Wireless Handover Performance in Industrial Environments: a Case Study

Jetmir Haxhibeqiri, Michael Mehari, Wei Liu, Eli De Poorter, Wout Joseph, Ingrid Moerman, Jeroen Hoebeke
Ghent University – iMinds, Department of Information Technology (INTEC)
Technologiepark-Zwijnaarde 15, 9052 Ghent, Belgium

***Abstract*—Wireless communication is an enabling technology for industrial automation. For mobile industrial devices operating in large areas, the performance of the wireless handover process is crucial. For the welfare of industrial processes short time communication outage must be ensured, especially for time-critical traffic. This paper assesses the handover performance for three industrial real-life use cases with different requirements. It covers handover performance under heavy interference, its impact on time-critical traffic and on broadcast traffic latency, followed by lessons learned and opportunities for further research.**

Keywords—handover; IEEE 802.11, industrial environment; mesh network; iPCF; iPCF-MC; Bluetooth;

I. Introduction

Industry is continuously looking for ways to further automate processes, improve efficiency, reduce energy consumption, increase economic benefits, improve working conditions, etc. This ongoing evolution is often referred to as Industry 4.0 [1], where everything becomes connected to a network by means of communication infrastructure. Wireless technology is seen as an important enabling technology. Compared to wired solutions, it enables device and personnel mobility, reduces installation cost, enables to connect hard-to-reach areas, etc. To provide wireless communication, a variety of technologies exists, with IEEE 802.11 or Wi-Fi as one of the key technologies being considered in this paper.

Wireless communication will become increasingly important for the welfare of industrial processes, but is challenging at the same time. Since most of the industrial environments are large areas like warehouses or production halls, multi access point (AP) systems must be used to provide coverage across the entire area and mobile devices must switch from one AP to another while moving around, called handover. Further, industrial environments are challenging and vulnerable which might result in coverage holes, packet losses and communication outage. A majority of the industrial communication traffic is time sensitive implying strict latency requirements, including fast handovers. On top of this, by deploying new wireless systems in the same frequency band, interference will increase for previously installed wireless systems, resulting in problems especially during handover.

Within this challenging context, robust and reliable wireless communication must be realized. In this paper we focus on mobile industrial devices such as Personal Digital Assistant (PDA), Automated Guided Vehicles (AGV) and cranes, which all rely on performant handovers for their proper operation. Three different use cases are being considered: a) handovers of Wi-Fi PDAs with Bluetooth voice communication used by workers in a warehouse for order picking, b) handover of a crane generating time-critical PLC traffic for safety purposes and c) handover of AGVs generating time-critical broadcast traffic. For every use case, we experimentally assess the handover performance in a real-life environment or using real industrial hardware and pinpoint problems that will be experienced. Where possible, we highlight potential mitigation issues. If not, we identify opportunities for further research.

The remainder of this paper is organized as follows. Section 2 provides the reader with the necessary background on Wi-Fi handovers. Next, sections 3 to 5 will present an analysis of the handover performance for each of the three use case, followed by a discussion on possible solutions or research opportunities. Finally, the last section concludes the paper and summarizes the research outlook.

II. Wireless Handovers

Larger industrial sites require multi-AP systems. In case a mobile node reaches the boundary of the coverage area of the AP it is connected to, it needs to perform a handover to reconnect to a new AP which takes over the communication. When the need for a handover arises (e.g. when the RSSI drops below a certain threshold), the node - while transmitting data towards the old AP - will probe for new APs with higher RSSI. As soon as it finds a better AP it takes the decision to perform a handover. First it exchanges the association and authentication packets with the new AP. Only after that it will be able to continue sending data. In case of the extended authentication protocol it also needs to send the EAPoL-Key packets to the new AP, which increases the handover time. The complete procedure is shown in Figure 1.

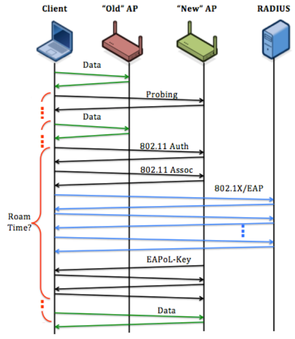

Fig. 1. Handover procedure.

