MetaPoL: Immersive VR based Indoor Patterns of Life (PoL) and Anomalies Data Generation for Insider Threat Modeling in Nuclear Security

Chathika Gunaratne†, Mason Stott‡, Debraj De*†, Gautam Thakur†
*Corresponding author
†Oak Ridge National Laboratory (ORNL), Oak Ridge, Tennessee, USA
‡University of Tennessee Knoxville, Knoxville, Tennessee, USA
Email: gunaratnecs@ornl.gov, stottmc@ornl.gov, ded1@ornl.gov, thakurg@ornl.gov

***Abstract*—Insider threats are perhaps the most serious challenges that nuclear and radiological security systems face. Insiders pose such a great threat due to their access, authority, and knowledge, granting them opportunities to bypass dedicated nuclear and radiological security elements. For example, in one of the latest major insider threat incidents to nuclear security, the Doel-4 nuclear powerplant in Belgium suffered a shutdown, the threat of nuclear materials diversion, and long-term loss of tens of millions of dollars. Seven years of investigation concluded that it was an inside job and attempted sabotage. In this regard, there is an immediate need for R&D and technology integration in the domain of modeling indoor Patterns-of-Life (PoL) and anomaly detection. This can be achieved by using datasets of facility users' mobility and activity, which can support the design of algorithms for insider threat modeling and detection. However, due to classification, privacy, sensitivity, and safety protocols, such datasets from real physical nuclear reactor facilities are not only hard to share but also not feasible to deploy and collect. Aiming to find an alternate solution, our proposed demo - *MetaPoL*, is the first-ever (for the application space) immersive VR (virtual reality) environment of a real-world secure facility and allows users to move-and-stay through the designed indoor physical layout and also encounter NPCs (non-player characters) that emulate other facility users. In the *MetaPoL* an interactive user performs realistic spatio-temporal movement, dwelling and activities using a Meta Quest Pro VR headset, and that generates high-frequency (in time) high-resolution (in space) indoor spatial-temporal datasets that are valuable for PoL modeling and anomaly detection research specifically for insider threat modeling and detection mission. Such generated realistic, rich in context, and mission specific datasets can boost AI/Machine Learning based research for modeling and detecting insider threats in nuclear security and nonproliferation.**

***Index Terms*—Nuclear security, insider threat and sabotage, insider threat modeling, patterns of life (PoL), anomaly detection, virtual reality (VR), Metaverse, indoor mobility data, spatial-temporal data, human-computer interaction (HCI).**

I. Introduction

Nuclear nonproliferation and nuclear security encompass a vast mission space. Within that, the insider threat detection and mitigation (ITDM) [6], [9] is a critically important research and application domain. According to [5], [7], insider threats are perhaps the most serious challenges that nuclear security systems face. The insiders with malicious intent can pose a significant threat to nuclear and radiological security due to the large scopes of their access, authority, and knowledge that grant them opportunities to bypass dedicated nuclear and radiological security elements [3]. Recognizing the international community's need to address the insider threat to nuclear and radiological security, in 2016 the United States sponsored Information Circular 908 – Joint Statement on Mitigating Insider Threats (INFCIRC/908) at the International Atomic Energy Agency (IAEA). The Joint Statement is now endorsed by 34 countries and the INTERPOL [3].

One of the recent major insider threats and sabotage incidents in nuclear security is the Doel-4 nuclear reactor powerplant incident in Belgium that took place on August 5th, 2014. The unit was automatically shut down following the loss of oil in its steam turbine. That and subsequent related outages had an impact of tens of millions of dollars in loss, and Belgium was left without half of its nuclear capacity at that time. Inspections revealed a disturbance in the steam turbine in a non-nuclear part of the complex [1]. Seven year long investigation concluded that the incident was an inside job and an act of sabotage carried out by an employee or a subcontractor who had legitimate access to the area but was not authorized to operate a valve that triggered the automatic shutdown of the reactor facility [1].

