Investigation of Insider Identification by Using Human Bio-Monitoring

Nuclear Security and Emerging Disruptive Technologies: The Impact of Cyber and Artificial Intelligence

22 March, 2018

Hoam Faculty House, Seoul National University

Man-Sung Yim

Researchers: Young-A Suh, Jung-hwan Kim

NENS Nuclear Energy Environment and Nuclear Security Laboratory

KAIST Department of Nuclear and Quantum Engineering

Research Motivation (Problem Statement)

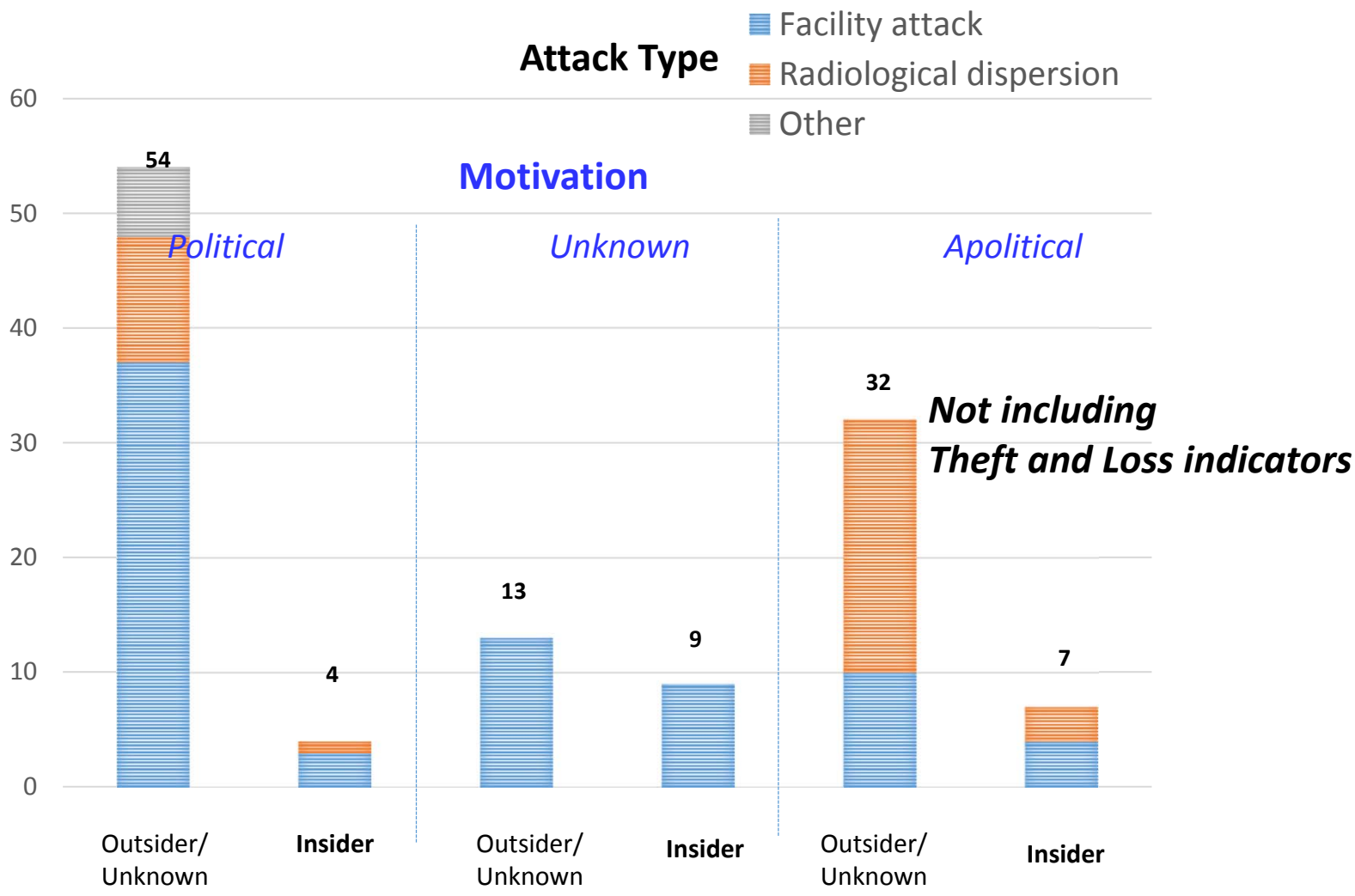


Fig.1. Distribution for 119 cases of serious nuclear and radiological incidents worldwide, from 1960-2013, by motivation, attack type, and insider involvement .

Source: WMD incident data (www.hegghammer.com)