III. Wireless Handover under Heavy Interference

A. Use case description

The first use case considered is the warehouse of a large manufacturing company. The warehouse, having a size of 415 by 200 meters, is equipped with 60 light-weight APs under the supervision of a central controller, operating in 3 non-overlapping Wi-Fi bands (channel 1, 6 and 11). This way, an IEEE 802.11g compliant network in the 2.4GHz band with coverage across the entire warehouse is realized. Workers in the warehouse are driving around with forklifts and make use of a PDA that is connected to the Wi-Fi network in order to assist them in the order picking process. The PDAs need to perform frequent handovers in order to maintain connectivity. At a certain moment, the company decides to further speed up logistical processes, and additionally equips their workers with a Bluetooth (BT) headset for voice assisted order picking. As both technologies are operating within the same 2.4GHz frequency band, these newly added BT devices may interfere with the existing Wi-Fi network, resulting in coexistence problems. Initially, coexistence problems were fully absent. Only at a later stage, after scaling up the number of voice picking systems, coexistence problems started to manifest themselves, resulting in Wi-Fi connectivity interruptions.

B. Problem assessment

In order to discover the root cause of the Wi-Fi connectivity problems, we applied several monitoring tools at the industrial site starting with a spectrum analyzers and BT and Wi-Fi traffic analyzers. In Figure 2 the spectrum occupancy of the 2.4 GHz band is shown, clearly illustrating a heavily used Wi-Fi network, but also strong BT interference.

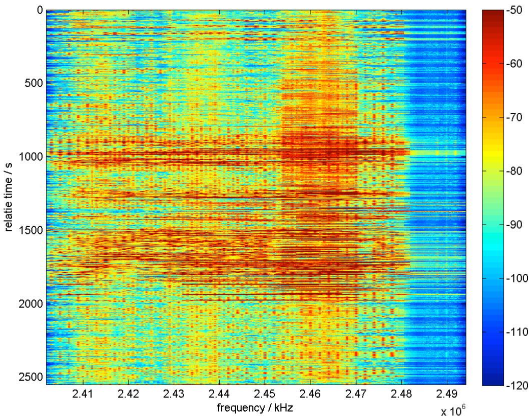

Fig. 2. Spectrum usage for 2.4 GHz band under Bluetooth interference.

Next, in order to find out how the BT interference exactly impacted the Wi-Fi connectivity, we deployed a WPA-supplicant enabled laptop at a fixed location that was pinging 2 factory servers every 1s, while being forced to roam between 3 APs every 10s in order to mimic the behavior of the PDAs. The WEP/PEAP authentication method was used in the factory Wi-Fi network. In order to measure the handover performance, Wi-Fi packets were sniffed. The packets per tick of both ICMP and handover traffic are shown as a moving average in Figure 3. The discontinuity in the ICMP traffic (white spaces between the black bars) was due to a long or failed handover procedure. On top of the long scanning time, the large server certificates used by the WEP/PEAP authentication method were easily corrupted due to the strong BT interference. This severely decreased the chance on a successful handover and resulted in the observed Wi-Fi connectivity problems.

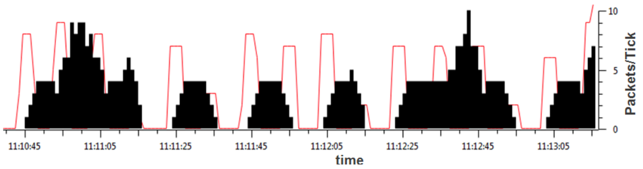

Fig. 3. Handover performance under Bluetooth interference. The Black bar indicates the ICMP traffic whereas the red curve shows the roaming traffic.

