Research Article **ISSN: 2393 – 9532**

International Journal of Arts and Science Research

Journal home page: www.ijasrjournal.com

FRAME ANALYSIS USING WIRESHARK AND TOPAS IN INDUSTRIAL INTERNET OF THINGS (IIOT) INDUSTRY 4.0

Om Prakash Yadav*[1] and V. V. R. Raman[2]

[1*]Research Scholar, CSE Department, Enrolment No: SSSCSE1515, SSSUTMS- Sehore, M.P, India.
[2]Department of Computer Science, Aurora's Degree and PG College, Hyderabad, India.

ABSTRACT

The acquisition and analysis of network packets are performed using the Wireshark. The adoption and deployment of "Internet of Things" (IoT) technologies is leading to the new era of industry 4.0 including greater connectivity to industrial systems. The key changes brought about Industry 4.0, and describe how the Industrial Internet of Things will affect your businesses, your governments, as well as your lives. Today's, in the industry 4.0 developments in neuroscience, 3D Printing, Mobile Networking and Computing. This paper reviews what is meant by Industrial IoT (IIoT) and Industry 4.0 and analysis frame using TOPAS and Wireshark. The Industry 4.0 improves production efficiency with quality, visibility, production optimisation and higher manufacturing responsiveness. Exported packets records are received by the real-time network analysis frame TOPAS and examined by the open-source network analyser Wireshark. The Industrial Internet of Things (IIoT) is not about breaking out recent automation systems in instruction to switch them with new ones. The IIoT lies in the ability to link automation systems with enterprise planning, scheduling and production of product lifecycle systems.

KEYWORDS

Frame, Industry 4.0, Internet of Things (IoT), IIoT, Wireshark and TOPAS.

Author for Correspondence:

Om Prakash Yadav,
Research Scholar, CSE Department,
Enrolment No: SSSCSE1515,
SSSUTMS- Sehore, M.P, India.

Email: yad.omprakash@gmail.com

INTRODUCTION

The aims of this paper are to improve on existing definitions of Industrial IoT (IIoT) and to propose a framework for IIoT components as a basis for analysing the use and deployment of IoT technologies in industrial settings. The IIoT devices and their uses, which is to be used as part of a vulnerability and threat analysis process for these devices. By being able to characterise the devices in a systematic manner, we anticipate being able to analyse cross-cutting threats and vulnerabilities and

identify patterns that may be obscured when focusing on the technology employed or sector specific issues.

The Industrial Internet of Things (IIoT) is frequently presented as a rebellion that is changing the face of industry in a profound manner. In reality that IIoT is a progress that has its origins in technologies and functionalities developed by visionary automation suppliers more than 20 years ago. As the necessary global standards mature, it may well take another 18 years to realise the full prospective of IIoT.

The appearance of the IIoT megatrend has created both hope and confusion among stakeholders responsible for operating industrial plants. Much of the early publicity is focused on the impact of technological improvements on existing automation platforms. However, one of the challenges in understanding the probable of IIoT is the very large scope of applications. In the area of smart enterprise control, for example, we will see self-organizing machines and belongings that enable mass customization and lot sizes of one. In the empire of asset performance, the collection and analysis of data from increasing intelligent sensors and numbers of cost-effective will increase business concert and asset uptime.

Wireshark

Wireshark is the network packet protocol analyzer. It is used for, analysis and troubleshooting development. Wireshark is an open-source analyzer which is designed by Gerald Combs and it can runs in Windows and UNIX platforms.

Wireshark implements a range of filters that facilitate the definition of search criteria and currently supports over 12004 protocols (version 3.0.1)[1].

Live data can be read from many types of network including Ethernet, IEEE 802.11, PPP, and other interfaces. Captured files can be programmatically converted or edited via command line switches to the "edit cap" program.

Wireshark will typically display information in three panels. The top panel lists frames independently with key data on a single line. The single frame selected in the top pane is further explained in the tool's middle panel. In this section of the display which is shows packet details, exemplifying how various aspects of the frame can be understood as belonging to the data link layer, network layer, transport layer or application layer. Finally, Wireshark's bottom pane displays the raw frame, with a hexadecimal rendition on the left and the equivalent ASCII values on the right[2,3].

