Traffic Measurement and Analysis of Building Automation and Control Networks

Radek Krejčí[1], Pavel Čeleda[2], and Jakub Dobrovolný[2]

[1] CESNET, z.s.p.o., Zikova 4, 160 00 Prague
Czech Republic
rkrejci@cesnet.cz
[2] Institute of Computer Science, Masaryk University
Botanická 68a, 602 00 Brno, Czech Republic
{celeda,dobrovolny}@ics.muni.cz

Abstract. This paper proposes a framework for a flow-based network traffic monitoring of building automation and control networks. Current approaches to monitor special environment networks are limited to checking accessibility and a state of monitored devices. On the other hand, current generation of flow-based network monitoring tools focuses only on the IP traffic. These tools do not allow to observe special protocols used, for example, in an intelligent building network. We present a novel approach based on processing of flow information from such special environment. To demonstrate capabilities of such approach and to provide characteristics of a large building automation network, we present measurement results from Masaryk University Campus.

Keywords: BACnet, BACnetFlow, network, measurement, analysis, building, automation, control.

1 Introduction

Network traffic monitoring and measurement using IP flow information has become useful instrument for network operators. It provides information about who is communicating with whom, at what time, for how long and how much data is transferred. Today, flow monitoring technologies are limited to IP networks. Flow information can be used for billing and accounting, network profiling, network planning and network security. There are similar needs to know what happens in special networks, like various sensor networks, Building Management System (BMS) networks or Supervisory Control And Data Acquisition (SCADA) networks.

With experiences from IP networks, we believe that the flow-based monitoring of special environment networks can have a positive impact on their management and security. Security of industrial and automation networks becomes much more important [1]. An attacker could set off a fire alarm, turn off an air-conditioning or turn off security systems such as a closed-circuit television (see Figure 1). The controll networks were originally physically separated from other networks.

R. Sadre et al. (Eds.): AIMS 2012, LNCS 7279, pp. 62–73, 2012.

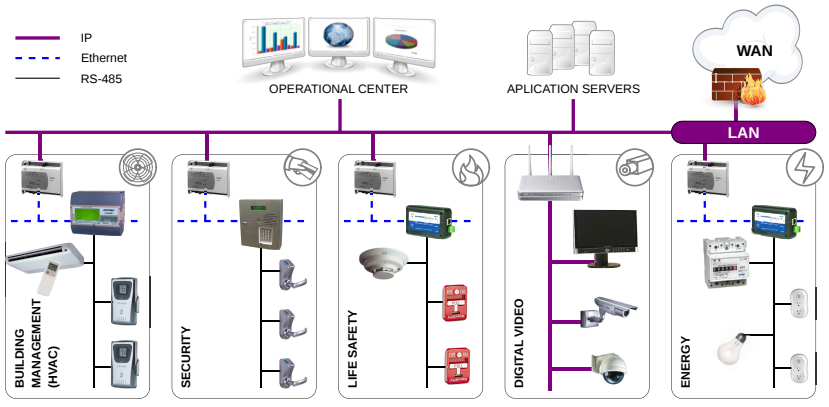

Fig. 1. Example of a BMS network with interconnected subsystems managing: *(1)* heating, ventilation, and air conditioning (HVAC), *(2)* access control to secure particular parts of the building, *(3)* life safety / fire systems, *(4)* digital video circuits observing important places and *(5)* systems controlling power consumption

Now, they have become more and more IP-enabled and they are now accessible to hackers from the other side of the world. In comparison to common IP networks, security of automation networks is still underestimated.

In case of BMS networks, the definition of a network traffic flow and information related to the flow is different in comparison to IP networks. Today, Cisco NetFlow [2] technology is a de facto standard for IP flow monitoring. However, NetFlow is inappropriate for the traffic monitoring of non-IP BMS networks due to the fixed NetFlow data format which is relevant mainly to IP networks. Possible approach to deal with this issue is to use the *IP Flow Information Export* (IPFIX) [3] protocol introduced by the Internet Engineering Task Force (IETF) as a new standard for flow information processing. The IPFIX enables anyone to define new information elements using enterprise IDs assigned by the Internet Assigned Numbers Authority (IANA). We plan to use IPFIX to transfer and store a specific information related to a BMS network traffic. Currently, we use SQL database for these purposes.

