Formal Analysis of Collision Prevention of Two Wireless Personal Area Networks

Amjad Gawanmeh\textsuperscript{12} and Youssef Iraqi\textsuperscript{1}

\textsuperscript{1} Department of Electrical and Computer Engineering, Khalifa University, Abu Dhabi, UAE
amjad.gawanmeh@kustar.ac.ae, youssef.iraqi@kustar.ac.ae
\textsuperscript{2} Concordia University, Montreal, Canada.

Abstract
There are several challenges in the design and operation of Wireless Personal Area Networks (WPANs) such as wireless networking and communication, power consumption, and mobility. Hence, the operation of several WPANs within the same area can result in collision if two WPANs operate in the same wireless channel and come in close range. Therefore, methods for collision detection and prevention need to be validated properly due to the sensitivity of the applications of WPANs. Existing approaches depend on paper and pencil methods to proof the correctness of proposed methods, which might not be enough when practical issues, such as mobility, are taken into consideration. In this paper, we use formal analysis in order to verify the correctness of collision prevention conditions for two WPANs.

Keywords: Formal Analysis, Model Checking, Collision Analysis, WPAN, Collision Prevention

1 Introduction and Motivation

Wireless Personal Area Networks (WPANs) are commonly used in healthcare systems due to the increasing need for technologies that enable the continuous remote monitoring of elderly people that provides alerting mechanisms for emergency situations. Hence, several types of medical sensors and devices are broadly available to individuals and are being used at their homes. This has led to the emergent of WPANs that enables communication between these devices. This technology has been widely used in several domain, in particular, in healthcare environments. Due to safety critical nature of their applications, the correctness of operation for these wireless systems is of paramount importance. Therefore, a significant portion of their design efforts is spent on analyzing the designs in order to catch as many functionality errors as possible at early stages of the design process, which enables enhancing the performance metrics prior to the production.

As opposed to detection methods that allow the collision to occur, collision prevention methods may stop certain collisions from happening during the operation of WPANs if certain conditions were met. Hence, collision prevention strategies can guarantee that collisions never
occur. The authors in [11] presented sufficient and necessary condition for collision prevention for two WPANs operating in close range. While the conditions were formalized and proofs were given mathematically, it is essential to provide formal analysis for the WPANs and show formally that the given conditions indeed are sufficient to avoid and prevent collisions. The automated proof can help provide more assurance, in particular, verifying the system for all possible states. Formal methods [2] use mathematical models for the analysis of computing, communication, and industrial systems in order to establish system correctness with mathematical rigor.

Formal methods have been used in modeling and verification of different types of medical systems [9]. The work in [7] presented an embedding and verification of ZigBee protocol in Event-B. A qualitative analysis of Collision Resolution Protocol for wireless networks was also proposed in [12]. The work in [10] used Higher Order Logic (HOL) theorem proving for analysis of the probabilistic properties in wireless systems. The work in [3, 4] formalized WBSN controller for reading ECG signal utilizing formal specification requirement of such medical systems [8]. Most formal analysis methods proposed for wireless systems addressed the issue of collision detection, and to the best of our knowledge, this is the first effort to provide formal analysis for collision avoidance mechanism in WPANs. This paper uses NuSMV model checker [6] in order to formalize WPANs, and then formally proof all collision prevention conditions provided in [11]. This will increase the trust in the safety critical system under consideration, provide automatic proof with full coverage, and provide the necessary background to generalize the proofs for more complex scenarios such as multiple WPANs.

2 Specifications of Collision Analysis in WPANs

In this section we present the specification of collision analysis and avoidance mechanism based on [11]. The WPAN system specifications are presented based on the beacon-enable mode of IEEE 802.15.4 MAC protocol [1] for the operations of WPANs. The Superframe duration (SD) represents the active portion of the superframe (beacon interval or BI), during which packets can be transmitted. The coordinator controls the beacon interval and superframe duration through two parameters, namely beacon order (BO) and superframe order (SO) as follows: $BI = a_{BaseSuperframeDuration} \times 2^{BO}$, and $SD = a_{BaseSuperframeDuration} \times 2^{SO}$, where $0 \leq SO \leq BO \leq 14$. The coordinator handles the values of BO and SO as well as the allocation between contention access period (CAP) and the contention free period (CFP).

A collision occurs when two coordinators are within the radio range of each other and part of their superframe active periods overlaps. Any overlap between active period and beacon is not considered as a collision because beacon transmissions have absolute priority over data packet transmissions. Active and inactive period durations are different for different WPANs according to the figure. In addition, superframe start time varies between different WPANs. Two WPANs, $W_a$ and $W_b$, can be supported if the active periods $SD_a$ and $SD_b$ do not collide at any time in the future. Figure 1 shows WPANs collision model with the following notation: $a = BI_a$, $a_1 = SD_a$, $b = BI_b$, $b_1 = SD_b$.
Theorem 2.3. \[11\]

Let $a\in\mathbb{N}$, such that $a > 1$, and $b > 1$. Let $a_1, b_1, p \in \mathbb{N}$, such that $0 < a_1 \leq p < a$, and $0 < b_1 < b$. Let $\alpha, \beta$ such that $0 < \alpha \leq a_1$ and $0 < \beta \leq b_1$.