INTRODUCTION

Problem Statement (1) Insider Threat Problem

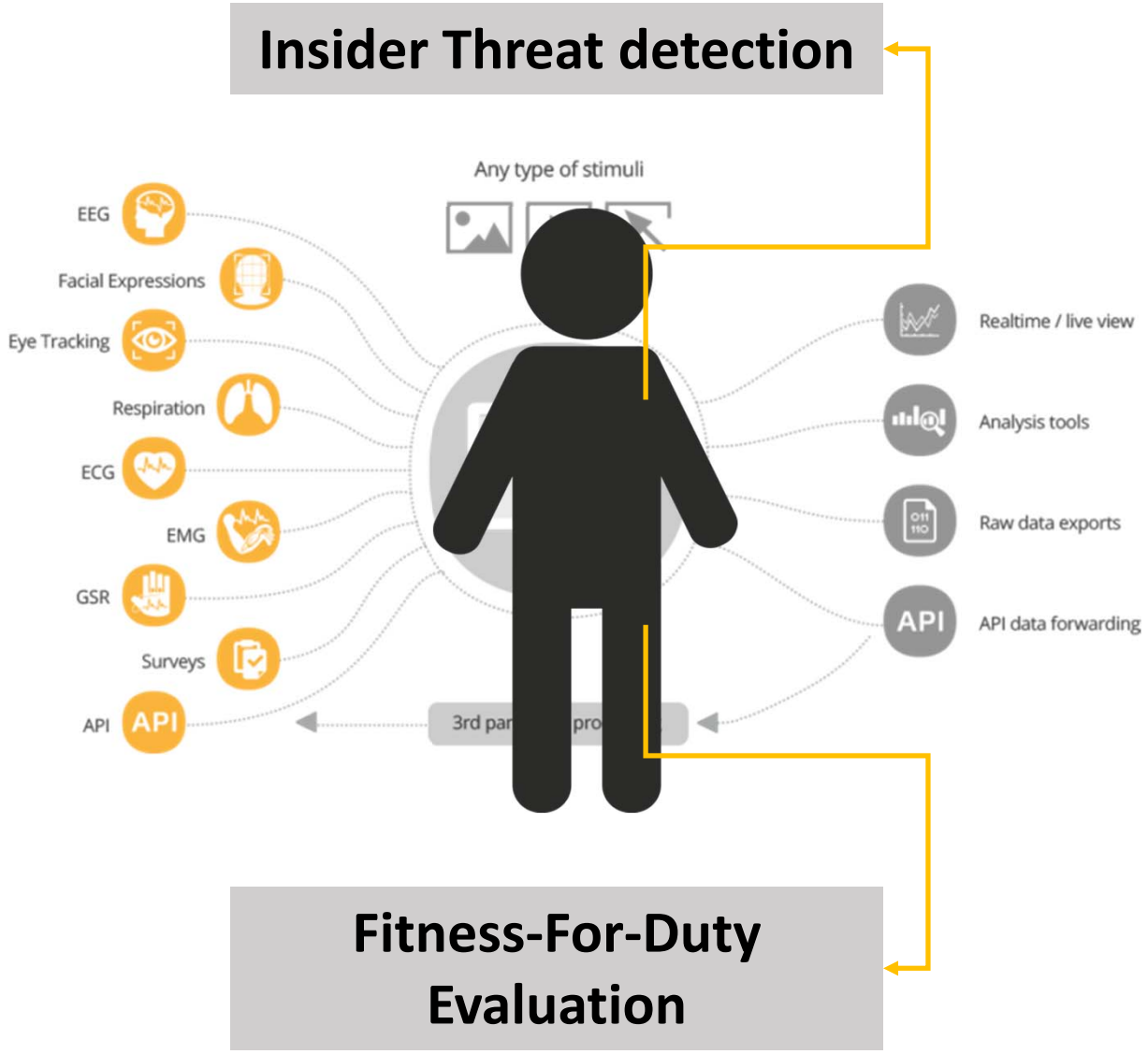
- The **insider threat** refers to harmful acts that a trusted insider might carry out (Schultz, 2002).
- **The importance of the insider threat**
  - Nuclear and International communities acknowledge demand
  - Indeed, disgruntled insiders at nuclear facilities have perpetrated many of the known acts of nuclear sabotage (Mott, 2007).
- **Current Status:** There are administrative and technical measures to prevent an insider threat.
- **Technical measure limitations**
  - The IAEA report (IAEA, 2008) mentioned **traditionally lots of focus on physical security against outsiders, which are a less difficult menace to detect than insiders** (Wolkov & Balatsky , 2013).
  - **Insiders can bypass many security safeguards by nature of their access authorization**.
- **Limitations of current administrative programs**
  - **1) Subjective and potentially biased.**
  - **2) Infrequently employed.**
  - **3) Reactive Approach.**

Research Hypotheses: EEG indicators may be useful to measure insider traits

	Specific features	Possible EEG Indicators
Emotional changes	Negative Emotion (fear, Sadness)	Frontal asymmetry Coherence Gamma
	Anger	F3-F4 Asymmetry
	Anxious	A selective increase in right parietal activity (P3-P4 or T5-T6).
	Worry	Alpha Increased gamma in left temporal and posterior area
Cognitive Change	High Stress	Alpha Theta
	High cognitive workload/ High engagement Poor decision-making Poor rational decision Poor emotional Understanding Poor social skill	Beta/(Alpha+Theta) Beta/Alpha Coherence Asymmetry
Malicious intention	Bad thinking/Willingness Impulse control capacity	Gamma/Alpha P300 N200

At-risk workers' psychological features and possible EEG based measurements

Overview of KAIST Research related to Human Bio-Monitoring



Research Objectives

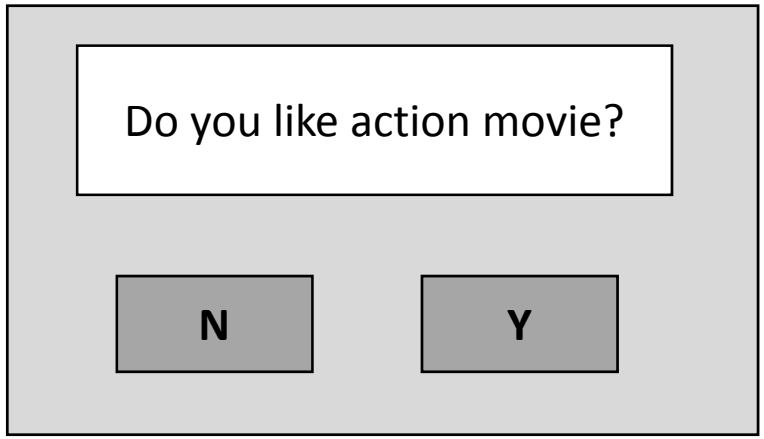
- **To utilize human bio-monitoring to minimize the risk** of **nuclear insider threats and human error**.