In this paper we present results of the network traffic monitoring using the special framework for measurement of flow information in an environment of BMS network based namely on the BACnet protocol [4], [5]. Presented data comes from the measurement performed in the BMS network of the Masaryk University Campus in Brno [6]. Detailed description of the measurement framework is also provided.

The paper is organized as follows. After the Introduction, Section 2 summarises state of the art in the field of security of the automation and control networks. Section 3 defines BACnetFlow as an equivalent of the IP flow in the environment of BMS network. Proposed framework for observation, storage and

further processing of BACnet network traffic flow information is described in Section 4. Section 5 reports on measurement results from monitoring Masaryk University Campus network. Deployment evaluation of the monitoring system is also included. Finally we conclude the ideas and propose further work in Section 6.

2 Related Work

Current monitoring of BMS networks is focused mainly to checking accessibility and a state of devices. Mainly Nagios [7] and other monitoring systems are used to actively access devices in the network and to check their proper functionality. However, this approach misses information about unexpected (forgotten or enemy) devices in the network or about a misconfigured device function which is not explicitly checked.

Barbosa et al. [8] apply flow monitoring in SCADA networks. However, they are limited to observe only IP related information. In contrast, we get insight into the specific BMS protocol such as the BACnet. To achieve this, we have modified the original IP flow definition to BACnetFlow (see Section 3) and we observe much more detailed information.

There is some research on securing BMS networks and connected devices using special protocols or systems preventing unauthorised operations [9,10]. The main issue of this approach is a very limited computational power and a lack of other resources available in such devices [11]. Therefore, it is quite challenging task to protect these devices when it is needed to implement any special, e.g. cryptographic, functions inside them.

Monitoring and analysing network traffic in BMS network is not a common approach. Analysing application part of the traffic is used for example in some firewalls as [12], which is used to protect Modbus devices from dangerous commands.

3 BACnetFlow

BACnet is a communication protocol for BMS networks. As a transport protocol, BACnet supports usage of LonTalk, PTP, MS/TP, ARCNET and Ethernet protocols. The last two mentioned protocols can be supplemented by an IP layer. Information carried by BACnet protocol is divided into separated layers (see Figure 2). Especially the information from the network layer protocol data unit (NPDU) is crucial to describe flows related to the BACnet protocol.

To identify flows related to the BACnet protocol, we defined specific set of items to distinguish particular BACnet flows. We named such flow record BACnetFlow (see Figure 3). Key fields are used to identify BACnetFlow, while non-key fields contain traffic statistics (timestamps, counters) and BACnet specific values.

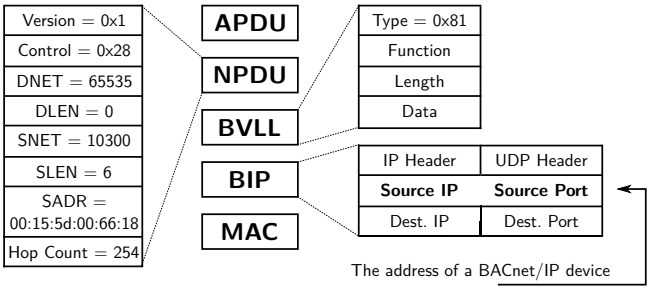

Fig. 2. BACnet over IP consists of IP layer, BACnet virtual link layer (BVLL), network layer protocol data unit (NPDU) and application layer protocol data unit (APDU). The MAC layer is unspecified.