These real-world unsolved incidents, future potential of global threats, and recent stress on insider threat detection and mitigation (ITDM) [3], [6] calls for research and development advancements in ITDM, patterns-of-life (PoL) and anomalies detection. These advancements can be satisfied and enriched by: (a) diverse and rich domain-specific datasets that can be made available more openly; and (b) designing data-driven AI/Machine Learning algorithms and also other modeling methodologies - but all needing rich and relevant datasets. Data availability and privacy issues remain central issues in the field of modeling and mitigating insider risk [8]. The classification levels, privacy, sensitivity and safety protocols surrounding the ITDM and PoL related datasets from from real-world nuclear reactor facilities are hard and complex to share with research community. Also, it is not always feasible to deploy certain types of sensing and data collection systems in every area of a nuclear reactor facility. Even more importantly, it is also not feasible to simulate or emulate diverse anomalous movements and activity patterns, but if allowed, it could generate diverse anomaly related datasets. Such datasets can be extremely valuable to ITDM and POL related data-driven modeling research. Driven by these needs in this proposed demo and paper, we present *MetaPoL*. In our envisioned bigger picture for *MetaPoL* i.e., Metaverse for patterns-of-life (PoL) capabilities and platform, this work is the first step where it has designed an immersive VR (virtual reality) based Metaverse for a real-world secure facility. In the current scope of its Metaverse, interactive users (aimed at nuclear reactor facility users and insider threat researchers) can stay and move around the facility virtually using our designed VR software (designed with Unity [4]) that runs on Metaquest Pro headset [2]. The interactive user experiences and interacts with the physical environments and physical layout of the nuclear facility (currently direct interaction with physical objects is limited), and also encounters NPCs (non-player characters) that also move around and represent other facility users (currently just viewing the NPCs, but no interaction yet). Now all these indoor spatial-temporal moving/dwelling activities of the interactive user and also the NPCs in *MetaPoL* automatically generate very rich and mission relevant datasets. The datasets currently being generated are indoor spatial-temporal data in the form of {user id, x coordinate, y coordinate, floor number, timestamp}.

II. Details of *MetaPoL* Design

In this section, we describe the *MetaPoL* platform and capability design in some detail. The software development of VR (virtual reality) based simulation environment has been done using Unity game engine software [4]. As for the hardware platform for software deployment (including executing NPCs movement in the virtual environment), user interaction, data generation and storage - the Meta Quest Pro VR headset is used [2]. There are three main components or functionality in the *MetaPoL*:

- Virtual immersive environment of real physical environment of the secure facility of interest.
- Player logic (follow instructions for real users performing activities in interactive VR).
- Non-player characters (NPCs) performing their movements and activities.

As the first component, the virtual immersive environment of the actual physical environment of the secure facility of interest is designed in Unity game engine software [4]. Following the general workflow (with repeated iterations and frequent testing), an immersive environment was created for the facility of interest.

- We gathered reference materials for the real space. This included photos and videos taken only whenever permitted for some areas, observations and notes from facility tours, and a 2D indoor layout diagram of the permitted areas. A potential option was directly scanning the 3D of the physical environment through Lidar (e.g., some are available in recent iPad versions), but that was not feasible for following the security protocols and restrictions of the facility of interest.
- Then, we created or purchased (from the Unity Store unity_asset whenever needed) 3D assets, textures, and visual effects comparable to the above-mentioned references to physical space.
- After that, we created the scene geometries in Unity software, again based on the above-mentioned references about the physical space. The 3D modeling and texturing are done with ProBuilder (Unity plugin) and Quixel Mixer as a texturing tool.

As a second component, user interaction in the simulation has player logic integrated, which has instructions (in the form of a task board) to follow for enacting certain activities in the interactive VR. All the simulation logic is written in C# programming for Unity. Although interactive users are not restricted to move through the virtual facility freely, this task board based player logic with instructions are meant to guide the users enacting normal PoL scenario as well as intended insider threat scenario. Expected interactive users here are the actual facility users and managers, and also ITDM and PoL researchers relevant to the facility. Now as the interactive users perform indoor spatial-temporal movement and activities, the platform generates and stores continuous data in the format {user id, x coordinate, y coordinate, floor number, timestamp}. The resolution for timestamp is default to every 1 second, but it is configurable as needed.

As third component, non-player characters (NPCs) are present in the VR scene and represent subset of other facility workers. The NPCs perform their indoor spatial-temporal movements and activities based on a pretrained model. The details of the model is out of scope of this paper.

III. Demonstration of Usecase in Insider Threat

In this section we present the usecase of our designed *MetaPoL*. The scenario is a secured facility with physical security needs, e.g., a nuclear reactor facility. There are two instances of the scenario generated with *MetaPoL*'s immersive and interactive capability: (i) "normal"/PoL, and (ii) "anomalous".

