



International Journal of Nuclear Security

Volume 2 | Number 3


Article 10

12-31-2016

Addressing the Tunnel Threat at Nuclear Facilities: A Case Study

Md. Mobasher Ahmed
University of Dhaka

Follow this and additional works at: <https://trace.tennessee.edu/ijns>

 Part of the [Defense and Security Studies Commons](#), [Engineering Education Commons](#), [International Relations Commons](#), [National Security Law Commons](#), [Nuclear Commons](#), [Nuclear Engineering Commons](#), [Radiochemistry Commons](#), and the [Training and Development Commons](#)

Recommended Citation

Ahmed, Md. Mobasher (2016) "Addressing the Tunnel Threat at Nuclear Facilities: A Case Study," *International Journal of Nuclear Security*. Vol. 2: No. 3, Article 10.

<https://doi.org/10.7290/v7gt5k34>

Available at: <https://trace.tennessee.edu/ijns/vol2/iss3/10>

This Article is brought to you for free and open access by Volunteer, Open Access, Library Journals (VOL Journals), published in partnership with The University of Tennessee (UT) University Libraries. This article has been accepted for inclusion in *International Journal of Nuclear Security* by an authorized editor. For more information, please visit <https://trace.tennessee.edu/ijns>.

Addressing the Tunnel Threat at Nuclear Facilities: A Case Study

Md. Mobasher Ahmed

M.S. Student, Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh

Omar Ahmed

M.S. Student, Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh

Md. Shafiqul Islam

Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh

Abstract

In this paper, a tunnel threat at nuclear facilities is introduced as a case study. A tunnel threat detecting sensor-based physical security system is presented, and a real time alert of tunnel digging by adversaries around the nuclear facilities is illustrated. This paper also describes the system design for tunnel threat detection, geophone sensor-based detection techniques, and how to response to that threat through an alarm and wireless communication system. This study claims that tunnel threats are not yet considered in designing the physical protection systems at existing nuclear facilities. The proposed tunnel threat detection system is a timely approach to designing the robust physical protection system of nuclear facilities. The inclusion of tunnel threats along with other threats will no doubt enhance the nuclear security regime of nuclear installations.

I. Introduction

Worldwide emerging adversary groups are using innovative techniques to conduct terrorist activities. They are using state-of-the art technology and hacking tools. The peaceful uses of radioactive and nuclear materials for power generation, research, medicine, and industry solely depends on their safe and secured handling at all nuclear installations. But the possible threat is that potential adversaries such a terrorists, criminals, extremists, hackers and insiders may try to gain fissionable nuclear (U-235, Pu-239) materials and/or radioactive materials (Cs-137, Co-60, Po- 210, Sr-90) for malicious purposes due to their ideological, economic and personal motivations. Often, the adversary groups clearly state their intention to inflict catastrophic casualties through making nuclear or radiological weapons with the capability of mass destruction. These terrorist activities are now a real and growing concern of the international

community and force the community to enhance nuclear security. The International Atomic Energy Agency (IAEA) states that between 1993 and 2013, 2477 nuclear incidences of illegal trafficking, theft or loss of nuclear and radiological materials are documented around the world of which only 40% has been recovered [1].

The prevention, detection of, and response to sabotage, unauthorized access, illegal transfer, theft, or other dangerous activities involving nuclear materials, radioactive substances, or their associated facilities is known as nuclear security.

The well-accepted nuclear security measures are physical protection systems, material control, and material accounting systems. Physical protection systems provide for the detection of any unauthorized penetration to barriers, portals and other security measures and trigger an immediate response to such penetrations, including the use of force if necessary. J. T.K. Mao and A Salvi present an approach to the design and installation of a plant security system in a nuclear power plant [2]. V. Sequeira, et al. describe 3D site modeling and verification of plant design for nuclear security applications [3]. Ryosuke Watabe, et al. propose security design of remote maintenance system for nuclear power plants [4].

