A Secure Novel Sensor Fusion Architecture for Nuclear Applications

Mohammed Khasawneh[1], *IEEE Senior Member*, **Rizwan-Uddin**[1]
Nuclear, Plasma, and Radiological Engineering
mkha@ieee.org, rizwan@uiuc.edu

Mohamad I. Malkawi, mmalkawi@aimws.com, AIM Wireless Inc., USA

Thaier Hayajneh[2], *School of Information Sciences*, and **Mohammad Almalkawi**[1], *CRHC*, *Coordinated Science Laboratory*
hayajneh@sis.pitt.edu, almalkawi@crhc.uiuc.edu

[1]University of Illinois at Urbana-Champaign
Urbana, IL 61801

[2]University of Pittsburgh, Pittsburgh, PA 15260

Abstract

We propose a novel architecture to fuse and synthesize data from multiple sensors. This architecture, based on wireless communication of data, can be applied to monitor system integrity, to help in system control, and for personnel guidance through potentially hazardous radiation areas in nuclear applications. The proposed architecture employs sensor fusion in a way that would lead to improved decision making. The sensor suites used are interconnected serially to warrant more robust sensing strategies while leveraging spatially correlated data. They are also fed in parallel into a data fusion center using wireless technologies to ensure enhanced system reliability. While the proposed architecture can readily be tailored for specific applications in the nuclear industry such as for plant monitoring and automated decision and control, it is also designed to track and guide personnel away from radiation-contaminated zones.

I. Introduction:

Combined sensory conception is as old as life itself. About every living being on earth, from as small as an ant all the way to the size of a whale, uses combined sensory data in one form or another upon which it relies to respond to its surroundings. Humans have long relied on their combined senses (fused information/data) to cope with their surroundings. Man relies heavily on data collected through his/her auditory (the ears) and visual (the eyes) sensors to help him/her arrive at a decision in response to actions from the environment. For example, he/she relies on the various haptic senses, augmented with his/her ability to measure (analyze collected information through visual and auditory contact) to protect him/herself from the harm of excessive heat or cold [1].

It was not until the early 1990's that the need arose to integrate what living beings have innately enjoyed all along into engineering tools [1 - 3]. Although initially confined to military and space applications, sensor fusion technologies and the smart schema that underpinned them gradually spread over to other applications [1]. Such new applications range from home appliances, and security/safety systems, to smart vehicles and intelligent traffic systems [4 – 6].

As smart as they can be, sensors working as single isolated units have less to offer, as compared to multiple sensors working in unison. Take for instance the human eye, as a visual sensor, which can operate from the range of sensing simple visual images to its ability to recognize objects, and situations which can be pleasing or life threatening! Nonetheless, the sight of people stampeding down the street escaping some life threatening situation may not trigger some form of action on the part of an individual until another form of sensed information, *viz.* auditory

978-1-4244-2034-6/08/$25.00 ©2008 IEEE.

signals, is made available to ascertain the need for an immediate course of action that would save the individual's life amidst the sequel of events.

The need to develop sensor fusion technologies and the underlying algorithms that extract features from multi-sensor data and elicit decisions is partly driven by the ever growing need for remote sensing and data collection using growing number of satellites, and the need to build space and terrestrial robots [1, 2, 7]. The associated wireless technologies to communicate multi-sensor data had already matured to a level where sensor fusion developments could, to varying degrees, utilize the ongoing progress in wireless communications. While sensor fusion technologies are not necessarily dependent on wireless communication, it is likely to enhance sensor fusion systems reliability and reduce cost. The schema proposed here is developed with wireless means of communicating the data in mind.

Some applications of wireless technologies have been reported at nuclear facilities [8]. Although none of these had much to do with safety-related applications, wireless systems in non-safety applications were identified in a number of areas. These include:

- communication infrastructure for mobile computing;
- installation of an electronic personal teledosimetry system;
- installation of a wireless barcode system for warehouse material management;
- installation of wireless sensors and data communication equipment for implementing condition-based maintenance (CBM);
- development of a prototype smart sensor for diagnostic and prognostic health assessment for the gearbox of a centrifugal charging pump;
- enabling of wireless access to information using WLANs for retrieval of documents, manuals, procedures and drawings by personnel in the field;
- institution of real-time wireless communication between work-order and scheduling software packages; and, finally
- tracking using RFID for parts movements from and into inventory.

In the next section, Section II, we present an overview of sensor suite configurations and typical sensor fusion architectures that are being used to develop various types of applications [2, 9]. In the following section, Section III, we draw some examples on the use of sensor fusion technologies with varying degrees of importance. In section IV, we propose a new model for sensor fusion which incorporates wireless diversity technologies aimed at monitoring and control of operation of nuclear facilities. Based on the model proposed, therein, we also propose a schema, specifically designed for radiation monitoring and to guide personnel working in radiation environments. Section V addresses alternate ways of enunciating radiation contamination levels. In Section VI we discuss related aspect to the proposed architecture together with related cyber security matters. Finally, conclusions and potential for further research are introduced in Section VII.

II. Sensor Suite Configurations and Fusion Architectures:

In the majority of cases, the sources of information for fusion are the physical sensors themselves. As such, physical sensors constitute a basis for categorization of the various fusion models and concepts [2]. Sensors have been classified as passive, active or a combination of the two. Although much of the research reported in the open literature addresses the use of passive sensors only or a combination of one active sensor together with one or more passive sensors, there has been significant work undertaken dealing with multiple active sensors addressing mainly defense applications. The presence of more than one active sensor in a sensor suite/network makes the problem somewhat intractable in terms of rigorous analytical treatment.