  - To examine the feasibility of using **Electroencephalogram(EEG) signal indicators** to identify p**otentially-at-risk workers,** especially those with malicious intentions in Nuclear Power Plants (NPPs)**.**

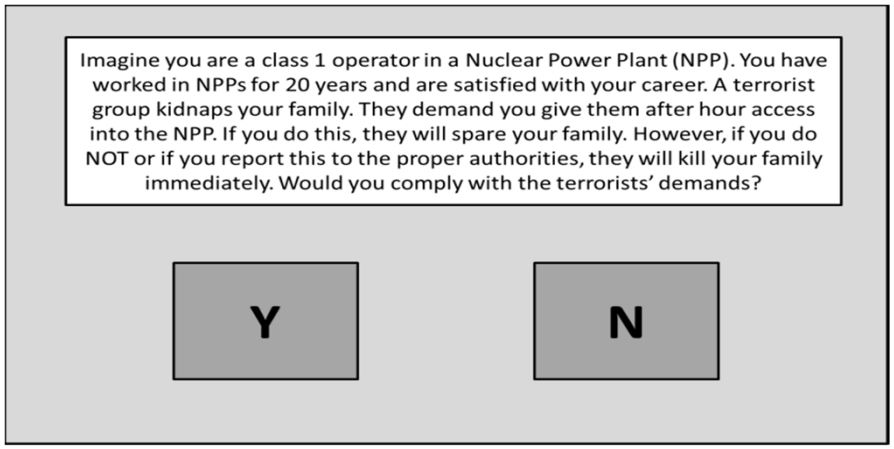
Research Method

Experimental Set-up

Task 1. Decision-making Tasks when a subject is placed in 140 situations similar to an insider



Casual Questions (20 questions)



Insider Situation-related Questions (140 questions)

- To verify the utility of the developed experimental tasks, the subjects were asked to perform two different sets of tasks.

According to literature reviews (Almehmadi, A., & El-Khatib, K., 2014 and Hashem, Y. , et al, 2015), **these experimental tasks are good trials for measuring an individual's malicious intentions.**

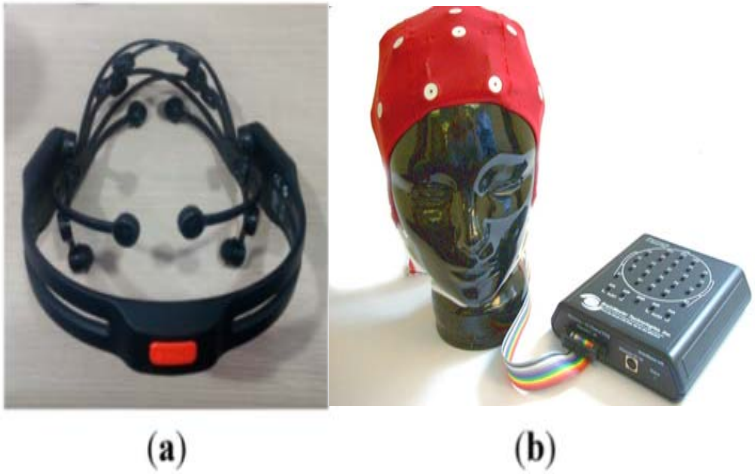
Task 2. Professor's Email Intrusion

- Eye Closed (EC): Normal Resting states.
- Eye Open (EO): Normal Resting states.
  - EC and EO: Check the health of subjects/ develop a baseline.
- **Internet Surfing:** Focus on the tasks but without malicious intent.
  - i.e., Open their email to check their work.
- **Professor's email Intrusion (malicious access, forbidden activity)** to find the answer sheet to a test.
  - If the subject gets a score of 100 on the test, they will get more prizes.

Research Method

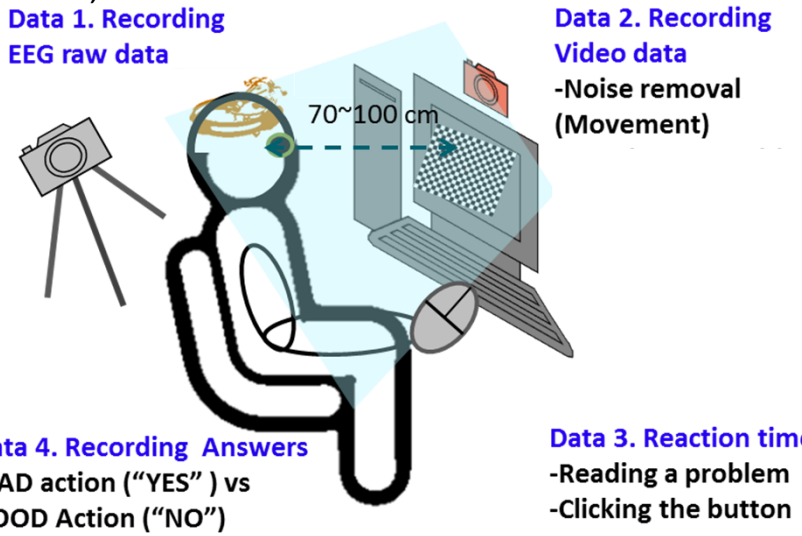
Experimental Set-up

- **Subjects and sample size**: 87 healthy subjects
  - **99.1% power (**the ability of a trial to detect a difference between two different groups) based on Post-Hoc Power analysis (Levine M & Ensom, MH. , 2001)
  - Age: mostly ~25 years old (except two people (60 years old))
    - The literature in 2012 (Taylor, G. S., & Schmidt, C. , 2012) , correlation were computed to determine the relationship between system performance and participant age, handedness and gender. No significant correlations were found (P>0.05 in each case).
  - Sex: 60 men and 27 women
  - Handed: 20 left-handed and 67 right-handed
  - Nationality: 10 from foreign countries and the others from Korea.
- **Stimulus** was mostly in **visual form (80% getting data from vision senses)** (Zeng, et al, 2009).
- **Controls:** Turn off the light, same room, silent environment, etc.