C. Problem mitigation, detection and prevention

As BT is continuously hopping from one channel to another, longer Wi-Fi packets will exhibit a higher probability to be corrupted. Therefore, one way of mitigating the failed handover activities is by changing the handover procedure to one that uses less and/or smaller packets (e.g. using EAP-FAST), at the expense of reduced security. This could partially solve handover difficulties, but company policies might not allow this. In line with this, one could lower the Maximal Transmission Unit of the network in order to reduce the size of all packets transmissions. Also, if supported by the devices, the BT transmission power could be lowered. These approaches can only partially mitigate the problem, as they cannot solve the root cause, namely BT and Wi-Fi interfering.

To fully avoid interference, more drastic networking reconfigurations are needed. For instance, Wi-Fi APs could be configured to only operate in 2 out of 3 non-overlapping bands, combined with adaptive BT frequency hopping (BT hopping within in the band not used by Wi-Fi). Again, the feasibility of the latter is fully dependent on the capabilities of the end devices. Alternatively, the company could move to a 5GHz Wi-Fi. However, due to legacy reasons (i.e., old equipment that does not support 5 GHz), such a solution is not always feasible. In addition, it might result in coverage problems as the network has been planned for 2.4GHz.

Several of the above mentioned measures cannot be realized due to the absence of the required device capabilities or the lack of interfaces to make appropriate reconfigurations. Another thing that has been observed is how difficult it is to pinpoint the exact cause of a network problem. End devices are closed boxes that do not incorporate appropriate diagnostic tools. At the AP side, there is an overload of logging data, which cannot be easily analyzed. To automatically understand the cause of the wireless network problem, APs together with clients should generate a collection of easy-to-understand network performance maps besides their normal operation.

Finally, ideally, companies should be able to assess prior to the deployment of a new wireless technology to what extend it can impact the proper functioning of an existing network. Today, no multi-technology planning tools (e.g. BT and Wi-Fi) that allow such an assessment exist. As part of our research, we are designing a Software Defined Radio that is able to emulating different BT traffic patterns. This way, the potential impact can be assessed in a cost-efficient way, without the need to deploy multiple BT devices.

IV. Time-critical PLC traffic

A. Use case description

The second use case considers a large industrial stockyard surrounded by a safety fence, where a moving crane is responsible for handling goods. A PLC is monitoring all entry points (gates) and communicates continuously with a PLC on the crane. If someone enters during operation of the crane or communication is interrupted during 100ms, the crane stops and a manual intervention is needed. In addition, due to the size of the stockyard, multiple APs are needed, requiring fast handovers. Further, packet loss and outage times should be kept low. Standard wireless roaming techniques have been analyzed, but fail to continuously meet the requirements. Therefore, state-of-the-art industrial APs and clients from Siemens have been deployed and evaluated in order to see whether they can support time-critical PLC traffic in the presence of handovers. These devices implement two proprietary extensions to the IEEE 802.11 standard, Industrial Point Coordination Function (iPCF) and iPCF with Management Channel (iPCF-MC), aiming to improve and guarantee fast handover for industrial communication [2]. As in normal 802.11 PCF techniques [3], the AP coordinates the communication within the cell by sending polling messages to the clients. With iPCF the AP cyclically scans all nodes in the cell every 5ms. At the same time it includes the downlink traffic for the clients, while the uplink traffic can be incorporated in the client reply. If a client does not receive a frame from an AP within a certain time window it will start the handover process. The iPCF-MC mode uses APs with two wireless interfaces, one to be used for data traffic and the other for management traffic. The latter will use the same channel in the whole network, enabling the client to receive beacons from all APs in range and selecting the best AP to associate to. The handover time claimed is less than 50 ms for iPCF-MC mode and less than 100 ms for iPCF mode, which could fulfill the requirements for the fast handover in our second use case.