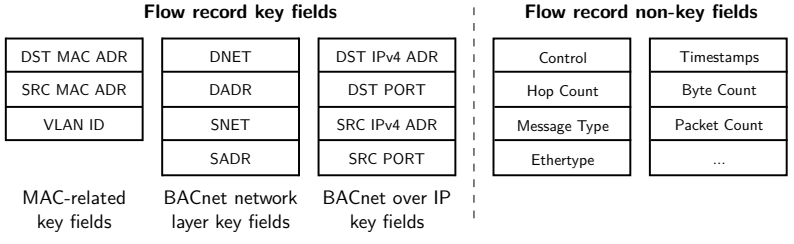

Fig. 3. BACnet flow record consists of key fields extracted from MAC/BACnet/BIP layer and non-key fields with additional statistics

Using the standard 5-tuple[1] identifying the IP flow is not possible since IP is not the mandatory transport protocol for BACnet. Furthermore, even if IP is used as the transport protocol, BACnet messages are often broadcasted to the whole network and identification of BACnet communication participants is not possible solely from the IP flow information.

4 System Architecture

Figure 4 shows the proposed system for a real-time network monitoring of BMS networks. The architecture of the proposed system consists of the following three parts.

BACnet network carrying data over Ethernet at a rate of 10–1000 Mbps. The system is connected to the network through mirror ports or network Test Access Ports (TAPs) inserted in backbone links. This approach provides the real-time overview of all traffic on the observed BACnet network.

[1] Source IP address, destination IP address, source port, destination port and transport protocol.

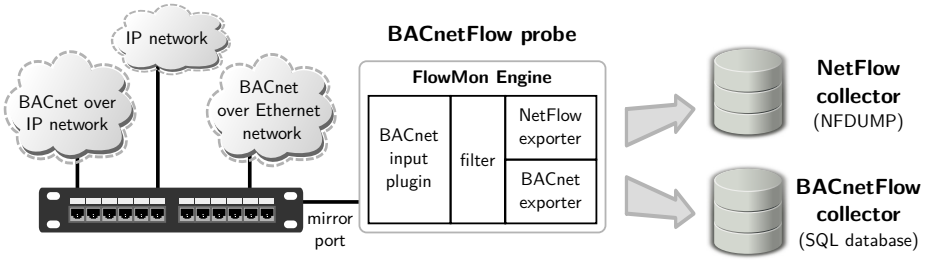

Fig. 4. Architecture of flow-based monitoring system for BMS networks using the BACnet protocol

BACnetFlow probes based on stand-alone FlowMon probes adapted to the specific environment of BMS networks. This part of the system is described in detail in Section 4.1.

BACnetFlow collectors supporting both BACnetFlow and NetFlow protocols. This part of the system stores flow information for a further analysis.

4.1 BACnetFlow Probe

According to our best knowledge, there exists no tool which can be used to generate flow-based statistics from a BACnet network. We decided to use FlowMon exporter engine [13] providing plugin API and to write own set of BACnet plugins. Source codes of the BACnet plugins are available at [14]. The plugins control how the packets are parsed, stored into a flow cache and exported.

BACnet input plugin reads packets, extracts information into BACnetFlow record fields and stores the records into the flow cache. Besides parsing standard IP traffic for NetFlow export, plugin processes BACnet packets of the following forms.

```
eth:llc:bacnet-npdu:bacnet-apdu
eth:ip:udp:bvll:bacnet-npdu:bacnet-apdu
```

BACnet over Ethernet uses *Logical Link Control* (LLC) as its data link layer. BACnet traffic is identified by *Destination Service Access Point* (DSAP) and *Source Service Access Point* (SSAP) both set to the value 0x82. This value is stored as the flow's ethertype to identify BACnet over Ethernet flow.

In case of BACnet over IP, the UDP protocol with source and destination ports 47808 is used. The Type field with value 0x81 is extracted from BVLL and stored as the flow's ethertype as an identifier of the BACnet over IP flow.

VLAN tagging (IEEE 802.1Q) is often used to share a physical Ethernet network link by multiple independent logical networks. Therefore, to distinguish traffic in various VLANs, the VLAN identifier is also extracted and used as one of the BACnetFlow key fields (see Figure 3).