(a) The Emotiv EPOC equipment (Emotiv Inc., USA)
(b) Brainmaster Discovery 24e (BrainMaster Technologies Inc., USA)

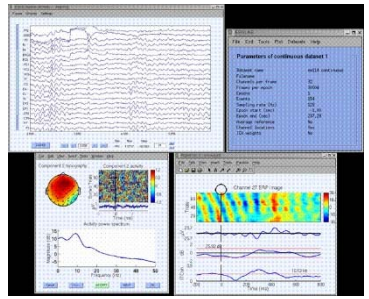
Depiction of experimental tools



Example of Experimental Setup

Research Method

Data processing



Present

EEG raw data → Preprocessing into FFT → Power spectrum Analysis → **Develop the indicators for measuring emotion and different mental state**

Develop the possible indicators

Develop the transform tool using MATLAB

$$X(k) = \sum_{j=1}^{N} x(j)\omega_N^{(j-1)(k-1)}$$

$$x(j) = (1/N)\sum_{k=1}^{N} X(k)\omega_N^{-(j-1)(k-1)}$$

where $\omega_N = e^{(-2\pi i)/N}$

is the N^{th} root of unity.

Equation 1. Discrete Fourier transform equation

1. Activation state

$$PF_{\frac{\beta}{\alpha}} = \frac{P_\beta}{P_\alpha}$$

2. cognitive state

$$PF_{\frac{\gamma}{\alpha}} = \frac{P_\gamma}{P_\alpha}$$

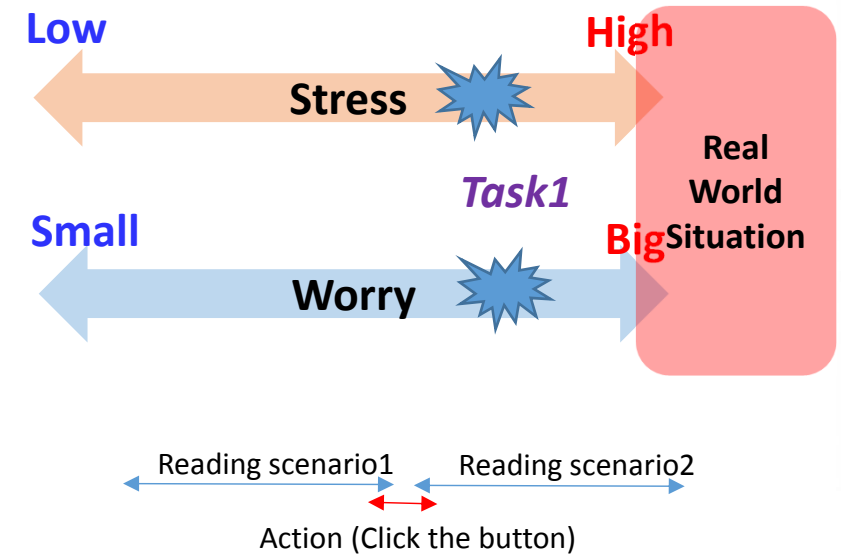
	Band	Frequency (Hz)	Normally	Brain state
Unconscious	Delta	1~4	Sleep, Continuous-attention tasks	Instinct
	Theta	4~7 Hz	Drowsiness, idling	Emotion, stress
Conscious	Alpha	7-13Hz	Relaxed/reflecting	Consciousness Vision function
	Beta	13-30Hz	Active thinking, focus, hi alert, anxious	Thought Busy, active concentration
	Gamma	30-50Hz	Short-term memory matching of recognized objects	Will Emotion

Characteristics of EEG rhythms

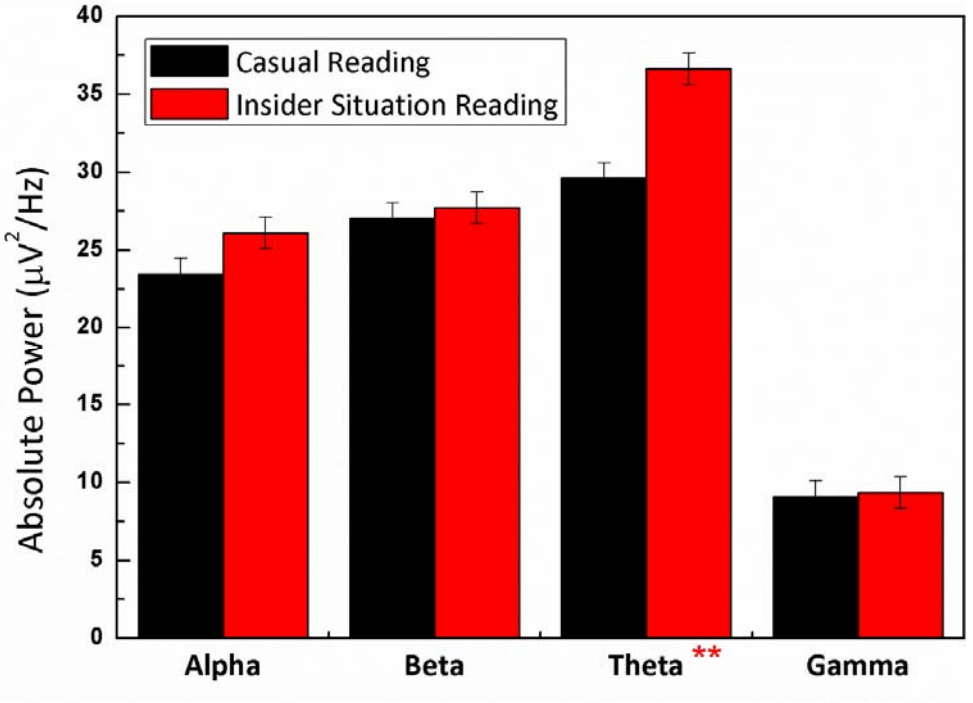
Results

Task 1. Decision-making Tasks when a subject is placed in a similar insider situation

Is it possible to realize the real insider case using experimental tasks?



