SPECIAL SECTION ON SECURITY ANALYTICS AND INTELLIGENCE
FOR CYBER PHYSICAL SYSTEMS

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received December 27, 2017, accepted January 22, 2018, date of publication March 6, 2018, date of current version April 18, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2812741

A Critical Analysis of Mobility Management Related Issues of Wireless Sensor Networks in Cyber Physical Systems

JALAL AL-MUHTADI[1,2], MA QIANG[1], KHAN ZEB[1,3], JUNAID CHAUDHRY[4,5],
KASHIF SALEEM[1,6], ABDELOUAHID DERHAB[1],
MEHMET A. ORGUN[6,7], (Senior Member, IEEE), RAJAN SHANKARAN[6],
MUHAMMAD IMRAN[2], AND MARUF PASHA[8]
[1]Center of Excellence in Information Assurance, King Saud University, Riyadh 12372, Saudi Arabia
[2]College of Computer and Information Sciences, Kind Saud University, Riyadh 12372, Saudi Arabia
[3]Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada
[4]College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ 86301-3720, USA
[5]Security Research Institute, Edith Cowan University, Joondalup, WA 6027, Australia
[6]Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
[7]Faculty of Information Technology, Macau University of Science and Technology, Taipa 999078, Macau
[8]Department of Information Technology, Bahauddin Zakariya University, Multan 60000, Pakistan

Corresponding authors: Ma Qiang (maqiang06@lzu.edu.cn) and Kashif Saleem (ksaleem@ksu.edu.sa)

The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no (RG-1439-022).

ABSTRACT Mobility management has been a long-standing issue in mobile wireless sensor networks and especially in the context of cyber physical systems; its implications are immense. This paper presents a critical analysis of the current approaches to mobility management by evaluating them against a set of criteria which are essentially inherent characteristics of such systems on which these approaches are expected to provide acceptable performance. We summarize these characteristics by using a quadruple set of metrics. Additionally, using this set we classify the various approaches to mobility management that are discussed in this paper. Finally, the paper concludes by reviewing the main findings and providing suggestions that will be helpful to guide future research efforts in the area.

INDEX TERMS Cyberspace, mobile ad hoc networks, mobile communication, wireless sensor networks, artificial intelligence, intelligent sensors, intelligent systems, routing protocols.

I. INTRODUCTION

A cyber physical system (CPS) is an intelligent system that includes both computational and physical components that are integrated seamlessly and interact very closely to perform monitoring and surveillance of a required area [1]–[3]. Applications that can benefit from CPS include air traffic control, smart medical technologies, electric grids, smart transportation, and many others [4], [5]. The major infrastructure of CPS that helps the system in fetching and providing the real-world data is wireless sensor networks (WSN) [3]. However, WSNs are currently deemed to be unreliable, stationary in nature and often perceived to be an extension to an existing network or the Internet to collect data in a cost effective fashion [6]. Wireless sensor nodes, because of their resource limitations, do not hold a pivotal role in common networks [7], [8]. Hence, if a WSN node moves or is moved physically by an external actor, it is considered ‘‘lost’’ by the existing network and ‘‘found’’ by the new network [9]. In WSNs, a considerable attention has been given to mobility management which encompasses six characteristics: deployment, localization, detection, routing, mobility optimization and cooperation of mobile nodes as shown in Table 1 [10]. There are many scenarios that illustrate how sensor nodes can be deployed: some aim to solve coverage related issues while others aim to solve network connectivity problems with a view to prolonging the overall lifetime of the network.

A large bulk of reported studies focus on solitary mobile nodes wherein their resources are considered as solitary assets [11]–[13]. These resources include processing capabilities, routing information stored on the nodes, and power resources/remaining battery power. We believe that the movement patterns of mobile nodes can be utilized to provide novel network services/functions in the near future. However, there are critical issues pertaining to mobility

TABLE 1. Characteristics of mobility management [10].

CHARACTERISTICS	Relevant Issues Depiction
Deployment	Connectivity, Coverage (uniform/non-uniform/location) and Deployment (static/random/dynamic).
Localization	Ranged-based (received signal strength (RSS)/time of arrival (TOA)/angle of arrival (AOA)) and Range-free techniques.
Detection	Discover and identify mobile nodes when they enter the range of static nodes. General detection protocols (strictly scheduled/loosely scheduled/on-demand) and Knowledge Based Detection Protocols.
Routing	Network Structure based (flat/hierarchical), State of Information based (topology/location), Mobility based (mobile sensors/sink/relays).
Mobility Optimization	Controllable (trajectory/speed) and Uncontrollable (deterministic and random).
Cooperation	Mobile nodes cooperate with static nodes could offer important benefits in all aspects of MWSNs.

management that requires urgent attention in Mobile Wireless Sensor Networks (MWSNs). For example, once a mobile node leaves a cluster, there are two major concerns: (1) privacy issues: the departing node might take sensitive information about or from the cluster along with it; and (2) resource issues: the departing node carries the physical resources such as computational power and battery supply with it, which in turn deprives the cluster from using and benefiting from such resources.