Feature

- Available for UNIX and Windows
- Capture live packet data in network.
- Display packets with very detailed protocol information.
- Open and Save packet data captured.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria.
- Search for packets on many criteria.
- Colorize packet display based on filters.
- Create various statistics.

INDUSTRIAL INTERNET OF THINGS (IIoT)

The industrial internet of things (IIoT) is the use of smart devices and technology to actuators and enhances manufacturing and industrial processes and known as the industrial internet or Industry 4.0.The IIoT is the powerful machines and real-time analytics to take advantage of the data that dumb machines have produced in industrial settings for years. The powerful philosophy behind IIoT is that smart machines is not only better than humans for communicating but also to capturing and analysing data in real time that can be used to drive business decisions faster and more precisely.

The Industrial IoT (IIoT) will transform how companies production and distribute products, impacting everything from the supply chain to the factory floor to the logistics of shipping, receiving, and maintaining products once they have left the premises. IIoT will open up new markets. It will disrupt existing systems including long-standing partner and supplier relations and produce totally new inexpensive predicaments[4].

IIoT is the use of IoT technologies in manufacturing and is part of the Industry 4.0 trend. In industry the machine learning, big data technologies, sensor data, and M2M communication and automation

technologies. The philosophy behind IIoT, according to Tech Target, is that "smart machines are better than humans at accurately, consistently capturing and communicating data[4].

The first three industrial revolutions are characterised as being driven by mechanical production relying on water and steam power, use of mass labour and electrical energy, and the use of electronic, automated production respectively[5]. Whilst the supposed fourth industrial revolution ('Industry 4.0') was first proposed in 2011 in the context of the goal of developing the German economy[1]. This revolution is characterised by its reliance on the use of CPS capable of communication with one another and of making autonomous, de-centralised decisions, with the aim of increasing industrial efficiency, productivity, safety, and transparency.

The term "Industry 4.0" to refer to a function industrial revolution with for characteristics is Vertical network, Horizontal Integration, through - engineering, Acceleration through exponential technologies. The introduction of the IoT and Services into the manufacturing environment is leading in a fourth industrial revolution. "The Industry 4.0 is new type of industry is based on model of Smart Enterprise, i.e. Smart Factory"[6]. "The IIoT manufacturing is holds great prospective for quality control, justifiable and great practices, supply chain traceability and overall supply chain productivity"[7].

HOW IIOT WORKS

IIoT is a network of smart devices connected to from systems that monitor, collect, exchange and analyze data. Each industrial IoT echosystem consists of:

- Intelligent assets that can sense data and store it.
- Public and/or private data communications infrastructure.
- Use applications to analysis the generate business information from raw data; and People.

According to Weyer *et al.*[8] in industry 4.0 fields devices, machines, production modules and products are comprised as Cyber-Physical Systems (CPS) that are autonomously exchanging information, triggering actions and controlling each other independently.

Framework

The framework that allows us to analyse the nature of IIoT devices and their uses, which is to be used as part of a vulnerability and threat analysis process for these devices. The specific limitations of the taxonomies can be summarised as follows [4/5/18]

1. The device-centric taxonomy.
2. The IoT stack-centric taxonomy.
3. The IoT sensor taxonomy.
4. The IoT-based smart environment taxonomy.
5. The IoT architecture taxonomy.
6. The Industrial Internet of Things taxonomy.
7. The domain or sector-based IoT taxonomies.

METHOD TO ANALYSIS FRAME

Topas

Traffic flow and Packet Analysis System. TOPAS integrates a collector which receives monitoring data exported by routers, switches and monitoring probes using Cisco Net flow[9], IPFIX (IP Flow Information eXport)[8] or PSAMP (Packet SAMP ling)[10] protocol. TOPAS provides a framework for modules that process and analyser the received monitoring data in real-time. Wireshark interface implemented on a module which transforms packet data received from PSAMP and Flexible Net flow[2] exporters into a stream of frames inp-cap format. Wireshark is enough capable to read this p-cap stream from a UNIX pipe and to perform continuous packet inspection and protocol analysis just as if the program was running directly at the observation point. To capturing the frames and exporting per-packet information cause a significant processing load at the monitoring devices.