What dictates the use of a particular type of sensor or sensor suite is the underlying application and the complementary nature of information derived from participating sensors. In either case, the sensors used should be compatible in terms of field of view, range, data rates, and sensitivity to weather conditions, amongst others, to make information fusion from the individual sensors more meaningful for a particular application [2].

II. A. Sensor Suite Configuration:

When used in groups while observing/monitoring a given phenomenon, sensors form what is referred to as *suites*. Sensor suites have been identified in the literature under two categories: parallel and serial or tandem [7]. Parallel sensors have been the most extensively studied in a variety of applications. This is attributed to the independence of the various sensors involved lending them quite readily to the Neyman-Pearson formulation for the distributed detection problem. Furthermore parallel configurations lend themselves quite well to more reliable levels of system performance. Serial sensors (where the output from one sensor feeds right into the next with all sensors observing the same phenomenon) or those used in tandem have been found to function better in terms of the decision quality involved. They, however, are more prone to accumulated network delays and pose a reliability challenge when failures occur to one or more of the sensors. Serial sensors are, nonetheless, well suited in application scenarios where the observations of the different sensors are temporally/spatially separated, as is the case in moving target tracking. In practical real-world

applications, sensor components in tandem may consist of sensor suites with multiple parallel sensors, which might, to certain extent, mitigate the reliability constraint/s. Hence, complex combinations of parallel and serial configurations are possible.

II. B. Sensor Fusion Architectures:

The sensor fusion community has traditionally categorized the levels at which data integration takes place as a three-level hierarchy, namely data- , feature- , and decision fusion, respectively [2]. This categorization is used to refer to the input or the output (result) of the fusion process. Data fusion (with reference to the input) has been the lowest level of fusion in the hierarchy, followed by feature fusion, and finally decision fusion at the highest level of the hierarchy. At each level of data integration, information is, to varying degrees, lost to the fusion process. Raw data registered by sensors and sensor suites is commonly the place where the highest resolution of information is kept; this resolution degrades to the next hierarchical level of integration [2]. Applications vary with their sensitivity to the level of hierarchy concerned. While certain applications, namely military and aerospace, rely heavily on resolution integrity of the measurements (data) involved, many other (non-mission critical) applications perform adequately with the types of features (fused data) extracted that lead to some level of manual or automated decision-making (fused features) process [1].

The fusion process itself is carried out by means of one algorithm or another [10]. Towards that end, many technologies have been employed towards achieving one objective or another. These include hypothesis testing, estimation theory, fuzzy logic, neural networks, pattern recognition, and artificial intelligence, amongst others [1, 2, 7]. Sensor fusion is often referred to as a "fission inversion process". Here, data is looked upon as fragmented bits and pieces of information with each sensor looking upon the pieces and bits of information it can relate to over a given time span. Hence, the information about a particular phenomenon or environment under observation is sometimes looked upon as a decomposition of the overall scene into the components perceived by the individual sensors. This is referred to as sensor-caused fission, with the ensuing fusion process doing what it can to assemble (counteract the fissioning process) the whole picture together.

According to an I/O-based characterization sensor fusion architectures can be classified into [2]:

1) *Data In-Data Out (DAI-DAO) Fusion:* This is the most basic form of fusion in the hierarchy. This form of fusion, where inputs are the data that form a data output, is commonly referred to as data fusion.
2) *Data In-Feature Out (DAI-FEO) Fusion:* Under this characterization, data from different sensors fuse to derive some form of a feature of the object in the environment or a descriptor of the phenomenon under scrutiny.
3) *Feature In-Feature Out (FEI-FEO) Fusion:* At this level of the hierarchy, both the input and output of the fusion process are features.
4) *Feature In-Decision Out (FEI-DEO) Fusion:* This is one of the more widely encountered fusion paradigms. Here, the inputs are features coming in from the different sensors assembled to form a decision at the output.
5) *Decision In-Decision Out (DEI-DEO) Fusion:* Here, both inputs and outputs of the process are decisions. This is often referred to in the literature as decision fusion.
6) *Temporal (Data/Feature/Decision) Fusion:* Data integration over time, as acquired from the different sensors, can be referenced as a temporal fusion process.

The classification outlined above has been commonplace in the design of sensor fusion architectures, as dictated by application or conceived from theory. Other architectures, which leverage the classification types mentioned above, have been found to exist in the real world. The Flexible Fusion System Architecture is a versatile architecture which integrates the five fusion types, listed above, under one common umbrella [2]. Depending on the particular application niche, the flexible architecture is capable of identifying, and hence, implementing the fusion type most suited for the application environment in question. It can even configure itself to implement more than one fusion type simultaneously. Moreover, certain fusion architectures have been known to exhibit some level of self-improvement. This is accomplished via some form of feedback from a central fusion processor to the local individual sensor subsystems. The decision made as such on the part of the subsystems or the features extracted thereof achieve some level of improvement in the process.

III. Examples on the use of Sensor Fusion Technologies:

Although the application of sensor fusion technologies originated from the realm of military and aerospace applications, their uses have indeed propagated to other walks of science & engineering [1]. Sensing technologies using conventional/classical sensor techniques have addressed the needs of industry, production, and the engineering and scientific professions to varying degrees. However, they commonly fell short of providing the

accuracy, precision, and reliability sought by defense needs and that of mission-critical applications.

Sensor fusion largely started with the need to identify/detect moving/flying objects, track them and be able to judge their maneuvers accurately and adequately before a decision is made to deal with a given situation. While certain types of sensing systems can measure the target range and velocity, other types are needed to measure their angle of approach to better assess their destination/intention. Target identification and the ability to determine friend-foe-neutral situations are strategic requirements within war zones.