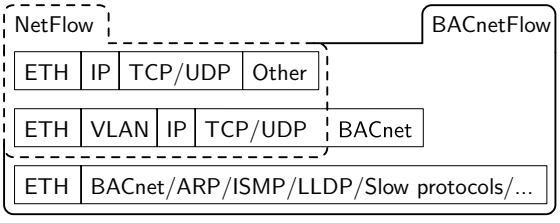

Fig. 5. Comparison of NetFlow and BACnetFlow coverage of packet information

Figure 5 shows the difference between BACnetFlow provided by the input plugin and standard NetFlow. In addition to NetFlow information, BACnetFlow provides information describing BACnet protocol.

BACnet filtering plugin is used to separate standard IP traffic from the rest of traffic processed by a BACnet input plugin. Common IP traffic is then exported by probe's standard NetFlow exporting plugin to the NetFlow collector, while BACnet data are processed by BACnet exporting plugin described below.

Originally, all flows including standard IP flows were processed by BACnet exporting plugin and stored in SQL database. This approach was not successful due to high amount of IP traffic that was hard to process by SQL database.

BACnet exporting plugin sends observed data to a storage for further analysis. The PostgreSQL database is currently used. To increase efficiency of database queries, the database partitioning is used. Commands for the database to add a new record are printed on the standard output by default. The output is redirected to the PostgreSQL interactive terminal (psql(1)) which sends database commands to the (remote) database server.

We are working on IPFIX export for a future use, which will enable to transport and store user-defined information elements. The IP flow and BACnetFlow information will be exported together this way.

Performance of the BACnetFlow probe was measured on a commodity PC[2]. The BACnet input plugin is able to process over 2 Mpps of BACnet traffic on each processor core. Furthermore, there can be multiple instances of the input plugin running simultaneously and processing the network traffic from dedicated input interfaces. The maximum packets per second (pps) rate on 1 Gbps network is 1,488,095 pps [15]. Thus, the proposed system using multi-core processor probe is able to process input data from several 1 Gbps fully saturated networks.

A bottleneck of the current implementation is a computation of the flow record hash which is implemented using OpenSSL MD5 hash functions. Performance of the BACnet input plugin can be further increased by reimplementing this part.

[2] Intel® Core™ 2 Duo CPU P8600 at 2.40 GHz with 4 GiB RAM running Linux kernel 3.1.0 for x86-64 hardware platform.

The limit of the BACnet exporting plugin is 63,000 processed BACnetFlows per second. Bypassing current connection with database via psql(1) and connecting the plugin directly to the database should increase the performance if needed. According to measured values (see Figure 12), there were only several tens of BACnetFlows per second in the monitored BMS network.

5 BACnet Measurement and Analysis

In this Section, we present measurement results to demonstrate the capabilities of the BACnet monitoring plugins and to provide information on the characteristics of BMS network in Masaryk University Campus. The results are organized in two categories. First, we present NetFlow version 9 statistics (e.g., traffic load, protocol breakdown and top statistics). These results are not unique to our measurement system. They can be obtained using standard NetFlow tools such as standalone probes, routers and collectors. However, these results are the first published traffic statistics from a large building network, and they show the impact of various systems connected to the network. The second category shows the BACnet statistics. These results show the native BACnet traffic, and they demonstrate the behaviour of control devices in a production network.

5.1 Deployment and Description of the Measurement System

BMS is an essential part of Masaryk University Campus. More than 24 teaching and research pavilions are monitored and controlled by BMS - dedicated LAN, BACnet over Ethernet and BACnet over IP network, interconnect several power systems, fire systems, security systems, data information systems, lighting, and so on. The network is managed from Windows servers and desktops through web user interface. Any system failure or attack against BMS can be critical for the entire Campus.

Our measurement system is connected to the mirror port (1 Gbps) of network core switch. The BMS management servers are located behind a firewall in a demilitarized zone. The management servers support BACnet stack and are able to access BACnet data. The mirror port can monitor traffic on up to 8 source ports. We selected the most significant ports to get as much as possible data from the monitored network. We generate non-sampled flow statistics using an active timeout 300 s and an inactive timeout 30 s.