Material control systems prevent illegal movement of materials and are provided for the prompt detection of theft or diversion of material. There are several techniques proposed including nuclear forensics and nuclear material detection to prevent the transport and use of nuclear materials [5–12]. Material accounting systems ensure that all materials are accounted for, enabling the measurement of losses and providing information for follow-up investigations of irregularities.

Nuclear terrorism is the use of nuclear or radioactive materials by adversaries to cause fear or to achieve political aims. Nuclear terrorism may also include radioactive materials used in medical, industrial, scientific research applications, and nuclear waste. A dirty bomb might be developed by the dispersal of these materials [13]. Sabotage of a nuclear facility is yet another form of nuclear terrorism [14–16]. Nuclear terrorism could be represented in several ways such as the use of a nuclear weapon, radiological terrorism, and nuclear or radiological sabotage [17–20].

The U.S. Nuclear Regulatory Commission (NRC) develops the design basis threat (DBT) based on its regular interactions with law enforcement authorities and federal intelligence. The design basis threat describes general characteristics of adversaries such as terrorists, criminals, extremists, hackers, and insiders that nuclear facilities must defend against to prevent threats to nuclear facilities.

Recent terrorist events have served as an impetus for the development of an array of new nuclear security regulation. Although malicious acts involving nuclear installations is not new, recent terrorist events have demonstrated that an attack on a nuclear facility might be undertaken and that terrorists have terrific capabilities and dedication. Recently, terrorist are showing their willingness to inflict mass casualties and announcing their intention to acquire nuclear materials. Particularly after September 11, 2001, protecting nuclear power reactors against terrorist groups worldwide has attracted the crucial attention of security and technical/scientist analysts. This has led to an increased focus on defense against terrorists at nuclear facilities as well as at other critical infrastructures. So it is imperative to find the new potential threats to nuclear facilities and to develop regulations.

Digging tunnels under the ground of nuclear facilities presents a threat to both military and law enforcement of a country. Criminals with intentions of avoiding border security have turned tunnels into transit routes for trafficking weapons, people, drugs, and other illegal materials. Many times prisoners have used underground tunnels to escape the prison. While drug and human trafficking have long been border concerns, the threat of international terrorism has transformed the effort to detect tunnels into a national security priority.

Terrorist attacks through tunneling are not new events or tactics. There are several examples of such events around the world. About 150 tunnels were discovered around the US-Mexico border, which were being used to smuggle drugs and other illegal items [21]. Hezbollah and Hamas in Gaza have been using tunnels for quite some time to smuggle weapons and launch attacks against Israel. Tunnel bombs are also emerging as a threat to global security. In Iraq ISIS is using tunnel bombs to blow up buildings and other targets. In Syria several of these tunnel bombs were detonated [22]. To this extent, nuclear facilities might face such tunnel threats in the future, and it should be a significant concern for regulators and operators. As far we know, this type of threat is not yet considered in designing the physical protection system (PPS) of nuclear power plants or any other nuclear facilities. This can be considered a potential threat when design basis threat (DBT) is analyzed.

The objective of this paper is to address the tunnel threat at nuclear facilities and to provide a tunnel threat detection-based security system to nuclear power plants and other nuclear facilities.

In this paper, we describe a tunnel threat detection-based security system, which is well suited to detect tunnel threats as well as to provide real-time alerts of digging. This paper is arranged by describing system design for tunnel threat detection in section II; the detection procedure in section III; the response to the threat in section IV; and the conclusion in section V. The threat assessment procedure of the total system is described in the next section.

II. System architecture for tunnel threat detection

Underground tunnels can be a potential threat for nuclear power plants, research reactors, and hospitals where nuclear materials and radioactive sources are kept. It is necessary to find a way to detect and neutralize this threat.