B. Handover performance assessment

In order to assess the validity of the claims we replicated the use case setup using two Siemens Scalance W700 APs and one client. To emulate handovers between two different APs a tunable attenuator and a splitter/combiner between client and APs are used in order to control the Tx/Rx power on the client/APs. The emulation of handover is then done by adjusting the attenuation on one of the paths in the tunable attenuator. The setup was fully automated and manageable, enabling real time monitoring of the handover performance. In addition, we used two PLCs to generate time critical traffic, one controller PLC connected to the APs and one IO-device PLC connected to the client. The PLCs are configured with a PLC IO cycle of 64ms, and watchdog time of 4 (4x64=256ms). This results in the generation of a packet every PLC IO cycle. When the watchdog time is reached and no packets are received from the controller PLC, the link is set down and a new connection is renegotiated. To measure the handover time, we measured the inter-packet time at the receiving side. Normally the inter-packet time at the receiving side is the same as at transmitting side (64ms ± 1 ms). When the handover happens, a peak in the inter-packet time will be observed, equal to the inter-packet time plus the handover time. Figures 4 and 5 show the inter-packet time at the receiving side. In both cases, the handover times are lower than 50ms, satisfying our requirements. The periodicity of the peaks in Figure 6 is due to the usage of the management channel, with the client scanning this channel cyclically resulting in a slight delay of the lower priority data traffic.

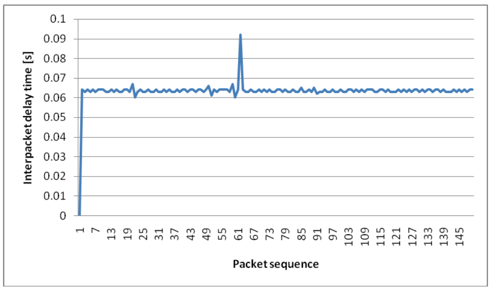

Fig. 4. Handover time for iPCF mode (92-64=28ms)

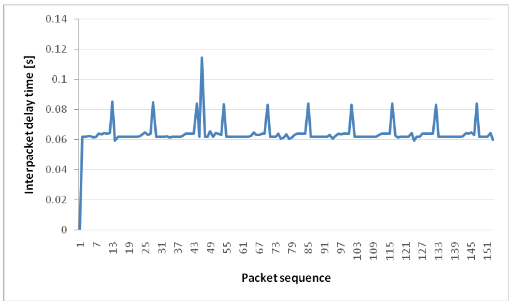

Fig. 5. Handover time for iPCF-MC mode (108-64=44ms)

C. Discussion

Although the Siemens extensions allow fulfilling the requirements, it must be noted that these are proprietary and not part of the Wi-Fi standard. This way, companies become fully dependent on a single vendor. In addition, the performance reported here can only be realized when a fully separated wireless network is established and parameters are configured appropriately. Ideally, next-generation Wi-Fi should take into account such use cases with stringent requirements, e.g. by moving towards TDMA-based solutions [4] with appropriate diagnostics and configuration properties.

V. Time-sensitive broadcast traffic between AGVs

A. Use case description

The last use case considers AGVs [5] in a warehouse that are used for carrying and placing goods autonomously from one place to other. The AGVs generate both unicast and broadcast communication. For the broadcast communication, the AGV manufacturer imposes an upper bound to the latency of broadcast packets of 20ms to arrive at neighboring AGVs. The unicast traffic between the AGVs and the central controller has to be reliable.

B. Handover performance assessment

In order to assess the impact of the handover performance on the broadcast latency we conducted a set of measurements in the w.iLab.t wireless testbed [6]. We assume the presence of a typical multi-AP wireless infrastructure that can be used for transmitting broadcast traffic between mobile robots. We consider three APs operating on non-overlapping channels (1, 6 and 11) in the 2.4GHz band and two AGVs. To enforce handovers from one AP to another, we remotely control their transmit powers, triggering handovers every 10s. The mobile robots are limited to only scan only mentioned channels to reduce scanning time. During the experiment, both robots are communicating with each other.

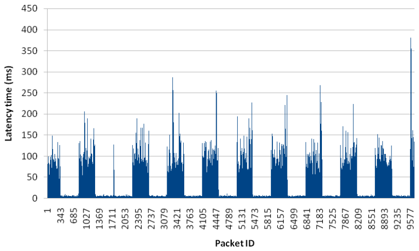

Fig. 6. Latency for broadcast traffic using infrastructure network

Figure 6 shows a severe negative impact of handovers on the broadcast traffic latency, due to the way broadcasts are disseminated through the network. Every broadcast needs to be rebroadcast to other devices connected to the same AP as well as to all other devices connected to other APs. This resulted in latencies of around 5ms when mobile robots are connected to the same AP, but increases up to 100m upon roaming. It is clear that even in this simple setup we can never meet the envisioned broadcast latency requirements (<20ms).