Due to space limitation, we present week-long measurement results from January 16 12:00, 2012 till January 23 12:00, 2012. Week-long statistics were chosen in order to take into account time-of-day and day-of-week variations.

5.2 NetFlow Statistics

Table 1 summarizes the traffic observed in BMS network over one week using NetFlow version 9. We identified about 220 unique hosts (IPv4 addresses) in BMS network. NetFlow statistics do not include any BACnet traffic.

Table 1. Protocols observed with NetFlow version 9

Protocol	Bytes		Packets		Flows		bps	pps
TCP	3.6 T	100.0 %	3.6 G	99.6 %	533628	12.7 %	47.4 M	6013
UDP	814.0 M	0.0 %	6.6 M	0.2 %	2.5 M	60.6 %	10757	10
ICMP	722.4 M	0.0 %	7.0 M	0.2 %	1.1 M	26.1 %	9550	11
OSPF	25.6 M	0.0 %	191079	0.0 %	1990	0.0 %	338	0
PIM	4.6 M	0.0 %	61131	0.0 %	6435	0.2 %	60	0
IGMP	2.0 M	0.0 %	31509	0.0 %	14012	0.3 %	26	0
ICMP6	1.7 M	0.0 %	18362	0.0 %	1261	0.0 %	22	0
Total	3.6 T		3.7 G		4.2 M		47.4 M	6034

Figure 6 shows the traffic load. The majority of the traffic belongs to TCP video streams generated by closed-circuit television system (CCTV). Unfortunately, the video streams do not use well-known ports (see Figure 8). Instead, we use the domain names to identify and to verify the applications. In our case, the domain names are based on a host functionality such as DVR or CCTV. We observe a diurnal TCP pattern, as can be seen in Figure 8. To distinguish between dominant TCP and other protocols we use a logarithmic scale which makes the TCP diurnal pattern less visible (Figure 6).

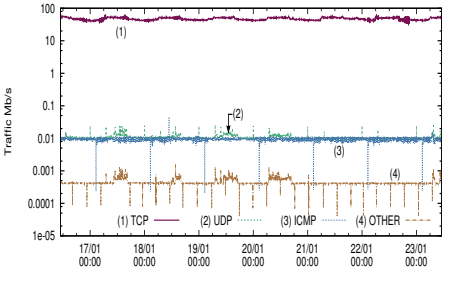

Fig. 6. Traffic load in megabits per second

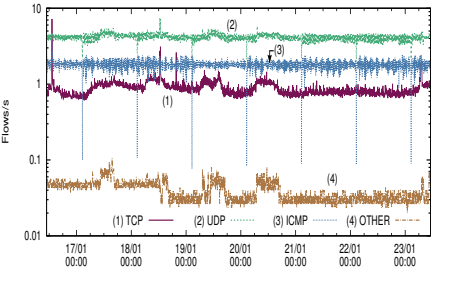

Fig. 7. Traffic load in flows per second

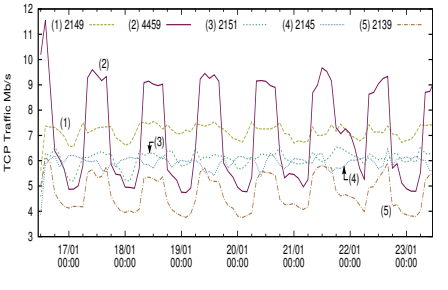

Fig. 8. TOP 5 dst TCP ports/bytes

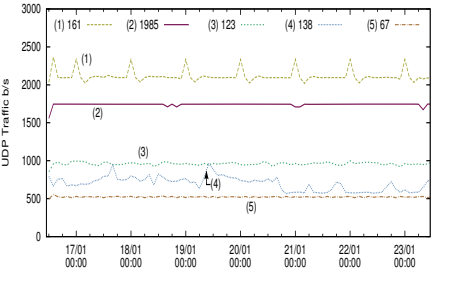

Fig. 9. TOP 5 dst UDP ports/bytes

Figure 9 shows UDP traffic. This traffic corresponds to well-known port numbers (165 - SNMP, 1985 - HSRP, 123 - NTP, 138 - NetBIOS, 67 - DHCP). UDP traffic is constant most of the time. Most of the flows are generated by UDP. The discrepancy in load (Figure 6) and flow (Figure 7) numbers shows the asymmetry based on the nature of the used applications.