In our tunnel threat detection system, we have shown that the central alarm station (CAS) at the protected area gets signals from the underground tunnel detection sensors outside of the controlled area. Figure 1 shows the graded approach to the tunnel threat detecting security system for physical protection of a nuclear power plant. In Fig.1, the CAS, which is located in the protected area of the nuclear power plant, gets information about tunnel threats from the tunnel detection sensors through a signal-processing device at the controlled area.

In Fig.1, the tunnel detection sensors are located outside the controlled area and completely surround it. These tunnel detection sensors will be inserted into the ground. According to the tunnel detection range of the sensors as well as our acceptable range, the sensors are inserted at a certain depth into the ground. These tunnel detection sensors are placed at distance from each other so that the detection range will overlap which increases the tunnel detection capability. With any signal from underground, the tunnel detection sensor gives a particular response to the signal-processing device.

The signal processing devices are placed inside the controlled area as shown in Fig.1. In the signal-processing device, the signal produced in the tunnel detection sensor is processed in real time using an advanced algorithm. The signal processing devices will typically take the form of a small, weatherproof box, mounted on the ground. One signal-processing device receives signals from a multiple numbers of sensors closest to it and a number of signal processing devices are used to cover all the sensors. In Fig.1, we have showed four signal processing devices.

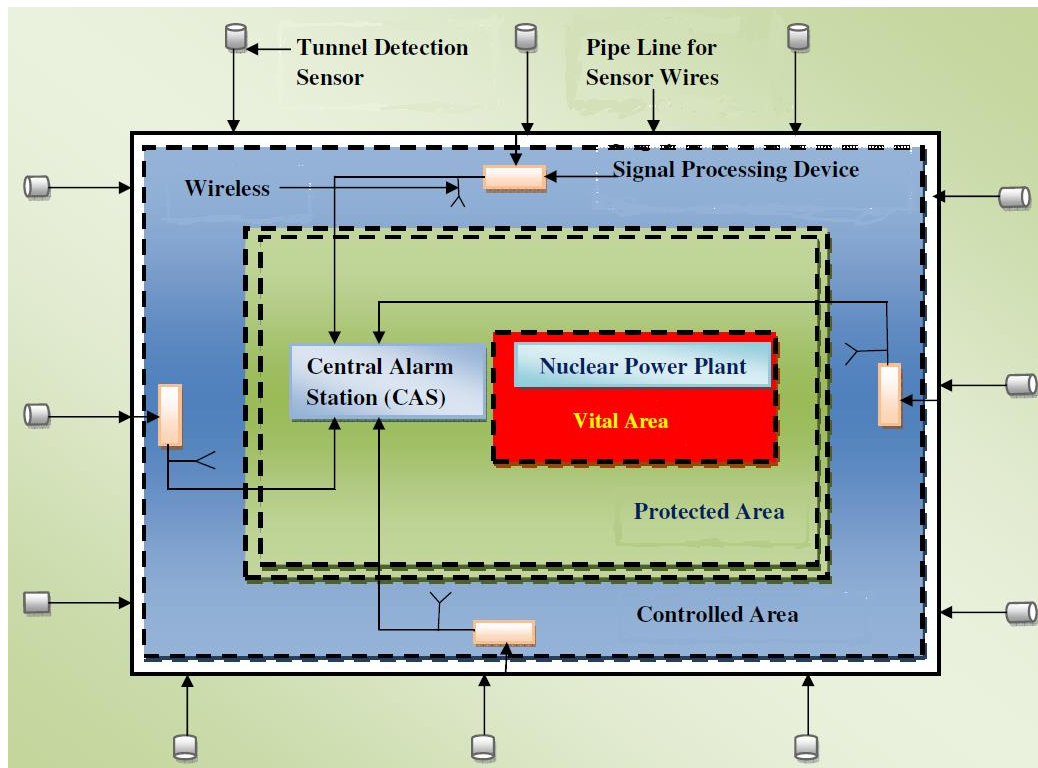


Figure 1. Graded approach for the tunnel threat detecting security system

The signal processing devices transmit the signal to the CAS situated in the protected area. In this tunnel threat detecting security system as shown in Fig. 1, there are two possible ways to transmit signals, including through wired and wireless transmission to the CAS from signal processing devices. Figure 1 shows that the CAS receives signals from all of the signal processing devices.