In Figure No.3, the Wireshark and TOPAS with Monitor Manager complements the talent to configure the capturing and export of packet information according to the requirements of the network analysis. Presently, the software monitoring review Vermont[11] is the only PSAMP implementation that supports remote configuration with Netconf. In[6], we evaluated the performance of TOPAS with respect to the maximum number of IP

Flow Information eXport packets and flow records that can be processed without losses, depending on the number of active detection modules. With one active module, we successfully tested rates of 35,000 IPFIX packets and 220,000 records per second.

RESULT ANALYSIS

For evaluating the performance of the TOPAS/Wireshark setup presented. We conducted additional experiments using PSAMP data. In the test setup, Vermont captured traffic from a monitoring port of a Gigabit Ethernet switch and exported packet records having a variable length field with the first 128 bytes. Each captured packet, and a timestamp of it indicating when the packet was perceived. An exported PSAMP packet included a maximum of 12 packet records in order to avoid IP fragmentation (in UDP). The TOPAS and Vermont were running on two dual processor Linux PCs.

The Management Information Base (MIB) and Remote Network Monitoring (RMON)[12]. Enables distributed network analysis using monitoring devices of different manufacturers in a standardized way. Switches and routers supporting RMON generate traffic statistics that can be queried using SNMP (Simple Network Management Protocol).

Wireshark

The IETF has been developing techniques for selecting individual packets at an observation point and exporting packet data to a remote analyser using PSAMP working group[13]. The PSAMP[3] makes use of the IPFIX protocol[8] to export packet records including header and payload information of the selected packets. The flow records, a packet record contains a time stamp that indicates when the packet was detected, and a set of packet header fields.

TOPAS[6] was developed by *Diadem Firewall* in the European project[11] where it has been deployed for real-time attack and anomaly detection based on flow records. The Wireshark run within TOPAS, we extended the collector to receive and process packet data.

CAPTURING PACKETS

To start the packet capturing process, click the Capture menu and choose Start. Wireshark will continue capturing and displaying packets continue the capture buffer is not fills up. The buffer is 1 Mbytes by default. The packet capture will show the details of each packet as they were sent over the wireless LAN. Figure No.2 have capture window on a screenshot of a sample packet. The window identifies each packet's source and destination nodes, protocol implemented, and information about each packet in top panel.

Filtering Packets

From the menu, click on 'Capture –> Interfaces', which will display the following screen.

Source and Destination IP Filter

A source and destination filter can be applied to restrict the packet view in Wireshark to only those packets that have source IP as mentioned in the filter. The filter applied on: ip.src=192.168.1.1&ip.dst == 192.168.1.1

Filter by Protocol

It's very easy to apply filter for a particular protocol. Using this filter: http

Using OR /AND Condition in Filter

Filtering the packets that match either one or the other condition. Exam: http &&ip.src==192.168.1.4, filter: http||arp,

Filter by Port Number

It can also a apply filter based on port number. filter: tcp.port= 82

RESULT ANALYSIS

Wire shark is a very powerful tool. It is use to examine security problems, debug network protocol implementations, and inspect network protocol internals.

The Input / Output graph will show you the throughput of all traffic in the trace file, in both directions. The basic graphics can be gained under the "IO graphs" section. One or more graphics can be added in the same window on a per display filter base.