Reading (Thinking about problem)

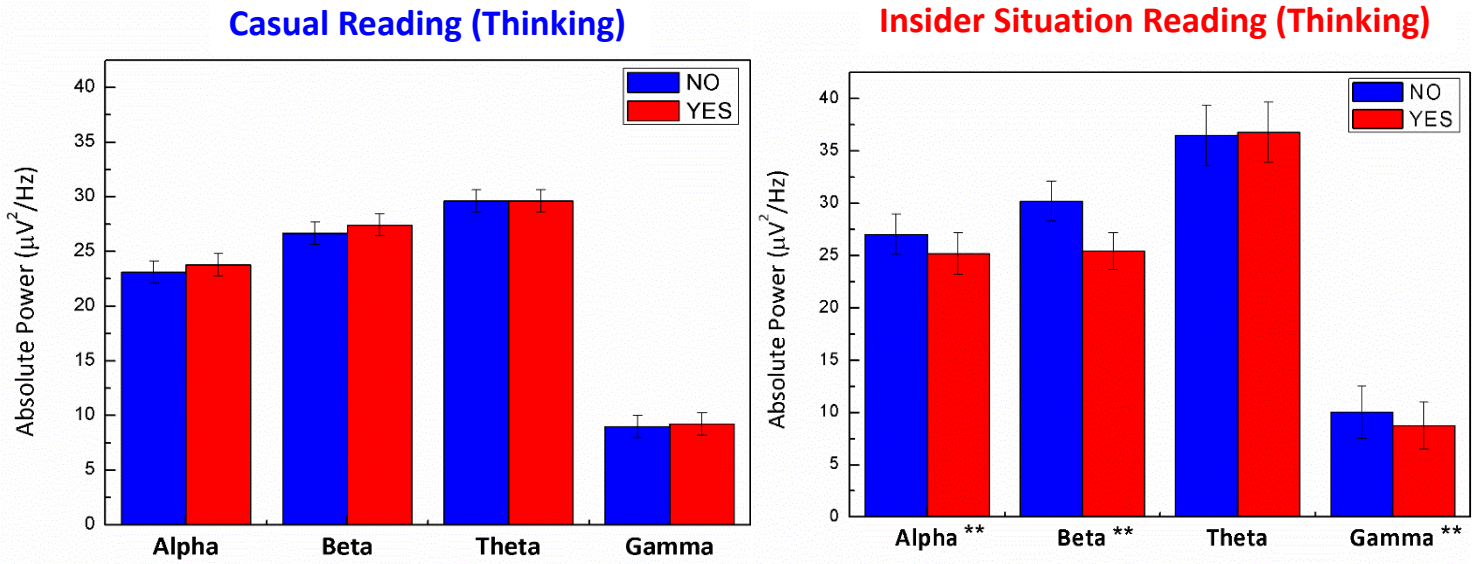


Absolute Power Difference Between Casual and Insider situation Reading (P-value<0.01)**

- An increase in the **"Theta" indicator** is associated with high mental stress (cognitive workload).
- The type of tasks, influence the theta indicator.
- Thus, for similar insider situations, our simulation (Task 1) can represent when a subject is placed in a high mental stress environment.

Results

Task 1. Decision-making Tasks when a subject is placed in a similar insider situation

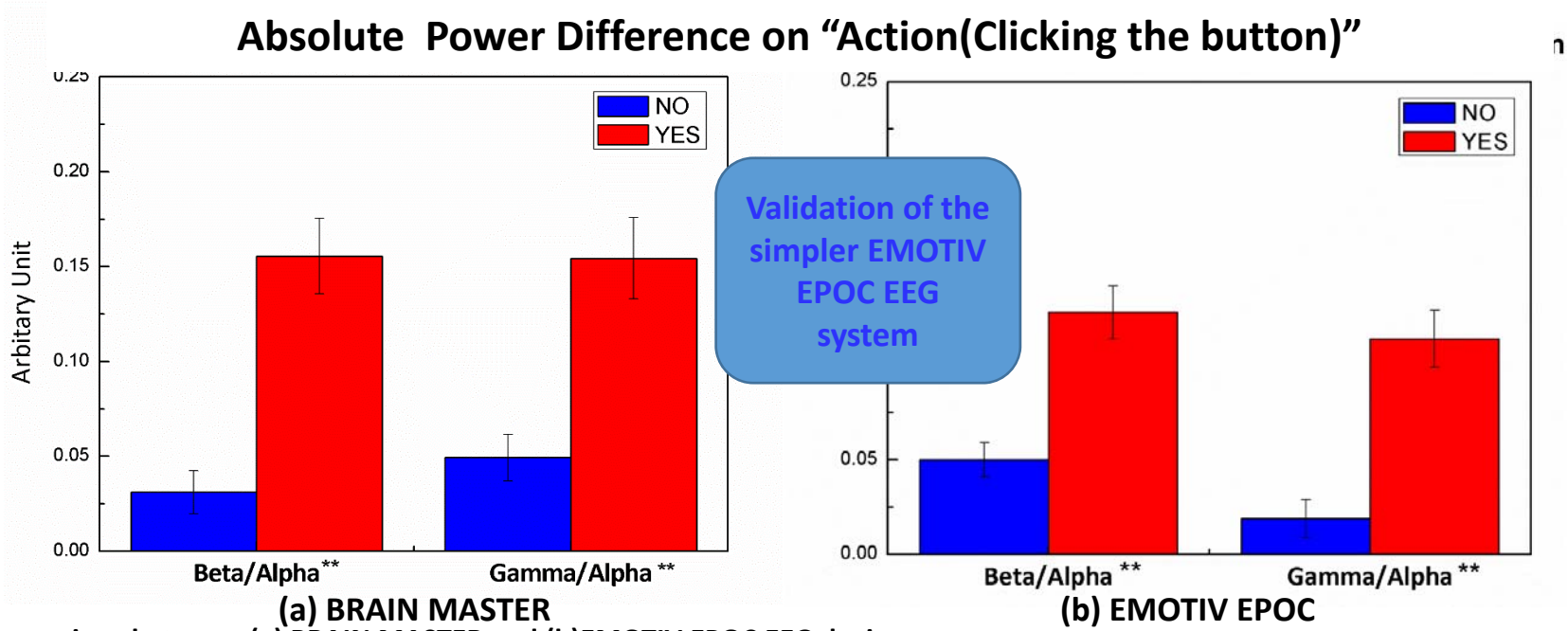


Comparison between (a) Casual Reading (Thinking) and (b) Insider situation Reading (Thinking)