In the "normal" or PoL (patterns-of-life) scenario there are six NPCs (non-player characters) spatially-temporally moving and dwelling (based on a pre-defined spatial-temporal activity model of normal or PoL behavior). As shown in Figure 1 the NPCs are labeled with identifiers "PoLNPC0", "PoLNPC1", "PoLNPC2", "PoLNPC3", "PoLNPC4", "PoLNPC5". Then there is one interactive real human user labeled as "PoL-Player". That interactive user in this "normal" scenario, moves and dwells spatially based on pre-defined task list, which is based on normal PoL behavior (the NPCs' model also follow that PoL behavior). Figure 1 visualizes the spatial-temporal trajectories datasets of the six NPCs and the interactive user (following normal behavior task list), as generated by our *MetaPoL*.

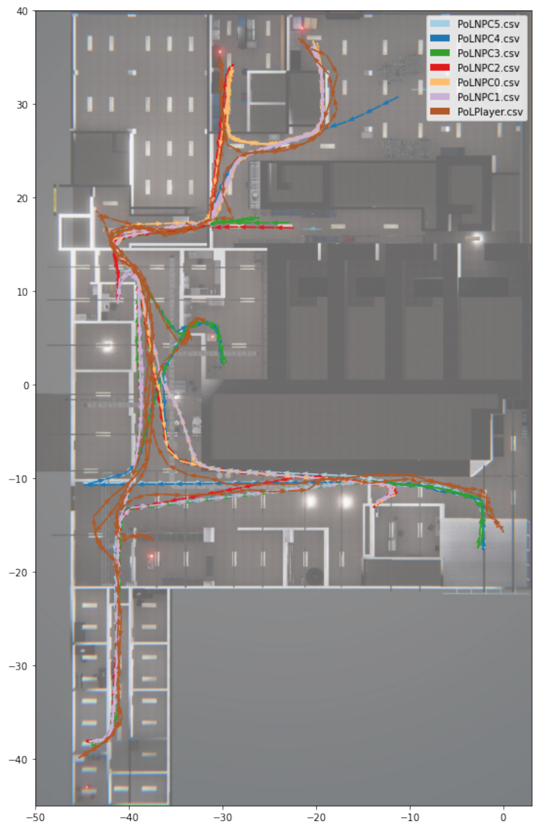

Fig. 1. Spatial-temporal movement trajectories visualized of the interactive user (labeled as PoLPlayer) and the six NPCs (labeled PoLNPC0-PoLNPC5), all in the "normal"/PoL scenario. (Note: the trajectories and background facility layout may be a little misaligned, and is not an artifact from *MetaPoL* but due to visualization used here.)

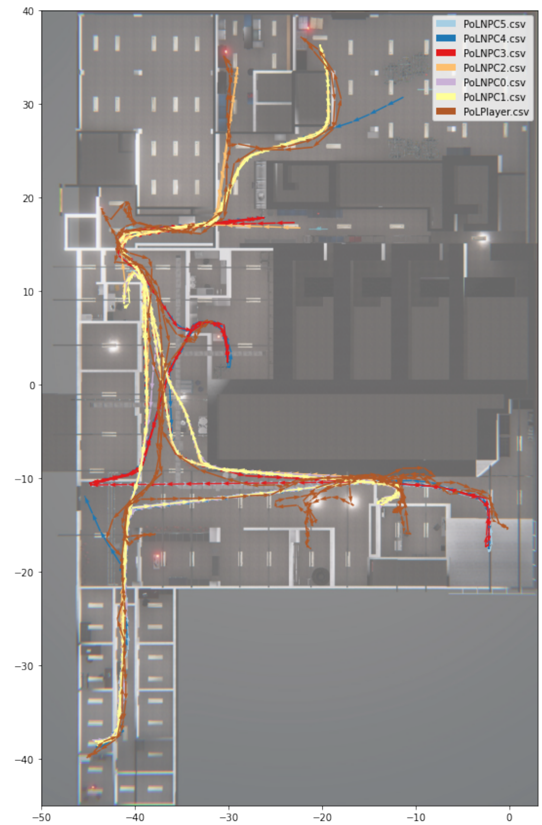

Fig. 2. Spatial-temporal movement trajectories visualized of the interactive user (labelled as PoLPlayer) and the six NPCs (labelled PoLNPC0-PoLNPC5), all in the "anomalous" scenario. (Note: the trajectories and background facility layout may be a little misaligned, and is not an artifact from *MetaPoL* but due to visualization used here.)