The DoD research/scientific community commonly focuses on issues dealing with characterization, location, and identification of such dynamic entities as types of weapons, emitters, platforms and military units. DoD users are often interested in higher level inferences about enemy maneuvers [1]. Examples of DoD scope of interest includes air-to-air defense, surveillance, target acquisition, ocean surveillance, battle field intelligence and strategic warning and defense, amongst others. These applications normally involve the use of sensor suites that encompasses radar, electro-optic image sensors, passive electronic support measures (ESM), and identification-friend-foe (IFF), amongst many others.

By the turn of the decade of the 90's, technology development had reached a peak. Information integration became more precise and meaningful. The ability of the industrial sector to produce more reliable machinery and hardware worked in support of high availability products [11 - 13]. Associated with that was higher levels of confidence and assurance in the underlying (driving) software.

There is also interest in such applications as automated control of manufacturing systems, implementation of robotics, development of smart buildings, design of bio-medical applications, and as of late, innovations in autonomous systems, and progress in telematics and intelligent transportations systems [1, 4, 6]. Indifferent to their military counterparts, these applications have their own challenges, sensor suites and deployment strategies.

IV. Proposed uses and models for use in the Nuclear Industry:

There is renewed interest in nuclear power as a, carbon-free, renewable source of energy. With plant life extension requests, there are also plans in the works to upgrade the technologies in the old fleet of nuclear reactors. This has come at a time when technology development has progressed by leaps and bounds. New technology should be fruitfully used to further improve nuclear power plants safety. Technologies used to better monitor and detect malfunctioning units or higher than expected radiation levels can improve reactor operations and performance. Similarly, improvement in help provided to operators in making decisions is also likely to reduce human errors.

A Proposed Sensor Model for Nuclear Applications:

To set the stage for areas within nuclear engineering where sensor fusion might be fruitfully utilized, it would be quite beneficial to review the accident scenario that led to the Three-Mile Island (TMI) disaster[1] in 1979, [17].

On March 28, 1979 at 4:00AM service personnel at TMI were conducting routine maintenance check on the feed water system of the plant. Inadvertently, the pump moving water from the condenser to the demineralizer was stopped. By design and due to the ensuing loss of suction pressure the main plant's feed water pumps also stopped. The plant would have automatically recovered from this benign incidence; an auxiliary feed water pump would have readily brought in water to the steam generator. Unfortunately, this did not occur since block valves downstream from the auxiliary feed water pumps had been left closed by mistake from a previous maintenance cycle. This was not noticed, due to lack of coordination, until 8 minutes into the accident, during which time a whole sequence of events took place, leading to an automatic shut down (SCRAM[2]) of the plant, which also led to an unwanted out-of-sequence depressurization of the plant. At this stage, the pressurization relief valve should have kicked in and stopped the discharge of the steam. Though the valve was energized, it did not function as expected and fell short of securing the steam leak. Even that problem could have been fixed but for the fact that the closure of the valve was relayed by the energization of the solenoid controlling the valve—rather than the actual stem position of the valve itself—leaving the plant operators under the impression that the valve had, in fact, closed. This went unnoticed until 2 ¼ hours into the accident.

Clearly, with today's technology and improved training an incident like this one can be easily averted. Specifically, a design that uses multiple sensor suites, upon which a more rugged decision making algorithm is built, can provide the operators the right information to avoid an accident. Possible uses of this technology in the field of nuclear engineering may range from improved instrumentation and control and better information feed to reactor operators to radiation level monitoring and ALARA (As Low As Reasonably Achievable) issues. Below we propose the use of a multiple sensor suite to monitor and control the flow of events in an existing nuclear facility, or in the design of new reactors.

---

[1] This overview is intended for audience with no nuclear background. Those familiar with the details of the TMI accident may skip this paragraph without loss in continuity.

[2] The acronym was derived from the phrase "**Super-Critical Reactor Axe Man"** since historically earlier reactor shutdowns were carried out manually by someone using an axe, when automated shutdowns would fail.

A single sensor can sometimes lead to the wrong conclusion about some observed phenomenon as was the case in the TMI accident. This is attributed, as discussed in section II.B, to an inherent sensor-caused fission of the information that can potentially be made available to the decision-making process. When used as aggregates, however, data collected by the different sensors can be used to complement one another, especially when the sensors used are such that each would be monitoring a phenomenon from a different aspect. If there was, for instance, a multi-sensory suite at TMI at the time of the accident, then one sensor element could be looking at the valve position, another at flow rate of the fluid in the pipes, a third one at current flowing through the pump, a forth one at temperature of the flow, some that would measure the stress and strain of the material making up the structure of the reactor core, and so on. The fact that the valve position was reported erroneously could have been corrected by complementary data from the sensor element measuring flow rate through the pump, and would have easily determined that the valve had not, in fact, closed. Under sensor fusion, data measurements not only complement one another, but can also be used to fuse into a more useful decision making process.

To help overcome critical situations and avert incidences of the type of TMI, we propose the use of a sensor suite as shown in Fig. 1. Each sensor 'unit' in the suite is designed to measure a particular aspect of the phenomenon in question, *viz., flow rate, temperature, current flow, valve position, stress and strain of material making up structure of the core, etc*.

