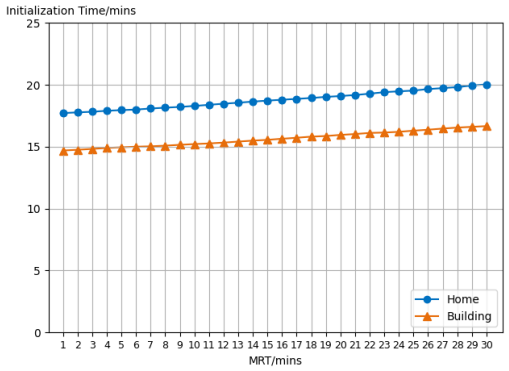
Technical Report

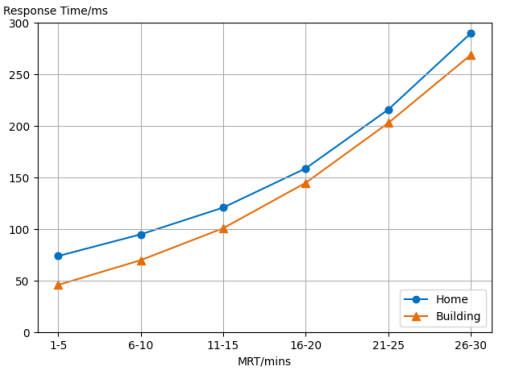
ANONYMOUS AUTHOR(S)

In the SysGuard approach, we introduce a configurable parameter called the maximum response time *MRT*, which defines the maximum time required for the effects of physical interactions in the environment to manifest. By configuring the *MRT* parameter, we calculate the order of the physical interaction graph PIG model (i.e., the number of previous time steps included in PIG) based on the average time interval *ATI* of device logs, where the order is determined as $\tau = \frac{MRT}{ATI}$.

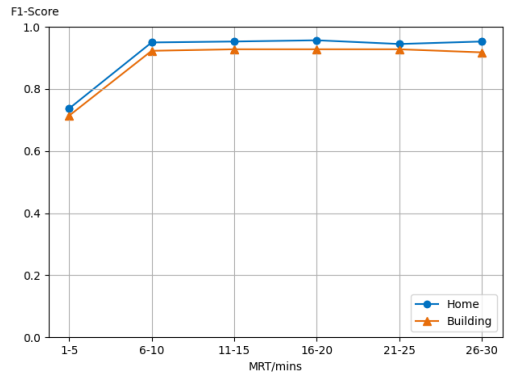
To investigate the impact of different *MRT* settings on the performance of the SysGuard approach, we conduct tests on our constructed WoT violation dataset with varying *MRT* configurations. Considering the cost of using ChatGPT for SysGuard initialization when filtering out the edges unrelated to physical interactions in the causal analysis process, we restrict the test range of *MRT* to between 1 and 30 minutes. This range is sufficient to cover all potential physical interactions present in each WoT system. For each *MRT* setting, we record the initialization time of SysGuard as well as its runtime response time for detecting violation and generating handling policy, as shown in Figure 1a and Figure 1b, respectively. Based on the detected violations and the generated corresponding handling policies, we access the performance of SysGuard for violation detecting and handling using F1-Score and mean reciprocal rank (MRR) as metrics, as shown in Figure 1c and Figure 1d, respectively.



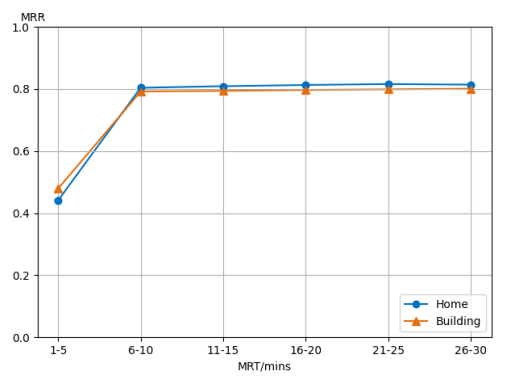
(a) Initialization Time



(b) Response Time



(c) Violation Detection



(d) Violation Handling

Fig. 1. The impact of different *MRT* settings on the performance of the SysGuard

The initialization time shows a slight linear increase as *MRT* grows. The majority of the initialization time is spent on the causal analysis of directed edges in the PIG using ChatGPT. As *MRT* increases, the number of device logs that need to be analyzed in each device interaction scenario provided to the ChatGPT also grows. This leads to increased network overhead, reduced response speed of the LLM, and consequently, longer initialization time. Additionally, the initialization time does not exhibit a stepwise increase as the order of PIG grows. This is because, during causal analysis, if it is determined that no physical interaction exists between two devices, all corresponding edges between these nodes at every time step are removed. As a result, causal analysis of the physical interaction relationship is performed only once for each directed dependency between devices. Therefore, the growth in model order (i.e., the increase in time steps) has no significant impact on the initialization time.

The runtime response time of SysGuard exhibits a stepwise increase each time *MRT* grows by ATI (approximately 5 minutes), with the magnitude of this increase growing exponentially. The reason is that, as the model order increases, the number of nodes and edges in the PIG rises substantially, resulting in an exponential increase in the computational complexity of PIG inference. Empirically, the response time increases relatively slowly for models of up to the fourth order, while beyond the fourth order, the computational complexity grows rapidly. Therefore, when setting *MRT*, it is important to avoid excessively high model order to prevent prolonged response times.

The violation detecting and handling performance of SysGuard significantly improvement when *MRT* is set above 5 minutes, and thereafter remains relatively stable. This is because shorter *MRT* settings correspond to lower model orders that can only capture short-term physical interactions (e.g., brightness, UV intensity, noise, circuit load), but cannot capture longer-term physical interactions (e.g., temperature, humidity, air quality). As a result, SysGuard is unable to accurately infer environmental attributes associated with long-term physical interaction effects, which negatively impacts its performance. After the model order becomes adequate to capture long-term physical interactions, further increasing the model order does not result in any additional performance improvement. Notably, the time required to capture physical interactions is also affected by the interval settings used to discretize continuous environmental attributes into distinct states. When larger intervals are used, a larger *MRT* setting is required compared to smaller intervals. For example, the temperature change of 10 degrees Celsius takes longer time to manifest than a change of 5 degrees Celsius. Therefore, when setting *MRT*, it is important to ensure that it is sufficient to cover the state changes of long-term physical interaction attributes.

Overall, the configuration of the *MRT* parameter effectively balances the performance of the SysGuard with computational complexity. By setting *MRT* based on the maximum time required for state changes in environmental attributes influenced by long-term physical interactions, it is possible to ensure that SysGuard accurately detects violations and generates appropriate handling policies, without incurring unnecessary runtime response time.