We found that the ICMP traffic is generated by the monitoring tools checking the hosts availability. They use ping-like tools to send ICMP echo request packets. The remote host answer is carried by the echo reply message.

5.3 BACnetFlow Statistics

Table 2 summarizes the traffic observed in BMS network during one week using BACnetFlow. We include ARP and other link layer protocols (LLDP, ISMP) supported by BACnetFlow to show this typically invisible traffic in a standard NetFlow.

Table 2. Protocols observed with BACnetFlow

Protocol	Bytes		Packets		Flows		bps	pps
BACnet/IP	7.2 G	53.9 %	79.5 M	52.9 %	5.3 M	38.1 %	95.2 K	131.4
BACnet/Eth	5.4 G	40.5 %	59.8 M	39.7 %	6.2 M	44.6 %	71.4 K	98.9
ARP	0.68 G	5.1 %	10.5 M	7.0 %	1.8 M	13.0 %	8995	17.4
Other	63.7 M	0.5 %	0.6 M	0.4 %	0.6 M	4.3 %	105	1
Total	13.3 G		150.4 M		13.9 M		175.7 K	248.7

Figure 10 shows the BACnet traffic load. We identified 42 BACnet over IP devices (IPv4 addresses), 103 BACnet over Ethernet devices (MAC addresses), 63 BACnet networks and 201 BACnet addresses in the BMS network. We observe that both BACnet protocols have similar characteristics. We suspect this is due to evolution of the BMS network. The Campus construction took place in several stages. In each stage the network evolved and new approaches were used. Early BACnet over Ethernet installations are now connected through BACnet over IP gateways. 12 virtual LANs are used to transport the traffic in BMS. This makes the observation even trickier.

We observe distinct diurnal and weekly patterns for BACnet traffic in Figures 10 and 11. The load comes up during the business hours. On the weekend and at nights, the traffic is constant and does not exhibit clear pattern.

Figures 12 and 13 show the flow statistics. The traffic load peaks (busy hours) do not necessarily translate in the high number of flows in Figure 12. The results in Figure 13 show distribution of packets per flow. We observe a large number of flows with a small number of packets. Number of single packet flows (SPF) is further shown in Figure 14.