- In decisions regarding casual questions, there were **NO significant differences** between YES and NO. However, in decisions related to insider situation, there were **significant differences** between YES and NO.
- Whether the outcome of a decision is good or bad, the cognitive thinking process of a potential insider (before committing to a decision) evoked significantly different patterns of changes in the EEG indicators.
  - The power **of "Alpha" decreased** significantly for the insider situation but not for casual reading.
    - When they thought their bad decision (YES), they felt more worry and fear.
  - The power of **"Gamma" slightly decreased** when they thought bad decision (YES).
    - This can be interpreted as a subject's willingness to decide YES (Bad decision) is weaker than NO.
    - Or, it can represents a subject's greater worry when he/she considers the NO button.
  - The power of **"Beta" decreased** significantly when they thought bad decisions (YES).
    - Usually , increasing "Beta" is related to conscious focus; high attentional level and problem solving (Gola, M., et al, 2013).
    - When a subject thought about committing a crime(YES), their cognitive processing was very high because of the volume of information to consider or their imagining they are a real NPP worker, can result in a decrease in Beta (Yuan, H., et al., 2010).

Results

Task 1. Decision-making Tasks when a subject is placed in a similar insider situation



Comparison between (a) BRAIN MASTER and (b)EMOTIV EPOC EEG devices.

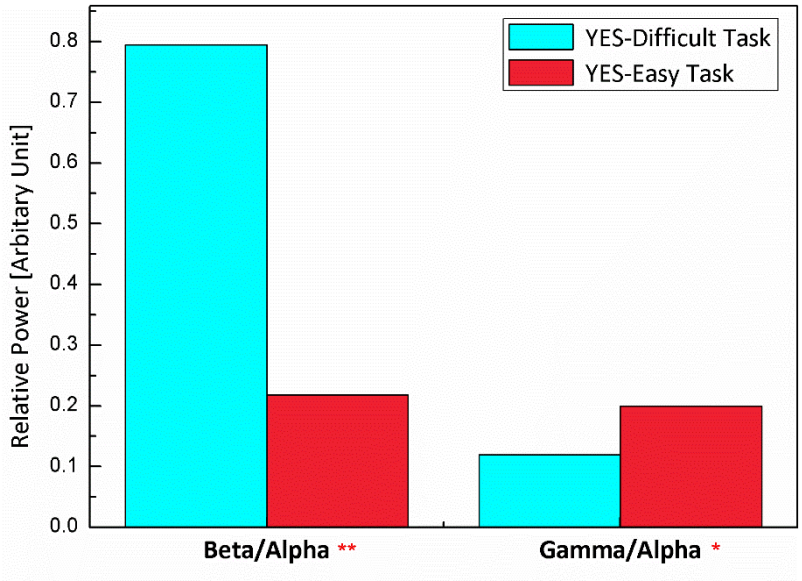
For all 140 scenario tasks, the significant indicator(P<0.01) differences between the two groups were marked as**.

BRAIN MASTER	EMOTIV EPOC
Non-wearable device (19channels)	Wearable device (14channels)
50 Subjects (Man:36, Woman:14)	37 Subjects (Man:24, Woman:13)

- **Fig 6. allows a quick identification of bad actor, supports current reactive program.**
- Depending upon whether the outcome of a decision is good or bad, **the corresponding decision making process of a potential insider (clicking YES or NO button) evoked significantly different patterns of changes in the EEG indicators.**
- Alpha and Theta and Gamma values were decreased, and "Activity" (Beta/Alpha) and "Willingness" (Gamma/Alpha) values were increased when the subjects made a decision to become an insider after a period of thinking about the actions required to becoming an insider.
- **Two indicators (Beta/Alpha and Gamma/Alpha) can be used to detect the insider right after committing a crime.**

Results

Task 1. Decision-making Tasks when a subject is placed in a similar insider situation



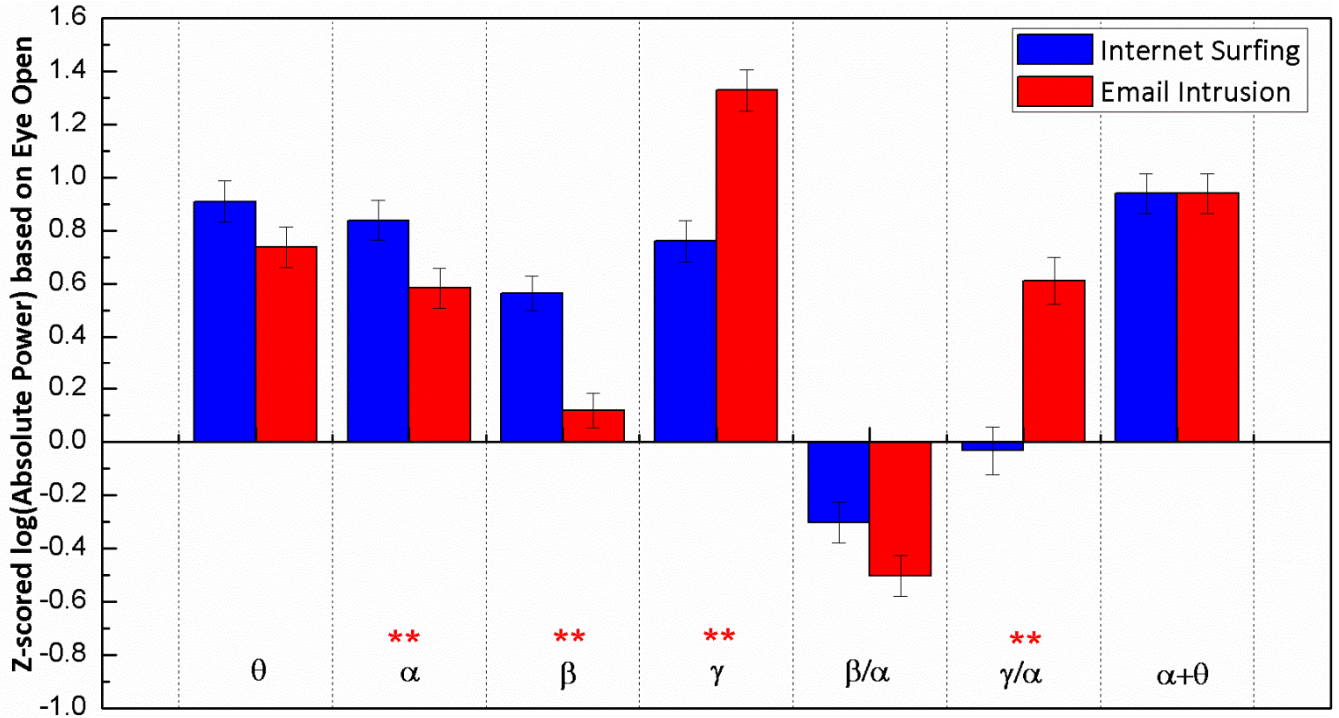
Variation in Difficulty of the Tasks reflect strength of two indicators for YES Response