There exist $n, m \in \mathbb{Z}$ such that $na + \alpha = mb + \beta + p$. This means that during the $n$th beacon of $W_a$ and $m$th beacon of $W_b$, points $\alpha$ and $\beta$ will collide. In the following, only cases where $p \geq a_1$ are considered, since $W_b$ comes after $W_a$, therefore, if $p$ is less than $a_1$, there will be a collision.

**Theorem 2.1.** \[11\] Let $a, b \in \mathbb{N}$, such that $a > 1$, and $b > 1$. Let $a_1, b_1, p \in \mathbb{N}$, such that $0 < a_1 \leq p < a$, and $0 < b_1 < b$. Let $\alpha, \beta$ such that $0 < \alpha \leq a_1$ and $0 < \beta \leq b_1$.

There exist $n, m \in \mathbb{Z}$ such that $na + \alpha = mb + \beta + p$. This means that during the $n$th beacon of $W_a$ and $m$th beacon of $W_b$, points $\alpha$ and $\beta$ will collide. In the following, only cases where $p \geq a_1$ are considered, since $W_b$ comes after $W_a$, therefore, if $p$ is less than $a_1$, there will be a collision.

**Theorem 2.1** states that if the value of $p + \beta - \alpha$ is a multiple of the greatest common divisor of $a$ and $b$: $\gcd(a, b)$, then the two WPANs, $W_a$ and $W_b$, will collide at some point in the future. Therefore, the value of $p$ should be chosen to be different from $k \ast \gcd(a, b) + \alpha - \beta$, otherwise there will be a collision between the WPANs. Since $0 < \alpha \leq a_1$ and $0 < \beta \leq b_1$, the range of $\gcd(a, b) + \alpha - \beta$ is $\gcd(a, b) - b_1 \leq \gcd(a, b) + \alpha - \beta \leq \gcd(a, b) + a_1$. Hence $p$ should be chosen outside this range.

According to Figure 2, there are no possible choices for $p$ if $a_1 + b_1 > \gcd(a, b)$. Corollary 2.2 states this fact formally, where $\text{Support}(W_a, W_b)$ is the predicate: “$W_a$ and $W_b$ can be supported simultaneously”

**Corollary 2.2.** \[11\] Let $a, b \in \mathbb{N}$, such that $a > 1$ and $b > 1$, then $\text{Support}(W_a, W_b) \iff \exists p, a_1 \leq p < a, \forall \alpha, \beta, 0 < \alpha \leq a_1, 0 < \beta \leq b_1, \neg \exists k \in \mathbb{N}, p + \beta - \alpha = k \ast \gcd(a, b)$

**Theorem 2.3.** \[11\]

Let $a, b \in \mathbb{N}$, such that $a > 1$ and $b > 1$, $\text{Support}(W_a, W_b) \iff a_1 + b_1 \leq \gcd(a, b)$

**Theorem 2.3** gives a straightforward collision prevention condition to check if two WPANs can coexist without collisions:

$$a_1 + b_1 \leq \gcd(a, b) \quad \text{(1)}$$

**Theorem 2.3** states that if the condition (1) is satisfied, then the two WPANs can be scheduled in such a way that they will never collide, on the other hand, if this condition is not satisfied, the two WPANs will collide in the future regardless of any collision avoidance mechanism used. In order to further simplify the collision prevention conditions in (1), taking into account the fact that the beacon interval and the superframe duration are power of 2, let $A$, $A_1$, $B$, and $B_1$ such that $a = 2^A$, $a_1 = 2^{A_1}$, $b = 2^B$, and $b_1 = 2^{B_1}$. Note that $\gcd(2^A, 2^B) = 2^{\min(A, B)}$. For any given three positive integers $A_1$, $B_1$, and $C$, the condition $2^{A_1} + 2^{B_1} \leq 2^C$ is satisfied iff $0 \leq A_1 \leq C - 1$ and $0 \leq B_1 \leq C - 1$.

The collision prevention condition (1) becomes $A_1 < \min(A, B)$ and $B_1 < \min(A, B)$, which states the necessary condition for collision prevention, where the order of the superframe of each WPAN has to be strictly smaller than the order of the beacon intervals of both WPANs. This means that the order of the superframe of each WPAN has to be strictly smaller than the order of its beacon interval, i.e., the superframe duration cannot exceed half of the beacon interval.