The transmitter associated with the signal-processing device transmits the data to the CAS. There is an alternative way for data transmission. This is in case a technical problem occurs. For example, if the transmitter were damaged. By using Ethernet or some other wired system, data can be transmitted to the central alarm station. With the data, a notification will be sent to the CAS relaying that the transmitter needs to be fixed so that steps can be taken to fix it. The CAS is a room which houses the monitors for the security equipment, terminals to the access control computer, and emergency communication equipment. The CAS monitors all the security issues in the nuclear power plant. The CAS analyzes the signals from the tunnel threat detection sensors through the signal processing devices. When any tunnel threat is detected, the CAS will generate an alarm and inform security personnel about the tunnel threat as well as the tunnel threat location.

The overall layout of our tunnel threat detecting security system is presented in Fig. 2. Figure 2 depicts three tunnel threat-detecting sensors, which receive signals from underground tunnel activity and send the signals to a signal-processing device. After preprocessing the received signal, the signal-processing device sends it to the CAS via wireless transmitter or wired connection. The antenna then receives the signal and sends it to the CAS. This antenna also can broadcast alert messages to security personnel.

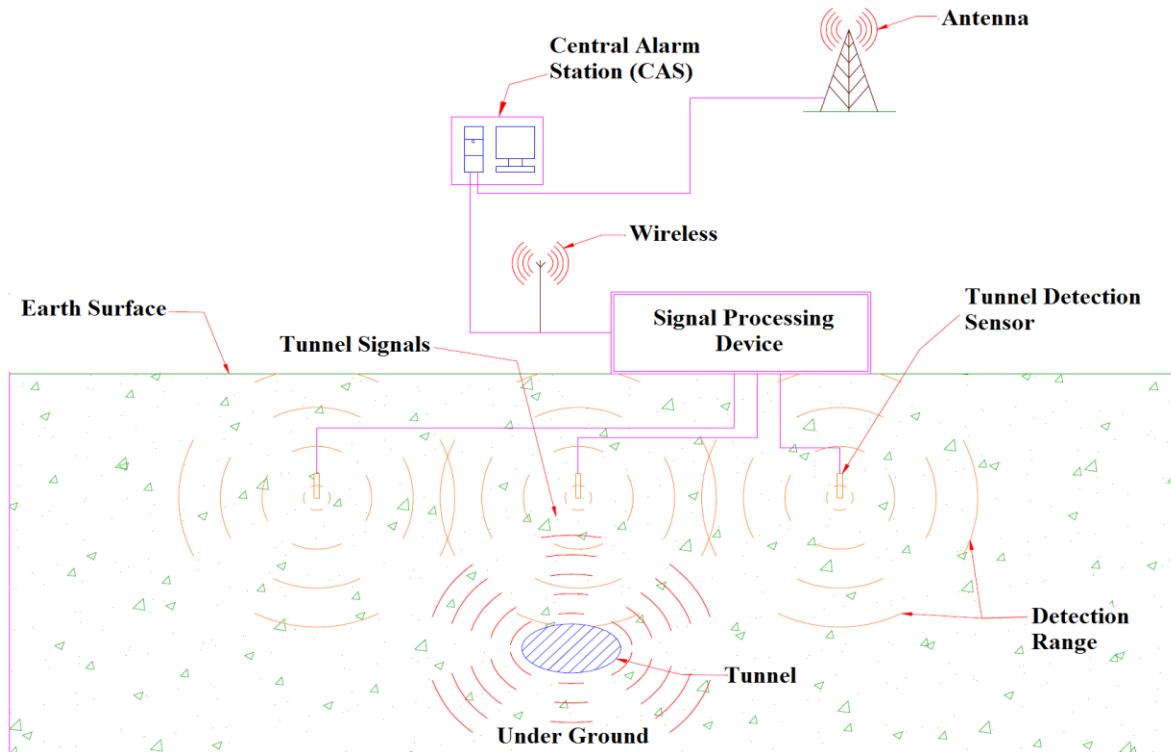


Figure 2. Overall layout of the tunnel threat detecting security system

In this tunnel threat detecting security system, the CAS receives signals of tunnel threats from tunnel detection sensors through signal processing devices and takes the required steps to handle the threat, which is shown as block diagram in Fig. 3.