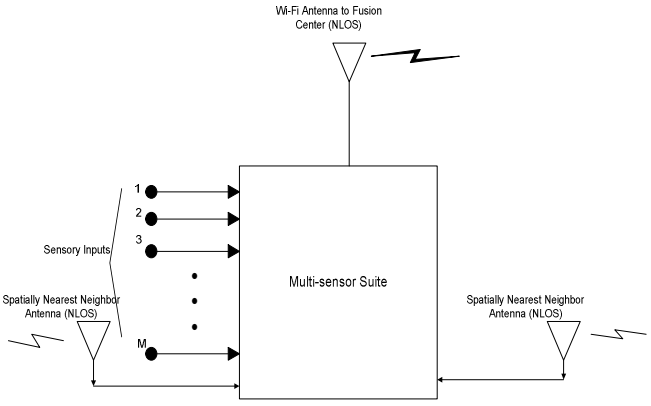

Fig. 1: Proposed multi-sensor suite

This sensor suite, while containing multiple sensors functioning in parallel, can be connected in series[3] to other suites measuring related phenomena at other (neighboring/adjacent) plant locations. This series connection can be used to improve/enhance/exchange measurements taken at other locations, since series sensor architectures are inherently more rugged at providing improved detection and/or estimation. Nonetheless, these sensors can also be coupled to a remote fusion center, where the merged readings result in data (as opposed to a feature or a decision) that preserve the resolution of the underlying measurements, in a parallel configuration. The data transfer may be accomplished using wireless technology to improve reliability of the system. This is illustrated in Fig. 2. To ensure reliability and robustness to interference and noise, we couple the various sensors to the fusion center through multiple antennas to exploit communication diversity [18, 19], which is known to provide an improved signal-to-noise ratio at the receiver. Reliability is ensured by the fact that if one sensor suite fails [20], other suites would compensate for the missing data. Also, the series connectivity of the sensors would be used to configure one sensor/suite to fill in for a failed one in the series. Furthermore, the series connectivity of sensor suites is quite useful when spatially separated measurements, which are commonly interrelated (correlated), can feed information from one sensor suite to another along the line; namely, what happens at one spatial location can be used by another sensor suite, at a different location, to predict the events or identify anomalies that follow based on events that happened elsewhere in the system.

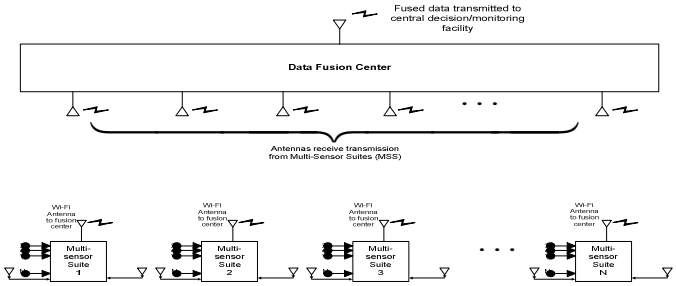

Fig. 2: Series connection of multi-sensor suites with wireless parallel connection to remote data fusion center

IV. A. A Radiation Monitoring and Personnel Guidance System for Nuclear Facilities:

Minimizing radiation doses to personnel working at nuclear power plant (NPP) sites is rather important. The International Commission on Radiological Protection (ICRP) has enunciated that the maximum permissible dose for occupational workers may not exceed 2 rems (Radiation Equivalent Man) per year averaged over five years, with a maximum of 5 rems in any one year period [21]. According to ICRP, members of the public, on the other hand, may not have more than 0.1 rem per year averaged over a 5-year period, with a maximum of 0.5 rem over a given 1-year period, which is one tenth of that permissible to occupational workers. By law, occupational

[3] The series connectivity conjectured in the proposed architecture could entail connectivity along one path, depending, of course, on the application, or that connecting sensors on a grid.

workers are periodically briefed on their exposure status and advised on best work-environment practices based on reviews of their dosimeter history. Dosimeters are commonly used on people operating under environments with radiation contamination hazards. Current day devices, while measuring radiation levels on the spot, can also store a history of exposure levels.

To provide additional radiation protection measures to workers, we herein propose a new sensory system that can monitor the workers and guide them to "minimum dose" paths when performing routine work and in cases of emergency. *Using multiple sensors, wireless technology and data fusion, the goal would be to determine the path to go from point A to point B in a radiation field that would minimize the dose*[4]. Additionally, this information needs to be supplied to personnel working in the field. The system being proposed is made up of three parts; a *fixed infrastructure*, a *man-borne mobile* unit, and *the localization and tracking subsystem*.

1) **The Fixed Infrastructure:** This is the part that constantly feeds data to the man-borne unit. This infrastructure sub-system is made up of a number of multi-sensor suite units distributed over the area of interest being monitored for radiation. Fig. 3 illustrates a possible architecture for the proposed sensor suite. This is fairly much the same sensor suite proposed in Fig. 1, save for the Line of Sight (LOS) inter-suite communication schema used (as opposed to that in Fig. 1). LOS communication is used between the sensors due to the proximity[5] of the suites to one another. This will eliminate the need for high power transmitters, which would otherwise cause interference with other plant sub-systems. Sensor suites, in this case, are data-in/feature-out devices. Each sensor suite has a number of sensors operating in parallel, with each sensor providing different information from the region the suite is expected to monitor. For example, a suite may have radiation sensors, temperature sensors, pressure sensors, etc. An RFID sensor is also mounted on few suites (usually around zonal access points and those used for target tracking) to communicate with the corresponding unit on the man-borne mobile unit. Furthermore, various multi-sensor suites are interconnected via dedicated wireless links, likely using Zigbee (IEEE 802.15.4), [22]. These interconnections are used to improve the measurements and provide self learning on the part of each sensor suite based on information being fed from those in the immediate neighborhood. This will further help each sensor suite to predict events within its locality based on data being fed from neighboring sensor suites that are spatially separated from it. This, in turn, enriches the information content at each sensor suite with spatial diversity. Each sensor suite extracts the relevant features based on the data it collects. These features are transmitted simultaneously from more than one sensor suites on to the *Man-Borne* device, where a continuous decision is made on the path of least dose. The proposed sensor suite interconnect configuration is shown in Fig. 4.