Obviously, MWSNs offer a more flexible, robust, and reliable solution by adequately addressing issues related to self-organization of networks and network coverage and lifetime. Nevertheless, such solutions increase the complexity of the mobility management algorithms with respect to cost. Moreover, most of the existing studies on mobility management in MWSNs support failure detection in 2D [9]. However, mobility in MWSNs follow a 3-D structure. Therefore, any failure detection method that is proposed must be able to operate in a 3-D setting [14] as depicted in Figure 1. Normally, it is difficult to predict the movement of a node in real time, but it is possible if the new location to which the node is likely to move is preassigned.

It is possible to predict whether a WSN node is mobile or not at any given time. The probabilistic quotient of the mobility of the node may be calculated and this is contingent upon whether a node decides to join or leave a cluster at time t. In a sinkhole, an intruder attracts surrounding nodes with unfaithful routing information thereby disrupting the network operation. In the face of a sinkhole attack, the mobility patterns of a victim node are hard to predict [15]. It is worth noting that the mobility pattern of a node can be predicted and planned after the movement of the node is detected [16]. In the next section, we highlight the major applications of mobility management and how the current implementations have failed to address the key issues. According to a recent study [10], all of the solutions in sensor deployment consider a 2-D sensing field whereas in the real world the mobile sensing field is often based on a 3D-structure.

In this paper, we propose a quadruple set of metrics that are derived from 3 key characteristics of a mobility management system. This set also enables us to classify the existing management solutions and helps to identify and analyze trends and challenges pertaining to mobility management that are prevalent in such systems. The trends and challenges are identified and analyzed in order to provide further guidance for future research in the field.

The rest of this paper is organized as follows. Section 2 presents the background of the review. In Section 3, we present a comprehensive review of the recent relevant studies together with their classification. The identified issues, challenges and trends are described and highlighted in Section 4. Finally, Section 5 concludes the paper with a summary of our findings and outlines future research directions.

II. LITERATURE REVIEW

This section summarizes the most relevant articles on mobility management and highlights their salient features, advantages and disadvantages.

In order to address the issue of packet delay and packet losses during congestion in emergency scenarios in low power and lossy networks (LLNs), Tang *et al.* [17] proposed a multipath congestion avoidance routing protocol, i.e., CA-RPL, based on a routing protocol for LLNs (RPL) [18]. In comparison to standard RPL, CA-RPL reduced the end-to-end delay and the packet loss rate and improved the overall throughput. However, just as RPL, CA-RPL also performs poorly in the presence of mobile nodes in the network.

Saleem and Fisal [19] proposed an energy efficient, self-optimized and secure hybrid routing protocol called biologically inspired secure autonomous routing protocol (BIOSARP) for WSNs. BIOSARP incorporates an ant colony optimization (ACO) algorithm and an artificial immune system (AIS) and it facilitates an efficient load distribution mechanism for sensor networks. The AIS component in BIOSARP provides a security element that safeguards the system from non-self/malicious sensor nodes in WSNs. Moreover, in BIOSARP, before packets are forwarded, the behavior of the neighboring nodes is evaluated based on the neighboring node's information in the neighboring table, for any abnormality using a statistical correlation approach. Once an abnormality is detected, a node is classified as self or non-self. The performance of BIOSARP is compared with that of the secure real-time load

FIGURE 1. Mobility Management in Multi-dimensional WSNs.

distribution (SRTLD) [20] protocol; it is shown that BIOSARP performs better in terms of energy efficiency, packet delivery ratio, packet overhead, and network lifetime.

Singh *et al.* [21] proposed a fuzzy ant colony optimization routing (FACOR) algorithm for optimal path selection between the source node and the destination node, i.e., the base station in WSNs. Fuzzy logic is employed in FACOR along with an ant behavior inspired algorithm for finding an optimal decision to improve the lifetime of WSNs. A comparative analysis of FACOR and ad hoc on demand distance vector (AODV) shows improved results for FACOR in terms of the end-to-end packet delay, energy consumption and the number of packets sent at the time of route discovery. Although, FACOR improves the results for static WSNs, it simply lacks mobility support.