Then in the "anomalous" scenario there are same six NPCs (non-player characters) like in the previous "normal" scenario, spatially-temporally moving and dwelling (based on a pre-defined spatial-temporal activity model of normal or PoL behavior). As shown in Figure 2 these are labeled with "PoL-NPC0", "PoLNPC1", "PoLNPC2", "PoLNPC3", "PoLNPC4", "PoLNPC5". Then there is the interactive real human user labeled as "PoLPlayer", moves and dwells spatially based on pre-defined task list. But unlike in the previous "normal"/PoL scenario, here the task list is carefully designed to reflect insider threat related intent and activities. In the task list here, the user generally perform same set of order of tasks and spatial tasks as was in "normal" scenario, except a few times the user is tasked to perform some anomalous/evasive tasks as follows. In the anomalous/evasive task related to insider threat intent, the user enters two rooms/spaces where it is allowed/authorized but not tasked in the PoL activity. Inside the order of normal/PoL tasks, the user with insider threat here enters those two rooms/spaces for short period of time (to dwell for brief time, emulating performing some malicious activities), and also notably enter those spaces only when the NPCs are not around visually in the vicinity. This is a highlight of our designed *MetaPoL* capability that this kind of scenario and dynamics (emulating anomalous activities only when there is no other facility users around) cannot be easily created (and repeated) in real-physical nuclear reactor facility (due to safety and privacy protocols) but can be created (and valuable datasets generated) in the virtual-physical representation of the facility like done here. Figure 2 visualizes spatial-temporal trajectories datasets of the six NPCs and the interactive user (following anomalous task list, emulating insider threat intent and hidden activities), as generated by our *MetaPoL*.

From the "normal"/PoL and "anomalous" scenarios described above, Figure 3 also visualizes just the interactive user's spatial-temporal trajectories datasets, as generated by our *MetaPoL*. The spatial area of the insider threat related activities in "anomalous" mode can be recognized here. Also, another Figure 4 visualizes the temporal nature (besides the 2D spatial nature) of the "normal" and "abnormal" trajectories of the interactive user.

IV. Conclusion

In this demonstration paper, we present *MetaPoL* - an immersive interactive VR (virtual reality) based platform that can be used to generate both PoL (patterns-of-life) normal/baseline behavior dataset and anomalies dataset for secure facilities.

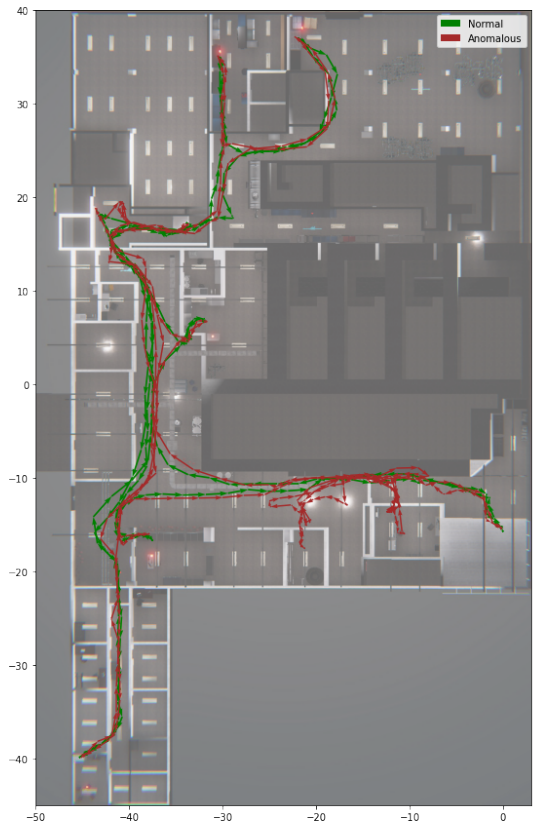

Fig. 3. Spatial-temporal movement trajectories visualized of the interactive user in the "normal"/PoL and the "anomalous" scenarios. (Note: the trajectories and background facility layout may be a little misaligned, and is not an artifact from *MetaPoL* but due to visualization used here.)

Using *MetaPoL* an interactive real human user can emulate normal/PoL activities as well as various anomalous activities (from a generated task list, or from own facility usage experience) in the virtual-physical facility. All these generate valuable indoor spatio-temporal datasets regarding movement and dwelling patterns in the facility through space and time. These datasets are very valuable for research and developments in patterns-of-life (PoL), anomaly detection, and, importantly, our mission/application focus on insider threats in nuclear security. To note that *MetaPoL* also integrated similar datasets generation capability from NPCs i.e., non-player characters (following models of spatial-temporal movement-dwelling) that represent other facility users. In the current stage of *MetaPoL* development, interactive real user can respond in behavior to the presence of NPCs. Future work include: automatic transition of interactive user in space and in time (for data generation through longer simulated time); social interaction between NPCs and interactive real user; allowing multiple interactive real users (multiplayer).