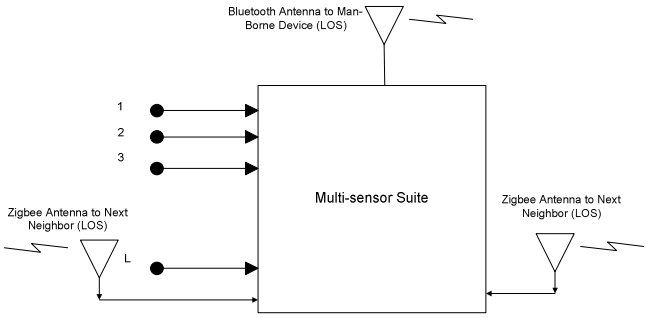

Fig. 3: Multi-sensor suite designed to measure radiation/temperature variations and to monitor and guide personnel Movement

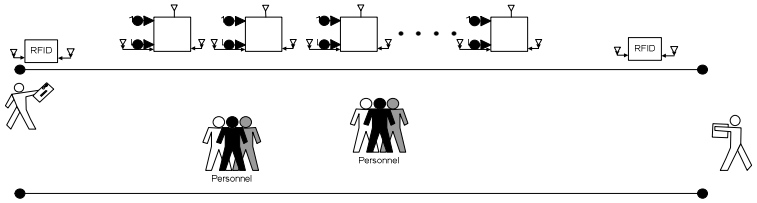

Fig. 4: Multi-Sensor suite configuration in a monitored area to monitor and guide Personnel movement

To enhance the reliability of the serial interconnection of the sensors, each sensor suite is connected to a *fusion center* via a dedicated wireless link. This link may be provided using the Wi-Fi protocol (IEEE 802.11a, b, g, and n) [22], *which are known for its relatively short range of transmission, which would, in turn, help in mitigating*

[4] Minimum dose does not necessarily refer to the shortest path treaded; rather, it refers to the lowest possible radiation-time product, which achieves ALARA.

[5] Relatively closely spaced sensor suites are only for the case of radiation monitoring applications.

interference issues. From the fusion center the information is sent to some control room for monitoring purposes. In order to increase the reliability of the transmitted data at the fusion center, multiple antennas may be used at the receiver/s of the fusion center to exploit the benefits of communication diversity (both spatial and temporal diversity). This is illustrated in Fig. 2.

The *Fixed Infrastructure* is, in turn, used to monitor and guide personnel walking through areas it spans. This is done by transmitting the *features* to the *Man-Borne Mobile* Unit, discussed below. Communication with the *man-borne* unit is done via Bluetooth (IEEE 802.15.1) technologies, [22], which are usually shorter in range than Wi-Fi with lower bit rates. This is intentionally done to help mitigate any radio interference issues with other communication systems on the facility [22].

Finally, channel selection and scheduling for the three modes of communication, viz., *Wi-Fi*, *Bluetooth* and *Zigbee*, can be made so that interference between the modes is avoided. Furthermore, some appropriate frequency (channel) allocation or reuse (scheduling) strategies can be instituted for communication links between any two sensor suites in the sensor serial connections to eliminate the possibility of assigning the same channel to adjacent sensor suites.

2) **The Man-Borne Mobile Unit:** This is the mobile unit worn by the personnel working in the monitored environment. A Man-borne unit is a decision device that bases its decision on *features* received from the various sensor suites as the individual passes by them. These features entail information about the hazard levels an individual comes across along the way, and directions that point to dose-reduced access paths. The Man-borne unit is linked to the Infrastructure Sub-System through, as mentioned earlier, *Bluetooth*. To activate the Bluetooth mechanism, an *RFID* (Radio Frequency Identification) tag, [22], is placed on each man-borne unit with a unique identifier. As the individual walks across an *RFID detector* associated with a particular sensor-suites he/she is identified by the sensor suite which then pairs, *via Bluetooth*, with the man-borne device. To avoid *communication interferences*, the RFID is used to identify which channel can be allocated for pairing with the device of the particular personnel involved. This information is also used to track the movement of the individual between the sensor suites.

   The synthesized features and possibly radiation and other relevant data transmitted from the various sensors are fused in the man-borne device into an appropriate decision that guides the individual though a "minimum radiation" passage. The proposed architecture of the man-borne device is illustrated in Fig. 5. Again, to avoid transmission interferences, Bluetooth channel allocation is made to pair each man-borne device on a channel that is associated with the RFID of the person involved, such that no single channel is allotted to two difference devices at the same time. Allocation strategies can also be made so that the same RFID tag can take on more than one channel allocation (using one channel at a time), depending, of course, on channel availability.

3) **Localization and Target Tracking:** The fixed infrastructure, in addition to its primary task of providing vital system measurements, is also used in localization of objects and in tracking of personnel. This is used as the indoor navigation system, where a GPS cannot reliably be leveraged.

   Based on their preset locations, the sensor suites can track the movement of personnel to provide location information. To date many algorithms exist [23-27], which can be used, to avail this particular functionality quite readily. However, the primary purpose of the sensor suites, as proposed in this paper, would be to provide guidance to occupational workers to avoid prolonged passage into radiation-contaminated areas.

   Our group is currently working on a navigation algorithm that would be able to both track movements of occupational workers as well as provide guidance to them away from the radiation-contaminated areas via information received by the man-borne device.

