Interference Effect of ACL’s and SCO’s IEEE 802.15 Transmission on IEEE 802.11 Performance

Adhi Rizal  
University of Singaperbangsa Karawang, Karawang, Indonesia  
E-mail: adhi.rizal@staff.unsika.ac.id

Susilawati  
University of Singaperbangsa Karawang, Karawang, Indonesia  
E-mail: susilawati.sobur@staff.unsika.ac.id

Received: 10 December 2018; Accepted: 18 January 2019; Published: 08 March 2019

Abstract—This study aims to investigate the effect of Bluetooth on WLAN 802.11 performance. In contrast to other studies, we distinguish Bluetooth into two mechanisms, namely Asynchronous Connectionless (ACL) and Synchronous Connection-Oriented (SCO). Various scenarios (with range variation between the sender node and the access point (AP) and also the presence of ACL or SCO transmission as interference) was designed to conduct experiment. In general, experiment was conducted with two nodes that act as sender and receiver node that connected through internet. In addition, to determine the effect of Bluetooth on WLAN performance we use several test parameters, which are received signal strength indication (RSSI), signal to noise ratio (SNR), upstream and downstream, jitter, and packet loss rate (PLR). The study revealed the both ACL and SCO did not significantly affect WLAN performance, because they can only reduce the performance based on certain parameters and scenarios. But when they were compared, SCO has worst effect on WLAN performance, particularly on upstream, jitter, and PLR.

Index Terms—Bluetooth, WLAN, ACL, SCO, interference.

I. INTRODUCTION

Over past two decades, the wireless network has grown rapidly. It is proved by most wireless network devices now available at very affordable prices [1]. Based on satellite communications, the impact of this phenomenon is the density wireless network signals is increasing. In addition, along with the development of data traffic on internet through wireless link, the popularity of one generation of wireless network technology, which is IEEE 802.11 is increasing [2].

Wireless networks can reach places that cannot be reached by wired in a particular scope or environment. This advantages have an impact on several aspects, the reduction in cable procurement costs, the installation process that is faster than cable networks, mobility, has a wide range, and so on [3]. However, the wireless network have one crucial problems, which is signal interference. This problem arises because spectrum resources on wireless networks have limitations. Some signals from wireless networks must be operating in overlapping conditions with other signals or even in the same spectrum band or transmission medium (channel) [4].

One of the most popular wireless network technology generation is IEEE 802.11n [2] and Bluetooth (IEEE 802.15) [5]. Nearly 75% of mobile computing devices around the world are equipped with both technologies. Similar to Bluetooth, IEEE 802.11n technology which is an IEEE 802.11 family also operates on the same frequency. Therefore, interference will occur in IEEE 802.11 technology [5, 6].

When IEEE 802.11 tries to send packets over a network, it will check whether the medium or channel has been occupied or there is an ongoing transmission through the medium [7]. If other transmission or radio frequency (RF) energy is not detected on the channel, the device will generate CTS (Clear to Send) status. At this step, the wireless network device will start transmitting data packet. But when there are other IEEE 802.11 devices that are transmitting, an IEEE 802.11 device that is in its transmission range will delay its transmission [5].

This technique provides the right solution for interference which comes from the same IEEE 802.11 technology. However, when there are Bluetooth and IEEE 802.11 that uses a shared transmission medium, they cannot communicate with each other. It triggers a packet collision when they are using the channel simultaneously at a certain time [5]. Further, this condition can disrupt the communication between several devices that using both technologies.

In general, Bluetooth transmission are divided into two modes, namely Asynchronous Connection Less (ACL) and Synchronous Connection Oriented (SCO) modes [8, 10].
Bluetooth device can transmit data using one of these modes, while at the same time transmission can also be done by IEEE 802.11 devices. This can cause interference, hence IEEE 802.11 sender node will be forced to retransmit when receiver node does not send the acknowledgment [8]. This lack of coordination is the core of interference between both technologies.

Based on these problems and other similar research, this study aims to investigate the interference of Bluetooth ACL and SCO transmission to IEEE 802.11n. Therefore, testbed and some scenarios were built to conducting experiment.

II. RELATED WORKS

Several studies have been conducted regarding investigation of the impact of signal interference on IEEE 802.11. First, [10] conducted a study on the existence of Bluetooth which can interfere with IEEE 802.11b. The results of the study showed that both transmission technologies can interfere with each other. Besides it also has a big impact on SCO voice links on Bluetooth. Similar research on interference has also been carried out by [1]. It was conducted to characterize the interference in IEEE 802.11ac devices. The results showed that the main transmission channel selection and the channel width can reduce the throughput of the links that operate on larger channel. Furthermore, a research has been conducted by [11]. The study was conducting experiments on hidden node interference with IEEE 802.11. The result showed that hidden nodes causes several problems, which are throughput degradation, rerouting process becomes unstable, and the RTS/CTS mechanism is not effective to overcome the hidden node.