In the next section, we provide formal analysis of WPANs, where we use NuSMV model checking in order to validate the above conditions for collision prevention.

## 3 Formal Analysis of Collision Prevention for Two WPANs

Model checking [5] (or property checking) is a formal verification technique that verifies whether a model of a system meets a given specification. The method provides exhaustive coverage
for the system and is conducted automatically. NuSMV model checker provides cutting-edge formal verification methods based on optimized techniques. Therefore, we will use NuSMV in order to model and verify the WPAN model. The specification of the protocol states that the frame interval is equal to $SFD \times 2^{BO}$, and superframe duration is equal to $SFD \times 2^{SI}$, where $1 \leq SI \leq BO \leq 14$. We used a variable that allows the verification of the system for several variables of the superframe duration. The final and most significant step is to define and verify the set of theorems given for the correct operation of the WPAN protocol described above.

**Property 1.** is used to formalize theorem 2.1, which states that the two WPANs $W_a$ and $W_b$ will collide at some point in the future if the value of $p + \beta - \alpha$ is a multiple of the greatest common divisor of $a$ and $b$: $gcd(a, b)$. This property is formalized as given below for the SMV model.

\[
\text{SPEC AG (EF((n \times a + \alpha = m \times b + \beta + p) \rightarrow (p + \beta - \alpha = k \times gcd)))}
\]

This property states that for all paths and for all states, anywhere in the path, if the value $n \times a + \alpha$ is equal to the value $m \times b + \beta + p$, then, there is a path in the future with $p + \beta - \alpha$ must be equal to $k \times gcd$. Equivalence between two propositions is defined using both ways implication. Hence, the second part states the other side of the implication, which, as a result demonstrates equivalence between the two propositions. This property is then verified for the system using NuSMV tool.

**Property 2.** is used to specify the situation where two WPANs are supported simultaneously as illustrated in Figure 2. The property states that there are no possible choices for $p$ if $a_1 + b_1 > gcd(a, b)$. Corollary 2.2 states this fact formally, where $Support(W_a, W_b)$ is the predicate: “$W_a$ and $W_b$ can be supported simultaneously”. Property 2 below is used to specify the required condition for the support predicate defined above as illustrated in Corollary 2.2, which states that if $p$ is chosen according to the condition given, then, there is a choice of $k$, where the collision can be avoided. This property is modeled and verified using NuSMV.

\[
\text{SPEC AG ((p > a_1 \& p < a) \rightarrow AG (!(p + \beta - \alpha = k \times gcd)))}
\]

**Property 3.** is used to model theorem 2.3 which gives a straightforward collision prevention condition to check if two WPANs can coexist without collisions: $a_1 + b_1 \leq gcd(a, b)$. This condition allows two WPANs to be scheduled in such a way that they will never collide. The theorem is formalized as show below, where the predicate $Support(W_a, W_b)$ is formalized using the definition given in Corollary 2.2, and two ways implication is used to represent equivalence. The property is verified in NuSMV successfully.

\[
\text{SPEC AG (((a_1 + b_1) <= gcd) \rightarrow (p > a_1 \& p < a) \rightarrow AG (!(p + \beta - \alpha = k \times gcd)))}
\]

\& (p > a_1 \& p < a) \rightarrow AG (!(p + \beta - \alpha = k \times gcd))) \rightarrow ((a_1 + b_1) <= gcd))
Property 4. is used to formalize the simplified collision prevention condition defined based on equation 1, where \(a_1 < \min(a, b)\) is defined using \(a_1 < a\) and \(a_1 < b\), which is equivalent. Corollary 2.2 is used to define \(\text{Support}(W_a, W_b)\).

\[
\text{SPEC AG (} ((a_1 < a) \& (a_1 < b) \& (b_1 < a) \& (b_1 < b)) \rightarrow \\
(p > a_1 \& p < a) \rightarrow \text{AG}(((p + \beta - \alpha = k \cdot \text{gcd})) \& (p > a_1 \& p < a) \rightarrow \\
\text{AG}(((p + \beta - \alpha = k \cdot \text{gcd})) \rightarrow ((a_1 < a) \& (a_1 < b) \& (b_1 < a) \& (b_1 < b)))
\]

4 Conclusion

In the operation of personal area networks, in particular for health applications, it is important to provide the necessary and sufficient conditions for collisions not to happen in neighboring IEEE 802.15.4 WPANs. If certain conditions are not satisfied, collisions will occur periodically, and hence, collision and recovery mechanisms will only provide temporary solution. Therefore, it is important to validate collision prevention mechanisms thoughtfully. In this work, we used model checking formal analysis method in order to model and validate these mechanisms in WPANs, where several properties were modeled and verified for collision prevention. It is intended to generalize these results for an arbitrary number of WPANs, and propose a distributed protocol for the selection of Beacon Intervals that ensure prevention of collisions.

References