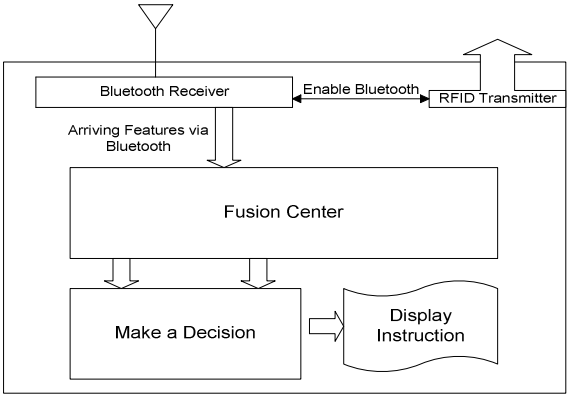

Fig. 5: Illustrative architecture of man-borne device

V. Alternate Ways of Enunciating Radiation Contamination Levels:

It is imperative for safety purposes to determine the level of radiation at various locations in a given building or environment. Without loss in generality, we may view a given environment as a grid with radiating elements placed at various locations on the grid. For personnel movement guidelines, we would mark the appropriate exit locations on the grid. At each point in time, it is required to mark the current level of radiation on the grid. Figure 6 shows a view of a hypothetical grid partitioned into equal size cells. The cell size can be chosen based on the environment to be studied and analyzed. A 1x1 foot cell provides a fine grain analysis. A more realistic size would be 3x3 foot cell. The level of radiation at each cell would depend on its relative location to the various radiating elements, and the power of radiation leak emitted by a given element. Based on the level of radiation the cells can be colored with different colors. This would be based on one graph coloring approach/algorithm or another. The objective is to mark the cells of the grid with marks indicating the level and power of radiation at particular cell locations. Two approaches can be used for this purpose; a centralized and a distributed approach.

In the centralized approach, we collect the power and location of each radiating element at a central server. The central server uses a wave propagation model to compute the power of each radiation as it travels across the grid. The power level at each cell will be the superimposition of the sum of all power signals at that location. A safe path on the grid will be one that moves along cell directions with relatively low radiation levels (acceptable radiation levels are provided by an entrusted regulatory body). Pre-determined pathways will be overlaid on the marked grid and enunciated to indicate to the workers involved the shortest and least hazardous path to a destination (or exit point) from a given current location. These paths can be pushed to hand held devices registered with the server (please refer to Section IV.A.2), or they can be displayed on screens dispersed along the pathways of the analyzed environment. A similar approach has been developed by AIM Wireless solutions[6] and used to compute the maximum permissible emission in a radio frequency environment.

In the distributed approach, each hand held device (HHD) will act as a local server which computes the "optimal" path for the current location of the device. For this purpose, the HHD needs to be equipped with an omni directional antenna and a wireless receiver. The omni directional antenna will collect levels of radiation received from several sensor nodes on the grid. The HHD is programmed to analyze several radiation measurements simultaneously. Each measurement is characterized by a certain level and a directional angle. As such, the HHD computes the direction of the pathway with the lowest radiation level. While moving, the HHD device should

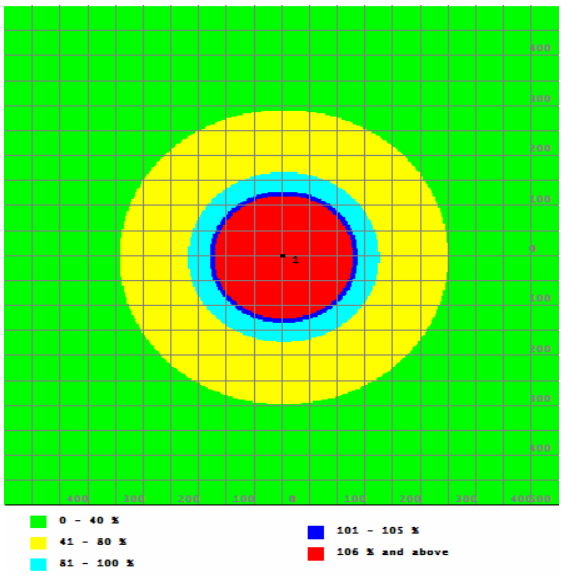

Figure 6: Maximum Exposure Grid

continuously be probing the nearest sensors, which, in turn, can reach further away sensors on the grid through the appropriate routing algorithm. Hence, the direction of movement could be computed dynamically as the person holding the device traverses a given path. This way, we can compute in real time the path with the least exposure to radiation.

VI. Discussion and Cyber Security Issues:

The combined sensor fusion schema proposed in this paper is designed to make available new means of safety to facilities as well as the occupational workers involved. The

[6] AIM Wireless, Inc., USA, www.aimws.com

associated wireless technologies are likely to play a significant role in minimizing the excessive cabling, and hence cost, that would otherwise provide connectivity between system components. They also serve to enhance the level of reliability of the underlying system against loss of communication in case of hazards such as fire. Reliability is also expected to be enhanced through the use of redundant communication links which introduce the much needed communication diversity into the system. Whether the proposed schema gets adopted in the nuclear industry is likely to depend upon certification from regulatory bodies such as the Nuclear Regulatory Commission in the USA. This is, in part, due to security/privacy issues involved in these mission-critical areas.

Cyber security is rather important in wireless communications. In fact, security is the main concern that precludes many applications from extensively using wireless technologies. Depending on the nature of the wireless medium of interest, attackers can easily inject malicious messages or alter the contents of legitimate ones. Consequently, there is a need for a security mechanism to verify the origin and contents of messages and, where necessary, ensure confidentiality of the data. Many attacks are easier to launch in wireless media as opposed to wired networks, mainly because Wireless Sensor Networks (WSNs) are connected using wireless links and lack the physical security that wired networks are capable of sustaining [28]. The broadcast nature of wireless communications makes data transmission difficult to protect. It is possible for adversaries to inject, eavesdrop on, intercept, and alter transmitted data in a broadcast medium. Moreover, attackers can use more powerful nodes than the ones used in traditional systems. Additionally, they can communicate with the WSN from a remote location using strong radio transceivers and workstations. Attackers could continuously flood the network to inflict Denial-of-Service (DoS) upon intended targets [29]. Wireless sensors are sometimes deployed in physically insecure environments so that attackers can capture the nodes, reveal their critical data (e.g., cryptographic keys) and create fake nodes as authorized nodes in the network. However, our system can be considered to be deployed in a secure area and protecting the sensors physically is beyond the scope of this paper.