Acknowledgments:

This research sponsored by the Laboratory Directed Research and Development Program of Oak Ridge National Laboratory, managed by UT-Battelle, LLC, for the U. S. Department of Energy.

This manuscript has been authored by UT-Battelle, LLC, under contract DE-AC05-00OR22725 with the US Department of Energy (DOE). The US government retains and the publisher, by accepting the article for publication, acknowledges that the US government retains a nonexclusive, paid-up, irrevocable, worldwide license to publish or reproduce the published form of this manuscript, or allow others to do so, for US government purposes. DOE will provide public access to these results of federally sponsored research in accordance with the DOE Public Access Plan (https://energy.gov/downloads/doe-public-access-plan).

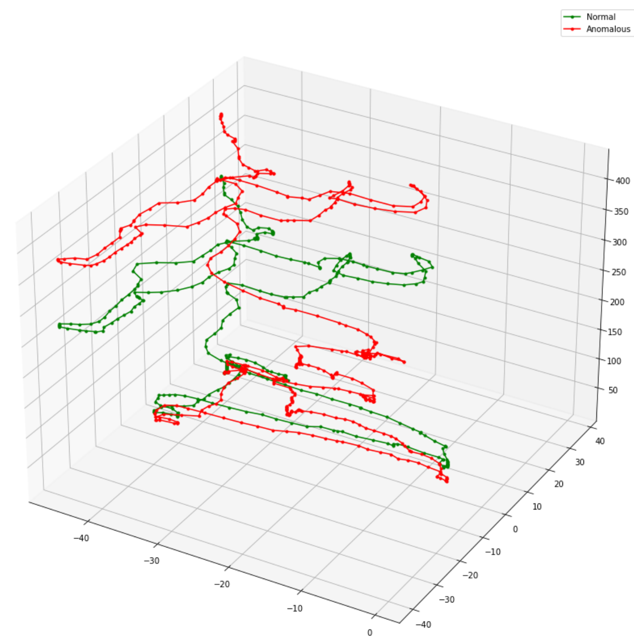

Fig. 4. 3-Dimensional visualization of the spatial-temporal movement trajectories of the interactive user. Here X and Y axis represent 2-dimensional x-y coordinates of the indoor space, while the vertical Z-axis represent time sequence (temporal granularity of data is every 1 second). The trajectories of the interactive user in both "normal"/PoL and "anomalous" scenarios are visualized.

References

[1] Enquiry into nuclear plant sabotage comes to no conclusion. Available online at: https://www.brusselstimes.com/181163/enquiry-into-nuclear-plant-sabotage-comes-to-no-conclusion, Friday, 13 August 2021.

[2] Meta quest pro vr headset. https://forwork.meta.com/quest/quest-pro/.

[3] Nnsa co-hosts international symposium on insider threat mitigation in brussels. Available online at: https://www.energy.gov/nnsa/articles/nnsa-co-hosts-international-symposium-insider-threat-mitigation-brussels, March 7, 2024.

[4] Unity real-time 3d development engine for immersive and interactive experiences. https://unity.com/products/unity-engine.

[5] Matthew Bunn and Scott D Sagan. A worst practices guide to insider threats: lessons from past mistakes. American Academy of Arts and Sciences Cambridge, MA, 2014.

[6] Colton Heffington, Adam D Williams, Shannon Abbott, Christopher Faucett, Sondra Spence, William Charlton, Katherine Holt, and Melinda Lane. Operationalizing insider threat potential and risk-significant insiders to enhance insider threat detection and mitigation. In *Proceedings of the INMM Joint Annual Meeting*, 2023.

[7] Scott D Sagan. Insider threats in comparative perspective. Technical report, IAEA-CN-203-156, Proceedings of International Nuclear Security: Enhancing ..., 2013.

[8] Steve S Sin and Kathryn A Lindquist. Datasets for modeling and mitigating insider risk final report and codebook. 2021.

[9] Adam D Williams, Shannon N Abbott, Nathan Shoman, and William S Charlton. Results from invoking artificial neural networks to measure insider threat detection & mitigation. *Digital Threats: Research and Practice (DTRAP)*, 3(1):1–20, 2021.