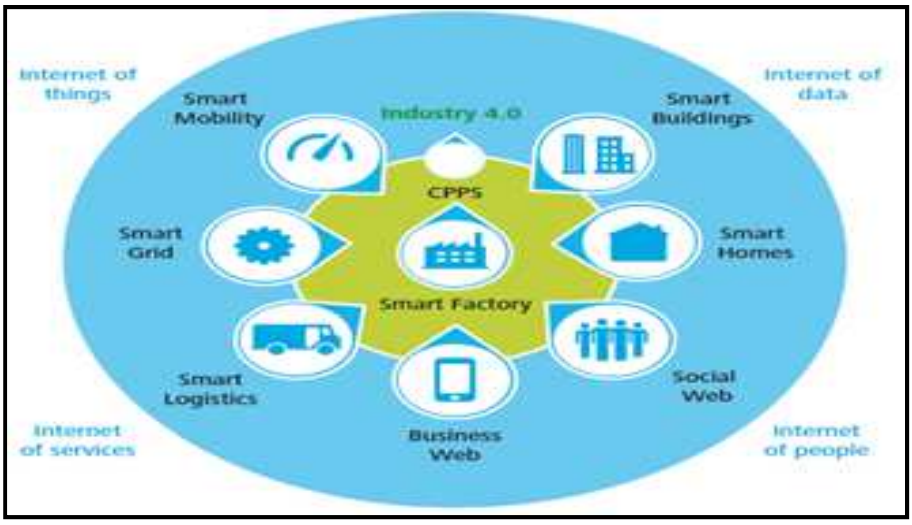

Figure No.1: The Industry 4.0 environment

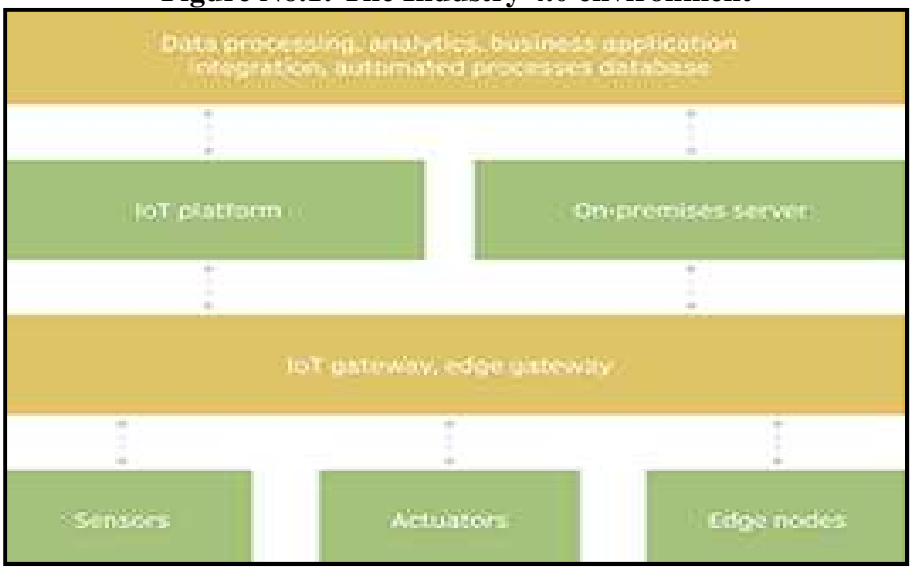

Figure No.2: IIOT Infrastructure

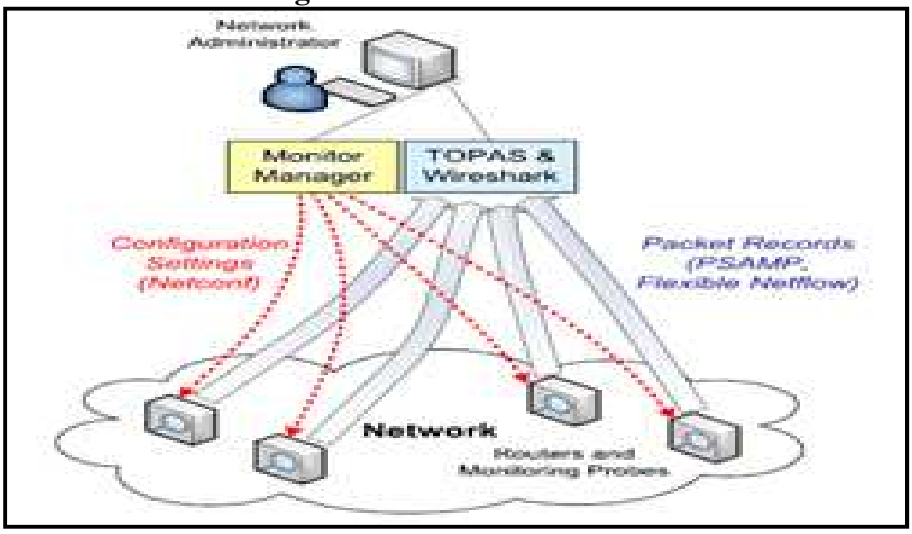

Figure No.3: Implementation of TOPAS and Wireshark

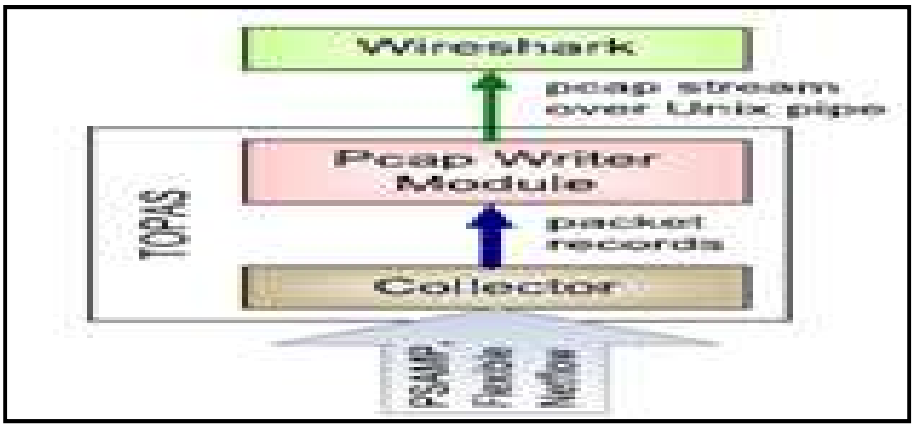

Figure No.4: TOPAS and Wireshark

Figure No.5: After capturing the packet by Wireshark

Figure No.6: Filter the frame based on IP address

Figure No.7: Analysis the selected packets

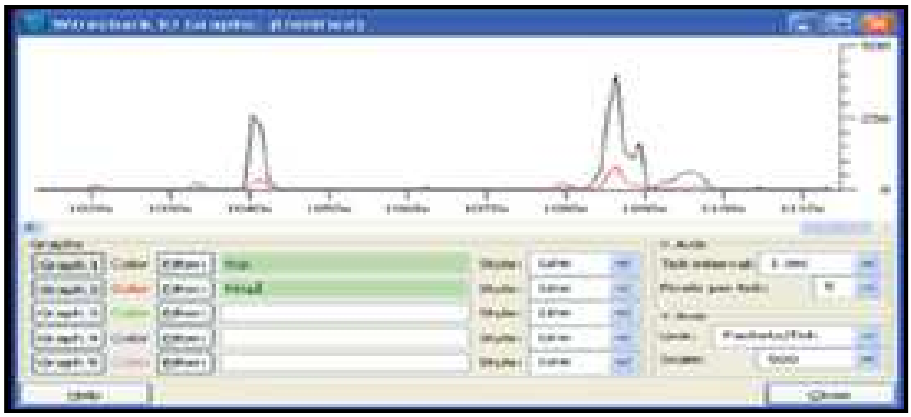

Figure No.8: IO Graph

CONCLUSION

Our solution broadens the Field of application of Wire shark and overcomes its conceptual limitation of only being able to inspect local traffic. As PSAMP is in the final phase of standardization, and as Flexible Net flow is already available on the market, we expect capturing and exporting packet information to become a commonplace functional extension. The major drawback of our solution is that in high-speed networks, we need to restrict the traffic analysis to specific packet streams. Otherwise, the amount of monitoring data threats exceeding the available bandwidth between the exporter and the collector, resulting in packet losses or intolerable high delays. In this respect, distributed network analysers have the advantage that they only export reports with analysis results which can be much smaller than the examined packet data. Concluding the discussion, let us denote that the proposed architecture and implementation is not limited or specific to the utilization of Wireshark. There are many other programs and tools which are able to receive and process p-cap data generated by the p-cap writer module. We have successfully deployed Snort IDS within the TOPAS framework in instruction to perform signature detection on packet records.

ACKNOWLEDGEMENT

The authors which to express their sincere gratitude to Department of IT, ISL Engineering College, Hyderabad, India for providing necessary facilities to carry out this research work.

CONFLICT OF INTEREST

We declare that we have no conflict of interest.