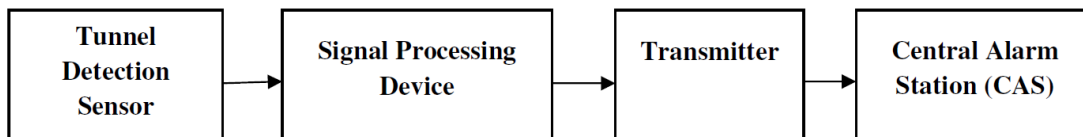


Figure 3. Block diagram of the tunnel threat detection system

III. Detection Procedure

The detection procedure of this tunnel threat detecting security system can be described in three stages of detection: the response of the tunnel detection sensors; the preprocessing of the signals from the sensors at signal processing device; and the threat signal detection at CAS.

In tunnel threat detecting sensors, geophone-based seismic sensors are placed into the ground. They would be adjustable to various types of terrain e.g. sand, clay, soil, etc. A geophone is a ground motion transducer. It converts ground movements into voltage. A typical geophone is manufactured by hanging a mass by a spring. With the application of a velocity at frequencies lesser than the resonance frequency, the geophone housing and the hanging mass start moving. If frequencies are greater than the resonance frequency, the mass will remain stationary. The motion of mass is based on either magnets or coils. The response of a magnet or coil geophone is proportional to the ground velocity. A basic schematic drawing of a tunnel threat-detecting sensor is shown in Fig. 4.

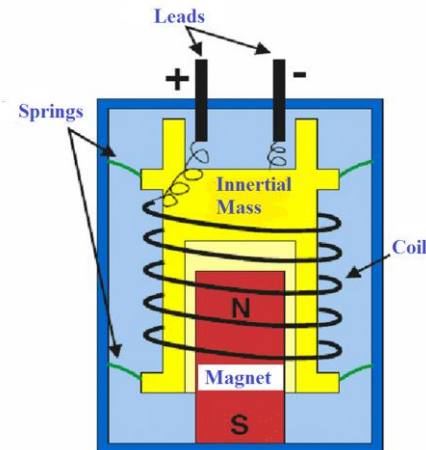


Figure 4. Schematic drawing of a tunnel threat-detecting sensor.

When an activity is registered within the area, the tunnel threat-detecting sensor produces a signal that is analyzed in real time using computer algorithms to identify the type of registered activity. The geophones can be installed at varying depths and distances from each other. Each geophone has an adjustable detection range that can usually be overlapped by some units to increase reliability. By design, the installation of sensors can be divided into the areas of revelation. In this method, a tunnel threat-detecting sensor responds to tunneling activity. The schematic diagram of the tunnel threat detection method is shown in Fig. 5. Figure 5 shows that signals from the tunneling activity spread all around the underground, and the sensors near the tunnel respond to the signal.