A study by [5] investigated the inference issues of 2.4 GHz radio frequency band between Bluetooth and IEEE 802.11. They also presented a new Bluetooth voice packet called Synchronous Connection Oriented with Repeated Transmission (SCORT). The result showed that the interference increased significantly along with the increasing number of participating devices, but SCORT can minimize the effect on interference between 802.11 and Bluetooth devices.

The paper on [12] discussed a solution of the interference problem caused by the proximity and simultaneous operation of Bluetooth and IEEE 802.11. A comparative analysis of their respective performance conducted and discussed the trends and trade-offs for different applications and interference levels.

Research by [6] investigated interference effects of Bluetooth on IEEE 802.11 performance. It aims to estimate the impact of Bluetooth signal interference on WLAN by measuring radiation from a WIFI Access Point (AP) in homogeneous and heterogeneous scenario. The study concluded that Bluetooth signal has minor impact on the IEEE 802.11 performance.

III. BLUETOOTH

Bluetooth is a low-power communication network technology that is intended to be applied at relatively close range [10]. Bluetooth is a specification for Wireless Personal Area (WPA). The wireless communication used by Bluetooth technology reaches 10 meters [17]. Table 1 is a comparison between IEEE 802.11n technology with Bluetooth [18, 19].

<table>
<thead>
<tr>
<th>Technology</th>
<th>Bluetooth</th>
<th>WiFi</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEEE Standard</td>
<td>802.15</td>
<td>802.11n</td>
</tr>
<tr>
<td>Data rate/Bandwidth</td>
<td>Low to high (720 Kbps)</td>
<td>Up to 72.2 Mbps (20 MHz channel)</td>
</tr>
<tr>
<td>Distance</td>
<td>10 m</td>
<td>Up to 100 m</td>
</tr>
<tr>
<td>Frequency Band</td>
<td>2.4 GHz</td>
<td>2.4 GHz</td>
</tr>
<tr>
<td>Output power</td>
<td>1 – 10 Mw</td>
<td>100 Mw</td>
</tr>
<tr>
<td>Application</td>
<td>M2M, IoT, sensor</td>
<td>Web application, voice, video, and data</td>
</tr>
<tr>
<td>Network size</td>
<td>7</td>
<td>32</td>
</tr>
</tbody>
</table>

In general, Bluetooth support two different types of transmission, namely Asynchronous Connection Less (ACL) dan Synchronous Connection Oriented (SCO) [20]. In ACL, receiver will will check the packet and verify cyclic redundancy code (CRC) to ensure that it is received correctly without any errors [20]. In general, ACL is used for transmitting non real-time data packets, for example file transfers [21, 22, 23, 24].

SCO link is symmetrical, point-to-point between master and slave [25]. In contrast to ACL, SCO packets are designed to support speech or voice data at 63 Kb/s [26, 27, 28, 29], but not for music or other signals that require high frequencies [20]. Moreover SCO link transmission does not support retransmission [21, 30].

IV. IEEE 802.11

IEEE 802.11 is a set of standards including technology and policies that define wireless local area networks (WLAN) [13, 14]. In addition, IEEE 802.11 can generally operate in two modes, namely infrastructure and ad-hoc.
In general, the hardware that we sent packet ined from simulation time e SCO mechanism was enabled by one thing to note s value, \( N \) is the Received power level (RSSI) and \( N \) is not be the same with its quality. 

\[ \text{Throughput} = \frac{\sum \text{delivered packet}}{\sum \text{simulation time}} \]  

\[ \% \text{packet loss} = \frac{\sum \text{lost packet}}{\sum \text{sent packet}} \]

A. Testbed

In this study we developed a testbed consisting of hardware and software. In general, the hardware that we used is an access point, laptop, bluetooth headset, and smartphone. While the software that we used is iperf, acrylic, and speedtest. Table 2 below showed the function of each software. Iperf was installed on sender and receiver node. While the remaining two were only installed on sender node. Based on Table 2 we used six parameters to examine the effect of bluetooth to 802.11 transmission.