BIBLIOGRAPHY

1. Munz G, Weber N and Carle G. Signature Detection in Sampled Packets, *in Proc. of IEEE Workshop on Monitoring, Attack Detection and Mitigation (MonAM 2007), Toulouse, France,* 2007, 1-6.
2. Cisco Systems, Introduction to Cisco IOS Flexible Net Flow, *White Paper,* 2008. [Online]. Available: http://www.cisco.com
3. Diadem Firewall Homepage, http://www.diadem-_rewall.org, 2007.
4. Enns R, Bierman A, Crozier K, Goddard T, Lear E, Shafer P, Waldbusser S and Wasserman M. NETCONF Con_guration Protocol, *RFC 4741 (Standards Track),* 2006.
5. Zseby T, Molina M, Duf_Eld N, Niccolini S and Raspall F. Sampling and Filtering Techniques for IP Packet Selection, *Internet-Draft, work in progress, draft-ietf-psamp-sample-tech-10,* 2007.
6. Dorsemaine B, Gaulier J P, Wary J P, Kheir N, Urien P. Internet of things: a definition and taxonomy, *Proc. - NGMAST 2015 9th Int. Conf. Next Gener. Mob. Appl. Serv. Technol,* 2016, 72-77. http://dx.doi.org/10.1109/NGMAST.2015.71.
7. https://www.tatateleservices.com/articles/the-six-applications-and-benefits-of-iot-in-manufacturing

8. Claise B, Bryant S, Sadasivan G, Leinen S, Dietz T and Trammell B H. .Speci_cation of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traf_c Flow Information, *RFC 5101 (Proposed Standard),* 2008.
9. Claise B, Sadasivan G, Valluri V and Djernaes M. Cisco Systems Net Flow Services Export Version 9 RFC 3954 (Informational), 2004.
10. Duf_Eld N, Chiou D, Claise B, Greenberg A, Grossglauser M, Marimuthu P, Rexford J and Sadasivan G. A Framework for Packet Selection and Reporting, *Internet-Draft, work in progress, draft-ietfpsamp- framework-12,* 2007.
11. Lampert R T, Sommer C, M¨unz G and Dressler F. Vermont - A Versatile Monitoring Toolkit for IPFIX and PSAMP, in Proc. Of IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (Mon AM 2006), *Tuebingen, Germany,* 2006.
12. Yaqoob I. *et al*. Internet of things architecture: recent advances, taxonomy, requirements, and open challenges, *IEEE Wireless Commun,* 24(3), 2017, 10-16.
13. Joseph, Roshan S Y. Smart parking system using wireless sensor networks, *SENSORCOMM 2012, The sixth international conference on sensor technologies and application*, ISBN: 978-1-61208-207-3, 2012, 306-311.
14. Claise B, Quittek J and Johnson A. Packet Sampling (PSAMP) Protocol Speci cations, *Internet-Draft, work in progress, draft-ietfpsamp- protocol-09,* 2007.
15. Beecham Research, M2M Sector Map, 2014. Available: http://www.beechamresearch.com/ download. aspx?id=18.
16. Ahmed E. *et al*. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges, *IEEE Wireless Commun,* 23(5), 2016, 10-16.
17. Four Use Cases Show Real-World Impact of IoT 2016 by TDWI, a division of 1105 Media, Inc.
18. Munz G and Carle G. Real-time Analysis of Flow Data for Network Attack Detection, *in Proc. of IFIP/IEEE Symposium on Integrated Management (IM 2007), Munich, Germany,* 2007.
19. Kaivan Karimi and Gary Atkinson. What the Internet of Things (IoT) Needs to Become a Reality, *White Paper, Free Scale and ARM,* 2013.
20. Schneider S. The industrial internet of things (IIoT), in: H. Geng (Ed.), *Internet of Things and Data Analytics Handbook, John Wiley and Sons, Inc., Hoboken, NJ, USA,* 2017. http://dx.doi.org/10.1002/9781119173601.ch 3.
21. John Conway. The Industrial Internet of Things: An Evolution to a Smart Manufacturing Enterprise, 1-15.

Please cite this article in press as: Om Prakash Yadav and Raman V V R. Frame analysis using wireshark and topas in industrial internet of things (IIOT) industry 4.0, *International Journal of Arts and Science Research,* 6(1), 2019, 4-11.