Due to a variety of threats and possible attacks [29], Ng *et al.* [30] argued that in WSNs there is need to address many security issues as: key establishment and trust setup, confidentiality and privacy, integrity and authentication, reliability and availability, resilience to node compromise, secure routing, secure group management, and data aggregation.

For the application presented in this paper we propose a security model based on Public key cryptography which is, also, known as asymmetric cryptography. In this case each node will have two keys; one is kept secret and only known to the key owner, called the private key K_R; the other is made known to every node in the network and called the public key K_U. Public key cryptosystem must satisfy certain conditions [31]: ciphering or deciphering a message given the appropriate key have to be computationally easy to implement. In addition, deriving the private key given the public key must be computationally infeasible.

Wireless sensors are known for their limitations in energy, computation, and communication capabilities. Thus, public key cryptography was considered expensive in computation and energy, which rendered it impractical for wireless sensor applications. However, recent research endeavors at SUN Microsystems laboratories [32] used simplified and optimized algorithms for elliptic curve cryptography [33] and other public key cryptography showing that they offer a practical solution in wireless sensor networks.

In our model, each sensor will have a public/private key pair. The private key of each sensor will only be known to itself; only the data fusion center needs to know the public keys for all the sensors involved. The sensors, on their part, will only need to know the public key for the data fusion center. Furthermore, and to ensure next neighbor inter-suite communication, each sensor will have access to the public key of the neighboring sensors and RFID devices located some *r* distance from it, including, of course, that of the Man-Borne unit. For increased security of the sensor network, we suggest that all the keys be securely installed at the sensors prior to their deployment on location. This will prevent serious attacks, such as: man-in-the-middle attack.

We also assume that the sensors have loosely synchronized clocks. Yoon *et. al.* [34] presented Tiny-Sync which is a time synchronization method relevant to wireless sensor networks. The proposed scheme uses minimal bandwidth, storage, and processing resources but achieves fairly good accuracy. Sun *et. al.* [35] presented TinySeRSync, which is a secure and resilient time synchronization subsystem for wireless sensor networks running TinyOS. They claimed that this protocol is resilient against external attacks and compromised nodes.

Before transmitting a packet the sensor needs to attach a time stamp to that packet. This will reflect the freshness of the packet and prevent replay attacks. The sensor, then, will sign a message with its private key using the Elliptic Curve Digital Signature Algorithm (ECDSA) [36]. This will authenticate the identity of the sender to the data fusion center and ensure the content of the message is intact; i.e., providing authentication for the origin and the content of the message. Where data confidentiality is needed, the sensor involved can encrypt the packet using the public key of the data fusion center. Upon receiving each packet, the data fusion center will first decrypt the

packet using its private key and will then verify the authenticity of the origin and the content of the packet using the public key of the sending sensor.

When the data fusion center wants to send a packet to all the sensors then it will encrypt that packet with its private key, thus all the sensors can use the public key of the data fusion center to decrypt the message. This will provide both authenticity and confidentiality to the packet.

When the data fusion center wants to send a packet to a particular sensor then it will sign the packet with its private key and then encrypt that packet with the public key of the receiving sensor. Thus, the sensor can use his private key to decrypt the message and then use the public key of the data fusion center to verify the signature. This will provide both authenticity and confidentiality to the packet.

VII. Conclusions and potential for future research:

The architecture proposed in this paper is, by design, made to service mainly the nuclear sector and other related industries. It is expected that with the use of the schema proposed in this paper, occupational workers, who are either in the nuclear industry or other affiliated/supporting industries will have more peace-of-mind when guided electronically by smart devices and systems.

An additional benefit of the schema proposed here is the use of wireless technology in the nuclear industry. So far, little has been reported on the use of wireless technologies, even those which involve non-safety related applications, within the realm of the nuclear industry; much less so for the use of sensor fusion. The proposed architecture will hopefully trigger additional ideas in the areas of sensor fusion and wireless communications; ideas that can potentially help push forward the level of technology used in the nuclear industry, and, hence, contribute to further improvement in the level of safety in the rapidly returning nuclear sector.

References

[1] David L. Hall and James Llinas, "An Introduction to Multisensor Data Fusion," *Proceedings of the IEEE*, vol. 85, No. 1, January 1997.

[2] Belur V. Dasarathy, "Sensor Fusion Potential Exploitation – Innovative Architectures and Illustrative Applications," *Proceedings of the IEEE*, vol. 85, No. 1, January 1997.

[3] J. Llinas and E. Waltz, *Multisensor Data Fusion*. Boston, MA: Artech House, 1990.

[4] Umit Ozguner, Christoph Stiller and Keith Redmill, "Systems for Safety and Autonomous Behavior in Cars: The DARPA Grand Challenge Experience, " *Proceedings of the IEEE*, vol. 95, No. 2, February 2007.

[5] J. C. McCall and Mohan M. Trivedi, "Driver Behavior and Situation Aware Brake Assistance for Intelligent Vehicles," *Proceedings of the IEEE*, vol. 95, No. 2, February 2007.

[6] M. Khasawneh, M. Malkawi, *et. al.*, "A Security Embedded Infrastructure for Tele-Traffic Speed Control, " *Proceedings of 4th Int'l Symposium on Mechatronics and Its Applications*, Sharjah, United Arab Emirates, March 2006.