<table>
<thead>
<tr>
<th>Software</th>
<th>Obtained Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Speedtest</td>
<td>Downstream</td>
</tr>
<tr>
<td>Iperf</td>
<td>Upstream, jitter, and packet loss rate</td>
</tr>
<tr>
<td>Acrylic</td>
<td>Received Signal Strength Indication (RSSI) and Signal to Noise Ratio (SNR)</td>
</tr>
</tbody>
</table>

a) RSSII represents the wireless signal strength obtained on the receiver’s antenna during packet reception [31]. RSSII value may vary from 0 to \( R_{\text{max}} \) [32], although the maximum values depend on the wireless card chipset. For example, an Atheros wireless card chipset has \( R_{\text{max}} = 70 \). Cisco cards has \( R_{\text{max}} \), while in Intel chipset card the RSSII provides the actual received power in negative dBm scale (for example, RSSII = -60 for the Intel cards means a received power equal to -60 dBm) [31]. Note that the higher the value, the stronger the signal.

b) In brief, SNR is a comparison of signal strength to background noise level, measured in dB, its value ranging from 0 to 100 [33, 34]. The higher the value, the better communication quality. One thing to note that a network can achieve very good signal strength, but may not be the same with its quality. From the RSSII, we can measure SNR using (1) [6].

\[ \text{SNR} = 10 \log \frac{P_r}{N} \]  

\( P_r \) is the Received power level (RSSI) and \( N \) is the Noise.

c) In this study we used throughput to represent upstream and downstream. Throughput is defined as the ratio the total number of packet delivered during a set time interval [34]. The throughput be measured using (2) [34].

d) Jitter is the interarrival time between successful packet transmissions of station and is obtained from the standard deviation of the latency or delay [36].

e) Packet loss occurs when one or more transmitted packets failed to its the destination and can be measured as percent value using (3) [37].

\[ \% \text{packet loss} = \frac{\sum \text{lost packet}}{\sum \text{sent packet}} \]

Detailed configuration of experimental parameters on sender node and AP is shown in Table 3.

Table 3. Experiment Configuration on Sender Node and AP

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>802.11n</td>
</tr>
<tr>
<td>Link capacity</td>
<td>75 Mbps</td>
</tr>
<tr>
<td>Traffic model</td>
<td>CBR (Constant Bit Rate)</td>
</tr>
<tr>
<td>Protocol</td>
<td>UDP (User Datagram Protocol) used by iperf</td>
</tr>
<tr>
<td></td>
<td>TCP (Transport Control Protocol) used by speedtest</td>
</tr>
<tr>
<td>Packet Length</td>
<td>1470 bytes</td>
</tr>
</tbody>
</table>

B. Experimental Scenario

As in [21, 24, 26, 27, 28] in this research we uses file transfer between two smartphone to enable ACL mechanism, while SCO mechanism was enabled by making voice call with smartphone that connected to bluetooth headset as interference source. As in [2] each transmission was tested 10 times to obtain reliable data.

The first scenario (Figure 2) was build to determine baseline network performance without interference. According to Figure 2, sender are connected with an AP within 2 to 10 m with 2 m range interval.
The next scenario (Figure 3) is similar to first scenario, but there is data transmission between Bluetooth devices in ACL mode that range from sender which is 1 to 5 m with 1 m range interval. At the same time sender is transmitting data packets to receiver.

In the last experiment (Figure 4), it is similar to second scenario, but ACL was replaced with SCO transmission.

VI. EXPERIMENT RESULT

The result and discussion of this study is categorized based on the testing parameters that used to examine the effect of ACL and SCO transmission on WLAN performance. Furthermore, value “0” of Bluetooth range from sender means that there is no interference from Bluetooth transmission, because it is begin from 1 m from sender.

A. RSSI and SNR

Based on Figure 5, there are various RSSI values. It is shows that Bluetooth transmission has little effect on RSSI. However, data obtained when SCO Bluetooth transmission are presence and the distance of the AP from the sender node is 4 m and 6 m, the RSSI value obtained tends to increase (signal strength increases) when the SCO Bluetooth transmission is getting far away from the sender node. Conversely, when SCO Bluetooth transmission getting far away from the sender node but approaches the AP, the RSSI value obtained tends to decrease (signal strength also decreases).

On Figure 6, regardless the type and distance of Bluetooth that interferes, in general the SNR will decrease along with the distance that getting away between the AP and the sender node. However, it drops significantly when there is a SCO Bluetooth signal and the distance between the AP and the sender node is 6 m and 10 m. While the results of other scenarios showed that SNR tends to remain stable (consistent). It means the existence of Bluetooth ACL and SCO does not affect the transmission of WLAN 802.11.
the SCO Bluetooth transmission (getting closer to the AP). Whereas in general, the presence of Bluetooth ACL and SCO does not significantly affect the speed of upstream.