C. Problem mitigation

The above experiment clearly shows the negative impact of handovers on broadcast latency. Next to this, there are also other drawback when relying on a multi-AP network. If there is no wireless network in the place, the costumer will be forced to roll out a wireless network. An existing network might not be allowed to be used as AGV communication heavily relies on broadcast traffic or might have coverage holes that can lead to malfunctioning of the system. Further, when moving at high speed, robots will need to perform frequent handovers that negatively impact latency.

To mitigate the aforementioned problems, and in particular to reduce the broadcast latency, we are exploring the possibility of using mesh communication. Figure 7 shows the resulting latency when using a mesh only network between the AGVs that exhibits frequent link breaks, every 10s in the experiment, due to mobility. We see that the broadcast latency is now much lower, with latencies up to 7ms for two hops and around 3.5ms for one hop, satisfying our requirement. Based on these observations, we are working on a solution with two interfaces per AGV, allowing mesh-only or mixed setups with flexibility on how to distribute traffic over different interfaces. For more information, we refer to [7]. This case illustrates that sometimes alternative architectures are needed in order to overcome handover problems.

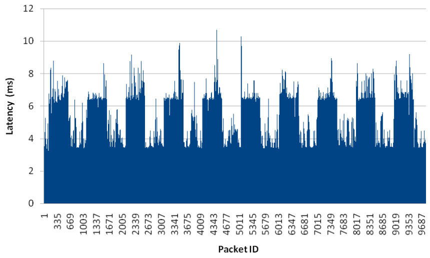

Fig. 7. Latency for broadcast traffic using mesh network.

VI. CONCLUSIONS

This paper presented three real-life industrial use cases that are all affected by the handover performance of Wi-Fi. The effect of interference on performance and the inability to deal with time-critical traffic was experimentally assessed and discussed. By tweaking parameters, moving to mesh communication or proprietary extensions some of the problems could be overcome. However, it also reveals more fundamental problems of the current Wi-Fi standard and the design of devices. Wi-Fi lacks proper features to deal with time-critical (mobile) applications and flexible reconfiguration possibilities. Devices are black boxes, not allowing proper diagnosis of wireless network problems and easy reconfiguration. Both observations offer great opportunies for further research to come to better diagnosable wireless solutions, configurable to the needs of industrial applications.

ACKNOWLEDGEMENT

Part of this research was supported by the FORWARD project, co-funded by iMinds, a research institute founded by the Flemish Government.

REFERENCES

[1] R. Drath and A. Horch, “Industrie 4.0: Hit or Hype?” IEEE Industrial Electronics Magazine, Vol. 8, 2014, pp. 56-58.

[2] Simatic Net, Sclance W-700, Configuration manual, Release 1.

[3] M. A. Youssef et al., "Analyzing the point coordination function of the IEEE 802.11 WLAN protocol using a systems of communicating machines specification.", Univ. of Maryland, 2002.

[4] Y. H. Wei et al., “RT-WiFi: Real-Time High-Speed Communication Protocol for Wireless Cyber-Physical Control Applications”, 34th IEEE Symp. On Real-Time Systems (RTSS), pp. 140-149, 2013.

[5] S. Arumugam et al., “Wireless Robotics: Opportunities and Challenges”, Wireless Personal Communications, Vol. 70, 2013, pp. 1033-1058, doi: 10.1007/s11277-013-1102-3

[6] w-iLab.t Zwijnaarde generic wireless testbed, http://wilab2.ilabt.iminds.be/

[7] E. Jarchlo et al., “To Mesh or not ot Mesh: Flexible Wireless Indoor Communication among Mobile Robots in Industrial Environments”, AdHocNow 2016