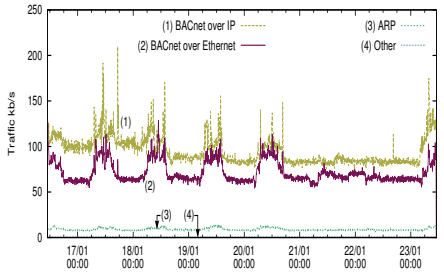

Fig. 10. Traffic load in kilobits per second

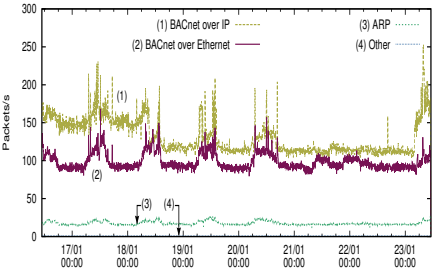

Fig. 11. Traffic load in packets per second

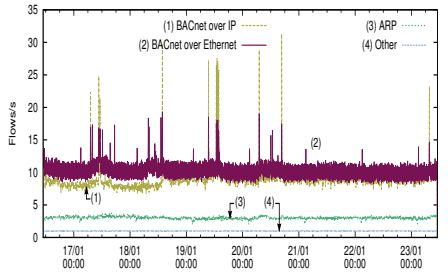

Fig. 12. BACnet flows per second

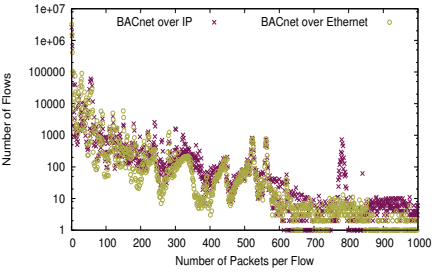

Fig. 13. BACnet packets per flow

We found out that the maximum transmission unit (MTU) is about 500–550 octets (see Figure 14). This corresponds with BACnet over MS/TP (master-slave/token-passing) which uses the maximum NPDU of 501 octets. MS/TP is used to connect the "last mile" devices of building infrastructure (RS-485 bus).

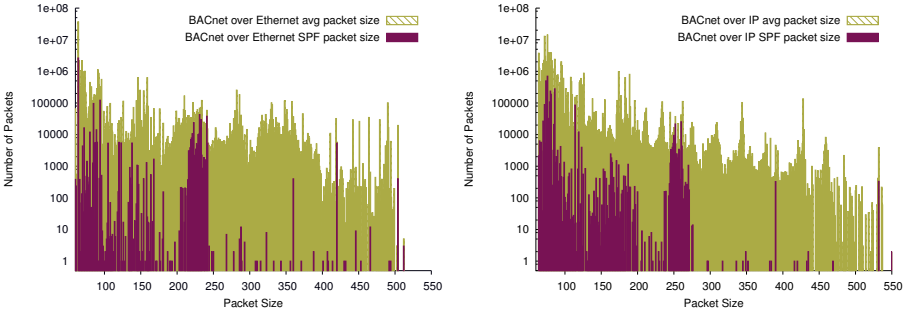

Fig. 14. BACnet average packet size and single packet flow (SPF) size

The BACnet TOP talkers are shown in Figure 15. It proves that BACnet traffic uses Ethernet and IP broadcasting heavily. Example of such traffic is *Who-Is* message used to discover all accessible BACnet devices.

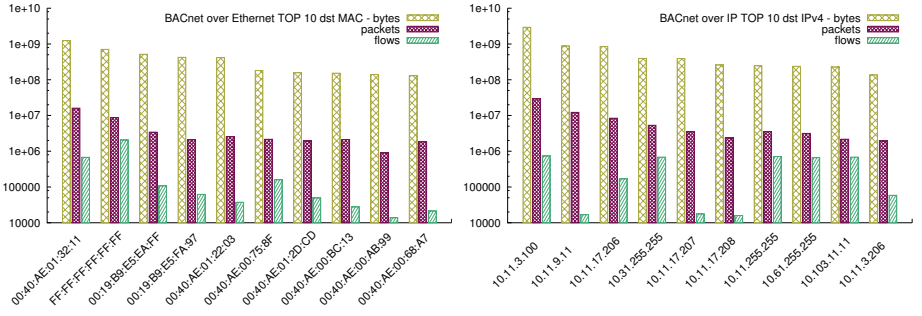

Fig. 15. BACnet TOP 10 destination addresses / bytes

Figure 16 shows the BACnet over Ethernet TOP 10 source and destination networks. Both TOP networks are not specified. Other BACnet packet header fields are used to identify a communication source or destination.