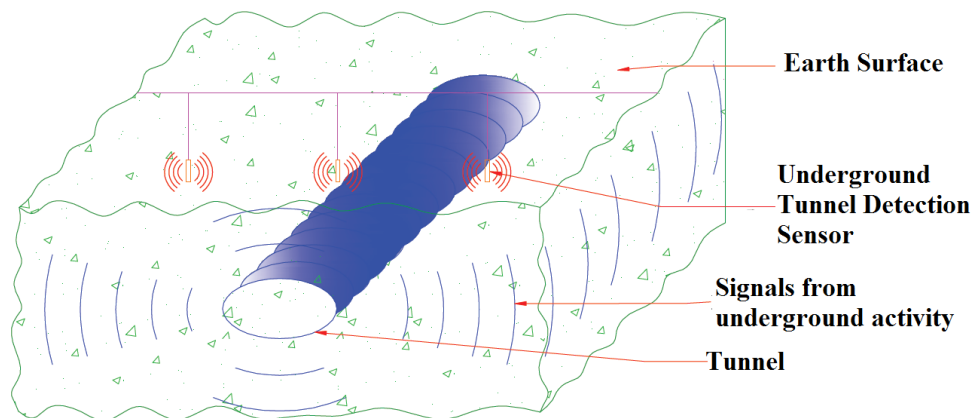


Figure 5. Detection method for tunnel threat

Preprocessing of the signals from the sensors is done at the signal-processing device where advanced intrusion recognition algorithms can be adopted to analyze the seismic signals to effectively filter out the false alarms. This is so the unwanted noise cannot interrupt the original tunnel threat signal, which is shown in Fig. 6. This smart signal processing will provide a high possibility of detection and an extremely low false and nuisance alarm rate.

At the CAS, a computerized system will further process the digital signals (Digital Signal Processing (DSP)) picked from the signal-processing device and display the results over the monitors of the CAS. A system can also be developed to send messages to the cellular phones of security personnel. When a

tunnel threat is observed, the CAS can respond quickly. Figure 6 shows the tunnel threat signal detection procedure.