- Expected difficulty of the tasks involved (i.e., outsiders' demands) is directly related to the type of an insider.
  - **Simple (easy) task** (i.e., Delivering a message or lending a security card): This could be carried by a non-violent passive insider.
  - **Difficult task** (i.e., Planting a bomb in a facility or releasing a biochemical weapon in an NPP): These types of tasks belong to the actions of a violent-active insider.

- When the subject's deep level thinking is in serious conflict with their highest life value priorities, he/she will hesitate in making the decision. Thus, the Gamma/Alpha between YES-difficult and YES-easy was decreased due to their weak willingness.
- The thinking process, when a subject was placed in a difficult task situation, was very busy and positively activated (i.e., he/she was really contemplating on carrying out the action). Thus, the Beta/Alpha between YES-difficult and YES-easy was increased due to their highly cognitive workload and engagements.
- These results indicate that the details of the variations of the scale of Gamma/Alpha and Beta/Alpha indicators may help to identify an insider's type.

Results

Task 2. Professor's Email Intrusion



Absolute Power Difference between non-malicious (surfing) and malicious activity (intrusion)

- When subject did **malicious action** (professor's email intrusion), the absolute power of:
  - **Alpha** indicator decreases (Fear or worry emotion, also true for an increase in the cognitive workload) ;
  - **Beta** indicator decrease (poor cognition);
  - **Gamma** indicator increases (worry and anxious feelings/ willingness); and
  - **Gamma/Alpha** indicator increases (big worry and strong willingness).

Results

Predicting the High Potential Insider (At-Risk Insider)

Machine learning (Training Set)		
Support Vector Machine (SVM) Fine Gaussian SVM	Classification Rate	85-96 %
K-Nearest Neighbor (KNN) Fine KNN	Classification Rate	91-98.8%
Prediction test		
Ability to Predict (SVM)	Validation Accuracy	0.9252-**0.9861**
Ability to Predict (KNN)	Validation Accuracy	0.9391-**1**

Classification Rate and Prediction Results

- **Use of machine learning**
  - For more accurate classification between YES and NO
  - To show the feasibility of predicting an At-risk insider based on "Activity" (Beta/Alpha) and "Willingness" (Gamma/Alpha) EEG indicators

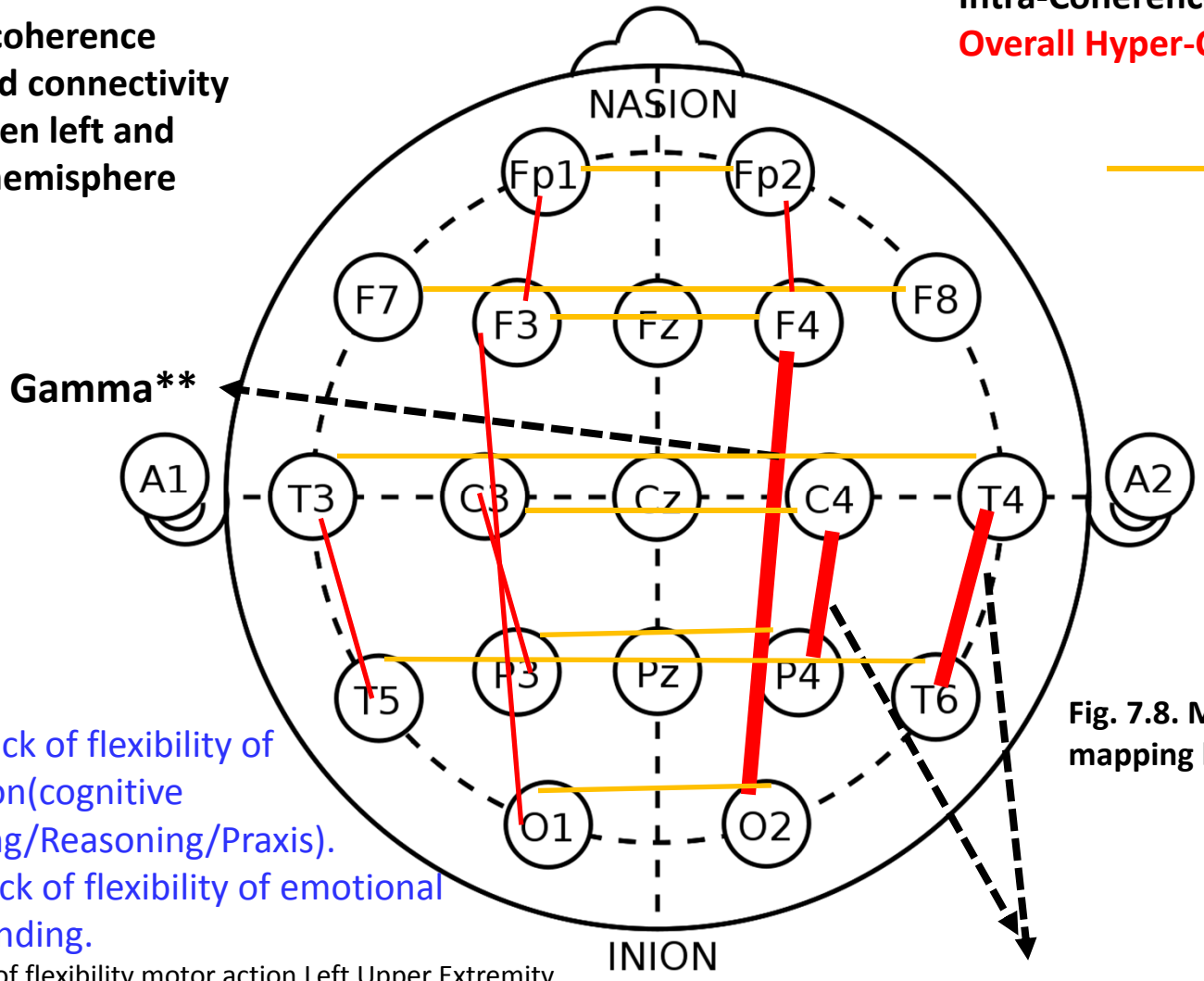
Classification Rate (Accuracy, %)=(True Positive +True Negative)/Total)