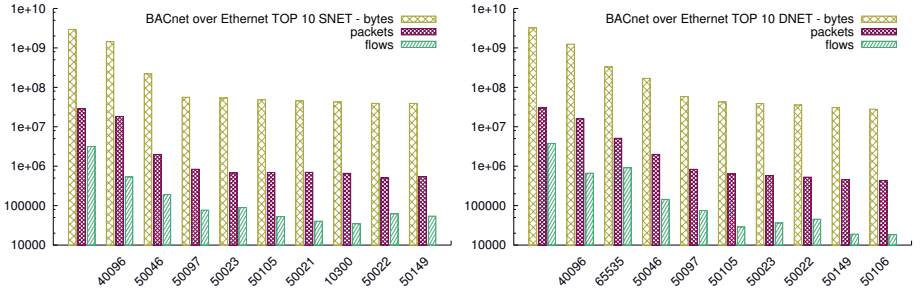

Fig. 16. BACnet over Ethernet TOP 10 source and destination networks / bytes

6 Summary

We introduced BACnetFlow as BMS networks' equivalent of the IP flow. We described innovative system for observing and storing BACnetFlow information in the environment of the BMS networks. We presented the observation results and experiences of using such system for monitoring the Masaryk University Campus.

In contrast to [8], our measurement results include diurnal patterns (see Figure 10). While Barbosa is monitoring highly automatic SCADA network with a low level of human activity, our BMS network is closely connected with a human activity in the university campus. We deduce, that a network traffic profile of an automation network depends on a way how it is used.

The pilot system deployment serves to prove the concept of flow-based monitoring in BMS networks. It will be further extended to support IPFIX collection

instead of currently used SQL database back-end. Currently, we have a flow-based profile of the whole network. Furthermore, we plan to validate anomaly detection techniques in the special environment of BMS and SCADA networks. In the long term, the goal of our research effort is to identify which metrics should be monitored in real-time to provide situational awareness in BMS networks.

Acknowledgments. This material is based upon work supported by Masaryk University and also supported by the "CESNET Large Infrastructure" project LM2010005 funded by the Ministry of Education, Youth and Sports of the Czech Republic.

References

1. Security Predictions 2012&2013 – The Emerging Security Threat, http://www.sans.edu/research/security-laboratory/article/security-predict2011
2. Cisco IOS NetFlow, http://www.cisco.com/go/netflow
3. Claise, B.: Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. RFC 5101 (Proposed Standard), IETF (2008), http://tools.ietf.org/html/rfc5101
4. American Society of Heating, Refrigerating and Air-Conditioning Engineers: Standard 135-2010 – BACnet A Data Communication Protocol for Building Automation and Control Networks. ASHRAE (2010)
5. BACnet Website – ASHRAE SSPC 135, http://www.bacnet.org
6. The new Masaryk University Campus, http://www.muni.cz/kampus?lang=en
7. Nagios – The Industry Standard In IT Infrastructure Monitoring, http://www.nagios.org/
8. Barbosa, R.R.R., Sadre, R., Pras, A.: Difficulties in Modeling SCADA Traffic: A Comparative Analysis. In: Taft, N., Ricciato, F. (eds.) PAM 2012. LNCS, vol. 7192, pp. 126–135. Springer, Heidelberg (2012)
9. Novak, T., Treytl, A., Palensky, P.: Common approach to functional safety and system security in building automation and control systems. In: IEEE Conference on Emerging Technologies and Factory Automation, pp. 1141–1148 (2007)
10. Granzer, W., Kastner, W., Neugschwandtner, G., Praus, F.: Security in networked building automation systems. In: IEEE International Workshop on Factory Communication Systems, pp. 283–292 (2006)
11. Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V., Culler, D.E.: SPINS: security protocols for sensor networks. Wireless Networks, 189–199 (2001)
12. Honeywell selects Tofino Modbus Read-only Firewall to Secure Critical Safety Systems, http://www.tofinosecurity.com/article/honeywell-selects-tofino%E2%84%A2-modbus-read-only-firewall-secure-critical-safety-systems
13. INVEA FlowMon Exporter – Community Program, http://www.invea-tech.com
14. BACnet Monitoring Plugins, http://dior.ics.muni.cz/~celeda/bacnet/
15. How many Packets per Second per port are needed to achieve Wire-Speed?, http://kb.juniper.net/InfoCenter/index?page=content&id=KB14737
16. BACnet over IP, http://www.bacnet.org/Tutorial/BACnetIP/default.html
17. IP Flow Information Export (IPFIX) Entities, http://www.iana.org/assignments/ipfix/ipfix.xml