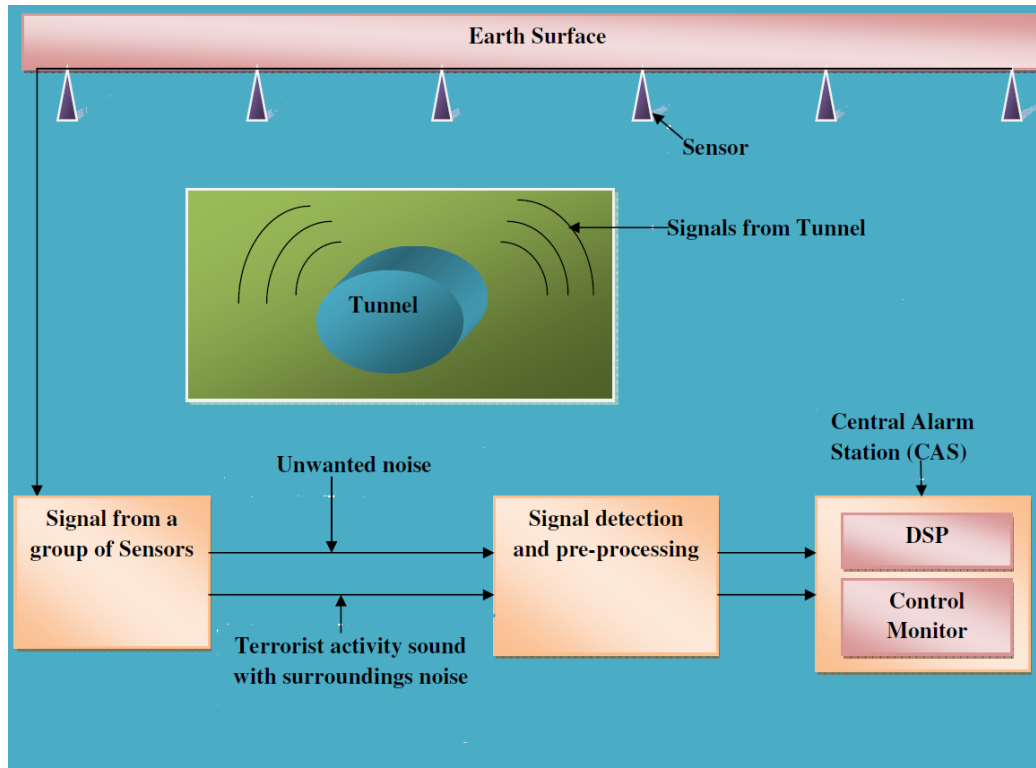


Figure 6. Signal detection system for tunnel threat

IV. Response To

A computer collects the data and analyzes it in real time. By using advanced computer algorithms, it is possible to differentiate between a real threat and a false alarm. This differentiation is required because it might be caused by an animal or a pedestrian whose movement triggered the alarm. To confirm the threat, real drones or quad-copters controlled from CAS can be used to inspect the location where activity is detected. Drones can inspect the area of occurrence by using ground-penetrating radar (GPR). Drones can also be used to check for any signs of explosives or weapons. Security personnel near the location of occurrence can also perform this. If the detected threat is real, the system will automatically trigger the alarm and indicate the level of threat, which will help security personnel take immediate action to locate the site where the threat is detected and take proper measure to neutralize the threat.

To facilitate this action, computer programs can be written which will locate and send an automatically generated alert message containing the location of the area in which the threat has occurred to security personnel, nearest to the area of occurrence. By using this procedure, time and resources can be saved.

V. Conclusion

In order to prevent, prohibit, and respond to malicious acts involving radioactive materials, nuclear materials, and their associated facilities, this paper introduces a new possible threat termed as 'tunnel threat' to nuclear facilities and describes a tunnel threat detecting security system. This tunnel threat detection system can easily be interfaced with the CAS of nuclear facilities. The geophone sensor-based tunnel threat detecting system can be considered a reliable system. In this system, we have proposed the use of drones for further site inspections in order to identify the exact location of the threat as a counter

measure. To respond immediately against the tunnel threat received from the CAS, the message could be forwarded to the security personnel using the broadcasting antenna. This study claims that tunnel threats should be taken into account with the design basis threat (DBT). Hence, designing physical security systems at nuclear installations needs to address tunnel threats along with other threats in order to enhance the nuclear security regime.

VI. Works Cited

1. IAEA, Incident and Trafficking Database (ITDB) (2013), (available at <http://www-ns.iaea.org/security/itdb.asp>).
2. J. T. K. Mao, A. Salvi, Design Considerations and Features for a Nuclear Power Plant Security System. *IEEE Trans. Power Appar. Syst.* **PAS-100**, 4493–4501 (1981).
3. V. Sequeira, G. Bostrom, M. Fiocco, D. Puig, J. G. M. Goncalves, in *2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '05) - Workshops* (2005), pp. 127–127.
4. R. Watabe, T. Oi, Y. Endo, in *SICE, 2007 Annual Conference* (2007), pp. 1700–1704.
5. E. Peskie, H. Hall, Radiation Damage as a Possible Metal Chronometer for Pre-Detonation Nuclear Forensics. *Int. J. Nucl. Secur.* **1** (2015), doi:10.7290/V7W66HPT.
6. E. Peskie, H. Hall, Impurity Diffusion as a Possible Metal Chronometer for Pre-Detonation Nuclear Forensics. *Int. J. Nucl. Secur.* **1** (2015), doi:10.7290/V7RF5RZ3.
7. H. Gowadia, B. Mardigras, The Department of Homeland Security's Approach to Countering Nuclear Terrorism through Detection and Technical Forensics. *Int. J. Nucl. Secur.* **1** (2015), doi:10.7290/V7V985ZR.
8. H. Yang, D. K. Wehe, in *2009 IEEE Nuclear Science Symposium Conference Record (NSS/MIC)* (2009), pp. 898–903.
9. J. A. Webster, Tensioned Metastable Fluid Detectors in Nuclear Security for Active Interrogation of Special Nuclear Materials—Part B. *World J. Nucl. Sci. Technol.* **1**, 66–76 (2011).
10. T. Köble, W. Rosenstock, M. Risse, J. Engelen-Peter, “Detecting Fissionable Material from a Travelling Vehicle by Neutron Coincidence Measurement,” *INMM 43rd Annual Meeting* (Orlando, FL, 2002).
11. T. Köble, W. Rosenstock, M. Risse, J. Peter, “Detection of Nuclear Material During Fast Road Transport,” *INMM 44th Annual Meeting* (Phoenix, AZ, 2003).
12. W. Rosenstock, W. Berky, S. Chmel, H. Friedrich, T. Köble, M. Risse, “Covert Search and Detection of Illicit Nuclear as Well as Radioactive Material” (Fraunhofer-Verbund Verteidigungs- und Sicherheitsforschung VVS, Karlsruhe, Germany, 2009), pp. 176–185.
13. M. Bunn, *Securing the Bomb* (Harvard University, USA, 2008; http://belfercenter.hks.harvard.edu/publication/18672/securing_the_bomb_2008.html).
14. The Code of Conduct on the Safety and Security of Radioactive Sources (2004), (available at http://www-pub.iaea.org/MTCD/publications/PDF/Code-2004_web.pdf).