[7] Ramanarayan Viswanathan and Pramod K. Varshney, "Distributed Detection with Multiple Sensors: Part I – Fundamentals," *Proceedings of the IEEE*, vol. 85, No. 1, January 1997.

[8] NUREG/CR-6882, Assessment of Wireless Technologies and their Applications at Nuclear Facilities, Oak Ridge National Laboratory, July 2005.

[9] L. A. Klein, *Sensor and Data Fusion Concepts and Applications*, SPIE Opt. Engineering Press, Tutorial Texts, vol. 14, 1993.

[10] D. Hall, *Mathematical Techniques in Multisensor Data Fusion*. Boston, MA: Artech House, 1992.

[11] D. Lee, J. Abraham, D. Rennels, and G. Gilley, A Numerical Technique for the Evaluation of Large, Closed Fault-Tolerant Systems, In *Dependable Computing for Critical Applications,* pages 95-114, Springer-Verlag, Wien, 1992.

[12] W. H. Sanders and J. F. Meyer, A Unified Approach for Specifying Measures of Performance, Dependability and Performability, In A. Avizienis, J. Kopitz, and J. Laprie, editors, *Dependable Computing for Critical Applications,* volume 4 of *Dependable Computing and Fault-Tolerant Systems,* pages 215 – 237, Heidelberg, Springer-Verlag, 1991.

[13] A. Williamson, Discrete Event Simulation in the Mobius Modeling Framework, Master's Thesis, University of Illinois at Urbana-Champaign, 1998.

[14] N. S. Embrey, "The Impact of TMI: Our Energy Future - Will Nuclear Play a Part?", The Bacock and Wilcox Company, NPGD-2M-10-79, 1979.

[15] Lord Marshal of Goring, "Comments on the Chernobyl Accident", *Nuclear Technology International*, Neville Geary, ed., Sterling Publications, Limited, London, 1987.

[16] J. G. Collier and G. F. Hewitt, "Introduction to Nuclear Power," Hemisphere Publishing Corporation, Springer-Verlag, 1987.

[17] M. Ragheb, https://netfiles.uiuc.edu/mragheb/www/NPRE%20402%20ME%20405%20Nuclear%20Power%20Engineering/Three%20Mile%20Island%20Accident.pdf, University of Illinois at Urbana-Champaign, December 2007.

[18] R. G. Gallager, *Principles of Digital Communication*, Cambridge University Press, 2008.

[19] David Tse and Pramod Viswanath, *Fundamentals of Wireless Communications*, Cambridge University Press, 2005.

[20] Mohammad Modaress, Mark Kaminskiy, and Vasiliy Krivtsov, *Reliability Engineering and Risk Analysis; A Practical Guide*, Macel Dekker, Inc., New York 1999.

[21] M. Ragheb, https://netfiles.uiuc.edu/mragheb/www/NPRE%20402%20ME%20405%20Nuclear%20Power%20Engineering/Ionizing%20Radiation%20Units%20and%20Standards.pdf, University of Illinois at Urbana-Champaign, September 2007.

[22] NUREG/CR-6939, Coexistence Assessment of Industrial Wireless Protocols in the Nuclear Facility Environment, Oak Ridge National Laboratory, May 2007.

[23] J. R. Guerrieri, *et. al.,* "RFID-Assisted Indoor Localization and Communication for First Responders," European Space Agency, (Special Publication), vol. 626, Oct. 2006.

[24]S. Thrun, D. Fox, and W. Burgard, "A Probabilistic Approach to Concurrent Mapping and Localization for Mobile Robots," *Autonomous Robots*, vol. 5, pp. 253-271, 1998.

[25] Z. Deng and W. Zhang, "Localization and Dynamic Tracking Using Wireless- Networked Sensors and Multi-Agent Technology: first steps," in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, pp. 2386-2395, 2002.

[26] L. Parker, B. Birch, and C. Reardon, "Indoor Target Intercept Using an Acoustic Sensor Network and Dual Wavefront Path Planning," Proc. Int'l Conf. on Intelligent Robots and Systems, Las Vegas, Nevada, Oct. 2003.

[27] Y. Zou and K. Chakrabaty, "Target Localization Based on Energy Considerations in Distributed Sensor Networks," Ad Hoc Networks, vol. 1, issue 2-3, pp. 261-272, Sep. 2003.

[28] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks," to appear, Proceedings of the Second ACM Conference on Embedded Networked Sensor Systems (SenSys 2004), Baltimore, MD, November 2004.

[29]Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, 2006.

[30] H. S. Ng, M. L. Sim, and C. M. Tan, "Security Issues of Wireless Sensor Networks in Healthcare Applications," British Telecom Technology Journal (BTTJ) 24 (2): 138-144, APR 2006.

[31] Introduction to Computer Security, by Matt **Bishop** (ISBN: 0-201-44099-7), Addison-Wesley 2005.

[32] N. Gura, A. Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing Elliptic Curve Cryptography and RSA on 8-bit CPUs," Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES 2004), Boston, August 2004.

[33] N. Koblitz, *Elliptic curve cryptosystems*, in *Mathematics of Computation* 48, 1987, pp. 203–209.

[34] Yoon, S., Veerarittiphan, C., and Sichitiu, M. L. 2007. Tiny-Sync: Tight time synchronization for wireless sensor networks. ACM Trans. Sens. Netw. 3, 2, Article 8 (June 2007), 34 pages.

[35] K. Sun, P. Ning, and C. Wang. Tinysersync: secure and resilient time synchronization in wireless sensor networks. In *CCS*, pages 264–277, 2006.

[36] D. Johnson, A. J. Menezes and S. A. Vanstone, The elliptic curve digital signature algorithm (ECDSA), Intern. J. of Information Security, Vol. 1 (2001) pp. 36-63.