Moreover, similar to upstream, in general SCO and ACL Bluetooth transmission does not significantly affect the downstream. However, based on Figure 8, when the distance between the AP and the sender node are 4 m and 10 m respectively and there were ACL and SCO Bluetooth transmissions, the downstream decreased, but does not significant, along with the distance of the Bluetooth transmission (closer to the AP). Among these results it was also found that when the distance between the AP and the sender node is 6 m and there is SCO Bluetooth transmission, the downstream decreased significantly but cannot return to the beginning speed (without Bluetooth interference).

C. Jitter and PLR

According to Figure 9, Bluetooth transmissions of both ACL and SCO has moderate effect on jitter. This can be seen from 10 combinations of experimental scenarios with 2 types of Bluetooth and various interference distances. 50% of the experimental results of experimental scenarios showed that Bluetooth transmissions ACL and SCO affect jitter. The effect was found when the AP with the sender node has a distance of 6 m, 8 m, and 10 m. But when the AP with the sender node has 8 m distance, only the SCO has worst effect to jitter.

Moreover, similar to upstream, in general SCO and ACL Bluetooth transmission does not significantly affect the downstream. However, based on Figure 8, when the distance between the AP and the sender node are 4 m and 10 m respectively and there were ACL and SCO Bluetooth transmissions, the downstream decreased, but does not significant, along with the distance of the Bluetooth transmission (closer to the AP). Among these results it was also found that when the distance between the AP and the sender node is 6 m and there is SCO Bluetooth transmission, the downstream decreased significantly but cannot return to the beginning speed (without Bluetooth interference).
Similar to jitter, ACL and SCO transmission can also worsen the PLR. It can be seen on Figure 10 that 50% of the experiment result show that ACL and SCO transmission can increase PLR. When the distance of the AP with sender node is 2 m and there is ACL or SCO transmission between them, the PLR will increase. But when ACL or SCO transmission is getting away from the AP and sender node, the PLR was decreased gradually even though it does not insignificantly. In addition, when the distance of the AP and sender node is 4 m, 6 m, 10 m and there was SCO transmission, the PLR value tends to increased.

VII. DISCUSSION

In general, Bluetooth SCO and ACL have minor effect on IEEE 802.11 transmission. Based on experiment result, this condition caused by several factors. Experiment on each scenario was carried out at different times, because all scenarios cannot be conducted in a day. Hence, at a certain time there are differences in the amount of data traffic or signals from various sources. Furthermore, the network conditions of provider are cannot be maintained to remain stable.

Moreover, all experiments were carried out in an open space. Even though we have minimized various other electronic devices around the experiment testbed, there are still a number of other objects that cannot be controlled. Some of these objects are people who move around the sender and receiver node which can causes significant variations, objects with metal material that can reflect signals, and woods, crystal, plastic, or brick can also reflect part of the signal, let pass the rest [38]. These objects can affect the transmission of IEEE 802.11 either directly or indirectly.

VIII. CONCLUSION

In general, the presence of bluetooth ACL does not affect the performance of WLAN 802.11. However, based on certain test parameters it can reduce WLAN 802.11 performance. They were upstream, jitter, and packet loss rates with certain test scenarios.

Moreover, similar to ACL, in general the presence of SCO also has slight effect on WLAN 802.11 performance. But the performance degradation of WLAN 802.11 is more visible when there was SCO compared to ACL. In addition, the further the distance between the sender and the AP and there was SCO transmission, the WLAN 802.11 performance will deteriorate, particularly on upstream, jitter, and packet loss rate.

ACKNOWLEDGEMENT

We gratefully acknowledge the funding received towards our research from LPPM of University of Singaperbangsa Karawang.
Interference Effect of ACL’s and SCO’s IEEE 802.15 Transmission on IEEE 802.11 Performance

Adhi Rizal, born in 1991. He received his master degree in Informatics with the specialization of Advanced Networking from School of Electrical Engineering and Informatics (STEI), Bandung Institute of Technology, Bandung, Indonesia. Currently he is working as lecturer in Informatics Engineering at University of Singaperbangsa Karawang, Karawang, Indonesia.

Susilawati, born in 1990. She received her master degree in Physics with the specialization of Instrumentation from Department of Physics, Faculty of Mathematics and Natural Sciences, Bandung Institute of Technology, Bandung, Indonesia. Currently he is working as lecturer in Informatics Engineering at University of Singaperbangsa Karawang, Karawang, Indonesia.

How to cite this paper: Adhi Rizal, Susilawati,"Interference Effect of ACL’s and SCO’s IEEE 802.15 Transmission on IEEE 802.11 Performance", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.3, pp.1-7, 2019.DOI: 10.5815/ijcnis.2019.03.01

Computer Science, Engineering and Information Technology (IJCSEIT), pp. 55-63, 2011.


