitoring [6]. These models, nevertheless, do not take into account routing and packet filtering despite the fact that these aspects may significantly influence the traffic coverage observed in the network. The intensive research needs to be done in order to find new models that would include dynamic view on the network.

Similarly to hardware and software analysis based on simulation, the network simulation methods are useful mainly to observe properties given by regular behavior of the system. Simulation techniques are incompetent in catching "what if" cases that occur rarely in the system. However, the real world systems inevitably exhibit also the unusual behavior. The use of formal methods is better suited for checking those situations to uncover hidden problems.

The dynamics of current network models is most often limited to changes of actual data in time. The other dimension of dynamics of routed networks comes from dynamic routing protocols and topology changes based on the availability of links and link parameters, e.g., reliability, bandwidth or load. The anticipated project results characterize a novel approach in the area of network traffic analysis.

B. *Dynamic network case study*

The recent work has focused on studying models and analysis techniques based on simulation and network monitoring [6][13]. These models, nevertheless, do not take into account routing and packet filtering despite the fact that these aspects may significantly influence the traffic coverage observed in the network. The intensive research needs to be done in order to find new models that would include dynamic view on the network.

In our work we explore how security and safety properties can be verified under every network configuration using model checking [4]. The model checking is a technique that explores all reachable states and verifies if the specified properties are satisfied over each possible path to those states. Model checking requires specification of a model and properties to be verified. In our case, the model of network consists of hosts, links, routing information and ACLs. The network security-type properties can be expressed in the form of modal logics formulae as constraints over states and execution paths. If those formulas are not satisfied, the model checker generates

 ISBN:978-1-61208-113-7

a counterexample that reveals a state of the network that violates the specification. If the formulas are satisfied, it means, that the property is valid in every state of the systems, see more detail in [13].

V. CONCLUSIONS

The paper discusses software architectures for intermediate system's control planes belonging to Intranets and Fieldbuses by two case studies derived from genuine implementations. The interest is focused both on network convergence and on network modeling in application architectures development. The applied solutions stem from design experience both with industrial network appliances and metropolitan networking. The first case study focuses on IEEE 1451 family of standards that provides a useful design framework for creating applications based not only on IP/Ethernet profile but also on ZigBee over IEEE 802.15.4. Next case study explores how security and safety properties of interconnected intranets can be verified under every network configuration using model checking.

Note that several various methods may fit modeling and analysis of the properties in the domains of interest. Most often, the combination of several methods leads to better results. The emphasis of the project's research is put on the formal verification methods, but other methods are certainly worthwhile to explore as well. The other methods may be orthogonal with formal verification, or they may support the formal methods.

In particular, monitoring may provide a fruitful data for classification and definition of security-related properties based on the real traffic. Modeling and simulation serve as a useful tool to specify and replay possible dangerous scenarios found by the formal verification. Therefore, simulators and monitors can efficiently support network-wide analysis namely during the design and development.

ACKNOWLEDGEMENTS

This project has been partially supported by the BUT FIT grant FIT-10-S-2, the research plan MSM0021630528 and through the grant no. GACR 102/08/1429. Also, the author was partially supported by the grant no. FR-TI1/037 of Ministry of Industry and Trade.

The author acknowledges contributions to this work by his colleagues (alphabetically) Petr Matousek, Ondrej Rysavy, Jaroslav Rab, Roman Trchalik, Radimir Vrba and Frantisek Zezulka.

REFERENCES

[1] P. Baronti, P. Pillai, V. Chook, S. Chessa, A. Gotta, and Y. Fun Hu, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," Computer communications, Vol.30, 2007, pp.1655-1695.

[2] P. Cach, P. Fiedler, M. Sveda, M. Prokop, and M. Wagner, "A Sensor with Embedded Ethernet," In WSEAS Transactions on Circuits, Iss.1, Vol.2, 2003, pp.213-215.

[3] I. Cernohlavek, J. Novotny, V. Slama, V. Zahorik, and M. Sveda, "Open-Box Routers with Academic Metropolitan Networking," Technical Report, Brno University of Technology and Masaryk University, Brno, 1994.

[4] E.M. Clarke, O. Grumberg, and D.A. Peled, Model Checking, MIT Press, Boston, 1999.

[5] L. Kania, S. Smolik, M. Sveda, and V. Zahorik, "The Brno Academic Computer Network and its Future Development," In Proceedings INVEX-CCT'95, BVV Press, Brno, 1995, pp.1-5.

[6] P. Matousek, J. Rab, O. Rysavy, and M. Sveda, "A Formal Model for Network-wide Security Analysis," In Proceeding of the 15th IEEE International Symposium and Workshop on the Engineering of Computer-based Systems, Belfast, GB, IEEE Computer Society, Los Alamitos, 2008, pp.171 181.

[7] K. Nguyen and B. Jaumard, "Routing Engine Architecture for Next Generation Routers: Evolutional Trends," In International Journal of Network Protocols and Algorithms, Vol.1, No.1, Macrothink Institute, Las Vegas, Nevada, 2009, pp.62-85.

[8] A. Nucci and K. Papagiannaki, Design, Measurement and Management of Large-Scale IP Networks: Bridging the Gap between Theory and Practice, Cambridge University Press, New York, 2009.

[9] O. Sajdl, Z. Bradac, R. Vrba and M. Sveda, "Data Acquisition System Exploiting Bluetooth Technology, In WSEAS Transactions on Circuits," Iss.1, Vol.2, 2003, pp.117-119.

[10] M. Sveda, "Routers and Bridges for Small Area Network Interconnection," In Computers in Industry, Vol.22, No.1, Elsevier Science, Amsterdam, NL, 1993, pp.25 29.

[11] M. Sveda, R. Vrba, and F. Zezulka, "Coupling Architectures for Low-Level Fieldbuses," In Proceedings 7th IEEE ECBS Conference, Edinburgh, Scotland, IEEE Comp. Soc., 2000m pp.148-155.

[12] M. Sveda, P. Benes, R. Vrba, and F. Zezulka, "Introduction to Industrial Sensor Networking," Book Chapter in M. Ilyas, I. Mahgoub (Eds.): Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press LLC, Boca Raton, FL, 2005, pp.10.1-10.24.

[13] M. Sveda, O. Rysavy, P. Matousek, and J. Rab, "An Approach for Automated Network-Wide Security Analysis," In: Proceedings of the Ninth International Conference on Networks ICN 2010, Les Menuires, FR, IARIA, IEEE CS, 2010, pp. 294-299.

[14] R. Vrba, O. Sajdl, R. Kuchta, and M. Sveda, "Wireless Smart Sensor Network System," In Proceedings of the Joint International Systems Engineering Conference (ICSE) and The International Council on Systems Engineering (INCOSE), Las Vegas, Nevada, 2004.

[15] ZigBee, 2006. ZigBee Specification. ZigBee Alliance Board of Directors Website http://www.zigbee.org/.

[16] M. Kosek and J. Korenek, "FlowContext: Flexible Platform for Multigigabit Stateful Packet Processing," In: 2007 International Conference on Field Programmable Logic and Applications, Los Alamitos, US, IEEE CS, 2007, pp. 804-807.

 ISBN:978-1-61208-113-7