15. IAEA, “The Convention on the Physical Protection of Nuclear Material, INFCIRC/274/Rev.1” (Vienna, Austria, 1980), (available at <https://www.iaea.org/sites/default/files/infcirc274r1.pdf>).
16. IAEA, “Regulations for the Safe Transport of Radioactive Material, IAEA Safety Standards Series No. RS-G-1.9” (2005), (available at http://www-pub.iaea.org/MTCD/publications/PDF/Pub1225_web.pdf).
17. IAEA, “Categorization of Radioactive Sources,” *IAEA Safety Standards Series No. RS-G-1.9* (Vienna, Austria, 2005), (available at <http://www-pub.iaea.org/books/IAEABooks/7237/Categorization-of-Radioactive-Sources>).
18. IAEA, “Physical Protection Objectives and Fundamental Principles, GOV/2001/41” (GOV/2001/41, Vienna, Austria, 2001), (available at <https://www.iaea.org/About/Policy/GC/GC45/Documents/gc45inf-14.pdf>).
19. IAEA, “Nuclear Security Culture,” *Nuclear Security Series No. 7* (Vienna, Austria, 2008), (available at <http://www-pub.iaea.org/books/IAEABooks/7977/Nuclear-Security-Culture>).
20. IAEA, “The Design Basis Threat”, Nuclear Security Series No. 10, Vienna, Austria, 2009.
21. T. Sanchez, U.S. and Israel Unite to Fight Border Tunnel Threats. *Truth Revolt* (2015), (available at <http://www.truthrevolt.org/news/us-and-israel-unite-fight-border-tunnel-threats>).
22. M. Weisgerber, ISIS Is Using Tunnel Bombs in Iraq. *Def. One* (2015), (available at <http://www.defenseone.com/threats/2015/06/isis-using-tunnel-bombs-iraq/114730/>).

VII. Authors’ Bio and Contact Information

Md. Mobasher Ahmed - is a M.S. student at Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh. Contact: md.mobasher@gmail.com

Omar Ahmed - is a M.S. student at Department of Nuclear Engineering, University of Dhaka, Dhaka-1000, Bangladesh. Contact: omarahmed8923@gmail.com

Dr. Md. Shafiqul Islam - PhD. in Thermalhydraulics in Nuclear Reactors, Saga University, Japan is an Associate Professor, Department of Nuclear Engineering, University of Dhaka, Dhaka 1000, Bangladesh. He has broad experiences in thermalhydraulics and is skilled in heat transfer & fluid flow characteristics. He has about eight years work experiences on research reactor operation and maintenance activities, nuclear reactor safety, security and safeguards matters during his past job at Bangladesh Atomic Energy Commission (BAEC). He has participated on nuclear safety, security and safeguards related technical meetings, workshops, and seminars at IAEA, USA, Japan, and Canada. He can be reached at msislam@du.ac.bd