Malicious Intention Mapping-Coherence (brain function connectivity)

Inter-coherence
-> good connectivity between left and right hemisphere

Intra-Coherence
Overall Hyper-Coherence

0.8-1.0
Too strong



Gamma**

C4-P4: Lack of flexibility of perception(cognitive processing/Reasoning/Praxis).
T4-T6: Lack of flexibility of emotional understanding.
F4-O2: lack of flexibility motor action Left Upper Extremity (LUE) or visual sensation(left)

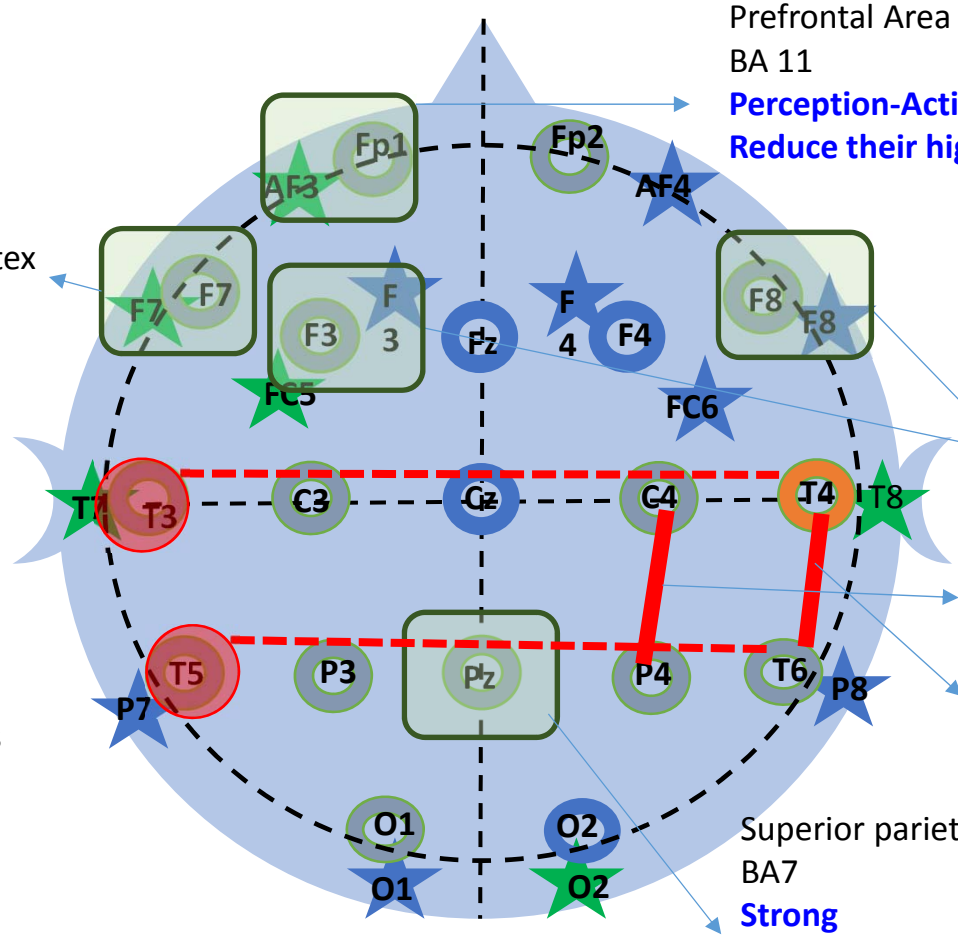
Theta, Alpha**, Beta**, Gamm**

Fig. 7.8. Malicious intentio mapping based on coherenc

Malicious Intention Mapping-Coherence (brain function connectivity)

EMOTIV

BRAINMASTER



Prefrontal Area
BA 11
Perception-Action(PA) Cycle
Reduce their high anxiety status

lateral prefrontal cortex
→ **Reward decision**

Risk choice
Impulse control (Inhibition)
Inferior frontal gyrus
BA44&45

Inter-asymmetry
Relatively gamma in **left temporal area (T3, T5)** is associated with negative emotional states (fear-sadness, worry).

Hyper coherence
C4-P4: Lack of flexibility of perception(cognitive processing/Reasoning/Praxis).
T4-T6: Lack of flexibility of emotional memory/understanding.

Superior parietal
BA7
Strong intention/motivation
Guilty emotion(Occurred P300 wave)

Malicious Intention Mapping

Summary of the Results

- The EEG frequency domain analysis showed that the selected indicators were useful as a quantitative measure to identify an “At-Risk (High Potential Risk)” insider.

- With the use of machine learning classification and these EEG indicators, “**identifying**” a high potential risk insider appears feasible.

- Possible explanations of the observed results from the channel analysis (malicious intention mapping) were proposed.

- The issue of information security needs to be addressed to implement the proposed approach to various security sensitive organizations.