In [22], an Advanced Hybrid Intrusion Detection System (AHIDS) is proposed to detect attacks in WSNs. AHIDS is based on a cluster architecture to enhance the low-energy adaptive clustering hierarchy (LEACH) protocol that aims to reduce energy consumption of sensors. Also, AHIDS uses anomaly and misuse detection based on fuzzy rule sets along with Multilayer Perception Neural Networks. Through the integration of different algorithms, different types of attacks such as flooding, wormhole, and Sybil attacks can be identified. The simulation results showed that the proposed system is highly efficient when evaluated against the following set of parameters; packet loss, throughput, and energy consumption when compared to other such contemporary solutions. The proposed solution is in line with the recent research trend in which the complex hybrid methods exhibit outstanding performance in comparison to contemporary solutions.

The WSNs are increasingly used in smart cities which need stringent quality of service (QoS) requirements. When misbehaving devices exist, the performance of the current delivery protocols degrades significantly but the majority of the existing schemes ignore the variability in faulty behaviors and time-variance in city services (e.g., health care units, traffic monitors). To this end, Zhang *et al.* [23] considered the problem of fault-aware multiservice delivery, in which the network performs secure routing and rate control in terms of a fault activity dynamic metric. A fault activity geographic opportunistic routing (FAGOR) algorithm is proposed and the simulations showed significant performance improvements when compared to other such algorithms.

The work in [24] focused on the stability time of WSNs and energy efficiency while using an evolutionary algorithm (EA) in evolutionary-based clustered routing protocol (ERP). The ERP incorporates the newly formulated clustering fitness function (the transmission distance function) of EA that integrates cohesion (intra-distance) and separation (inter-distance) and error aspects of clustering. The performance of the ERP is evaluated through simulations against well-known protocols such as LEACH, hierarchical cluster-based routing (HRC) and stable election protocol (SEP). The work in [24] shows that the stable election protocol (SEP) has longer network lifetime, longer stability period, and more efficient energy consumption model when compared to those of LEACH and HRC. However, SEP achieves longer network lifetime and performs better with respect to energy consumption at the expense of less stability.

Karaboga *et al.* [25] used an artificial bee colony (ABC) algorithm for the optimal selection of cluster-heads in a cluster based routing protocol for WSNs. Such a scheme not only increases the network lifetime but also maximizes data transfer speed. The clustering method in [25] is inspired from the well-known LEACH protocol but with one major architectural change involving the use of a centralized clustering method for the selection of cluster heads, which is implemented in the base station. Furthermore, the positions of the nodes are obtained by determining the distances between the nodes using the received signal's strength instead of using the GPS. In this protocol, the communication between cluster-heads and nodes uses TDMA MAC. Conversely, for communication with the base station, CDMA MAC is used. The performance analysis results show that the ABC based protocol improves the network lifetime and minimizes the transfer delays compared to those of LEACH and particle swarm optimization (PSO) based protocols.

Since mobility is critical for the effective deployment and operation of WSNs, mobility related issues in the overall operation of MWSNs are worth investigating. Many advantages of mobility in WSNs can be outlined as follows: coverage and connectivity, reliability, lifetime, target tracking and channel capacity, where the reliability analysis may be performed as in [26]. MWSNs have gathered much attention in the research community and several recent studies have been conducted in this discipline. For example, a survey in [10] and other related studies show that the development of mobility aware, energy efficient, reliable, secure and optimized routing protocols are essential for MWSNs. In the literature, numerous models and protocols have been developed for routing in MWSNs, wherein the main challenges identified are scheduling, reliability, mobility, localization and dynamic network topology.

III. CLASSIFICATION METHOD OF MOBILITY MANAGEMENT ISSUES IN MWSNs

Seyyed and Becker [10] conducted an extensive survey on the proposed data collection techniques in MWSNs as well as on issues related to the operation aspect of MWSNs due to mobility which influences the data collection process directly or indirectly. In particular, they discussed the mobility related issues in six areas as follows: deployment, localization, mobile node detection, routing, mobility optimization, and cooperation among mobile and static nodes. These six areas are taken to be the six aspects of mobility management issues in MWSNs as shown in Table 1. Such a taxonomy could be considered as a general classification of mobility management issues in MWSNs.

The work in [27], has classified mobility management algorithms into different categories. During the deployment of sensors the issue of obstacles in the sensing field also need to be considered, since these obstacles tend to degrade the signal quality and thus the overall network performance. Similarly, in order to increase the lifetime of the network, an investigation of fault tolerance is also needed in this phase. Furthermore, localization is another important aspect of MWSNs. Effective techniques for a secure, accurate, reliable and efficient localization of the network are needed. Moreover, a cooperative localization algorithm is necessary to take advantage of cooperation between static and mobile sensors. Most of the mobile detection techniques that are currently in use are designed to cater to static WSNs and not specifically for MWSNs. In addition, the detection schemes are based on radios, whereas non radio based schemes are yet to be explored. Furthermore, most of the schemes for mobility optimization are based on linear path assumptions and they usually do not consider physical obstacles in real-world scenarios. For such mobile nodes, there is also a pressing need to deploy and use novel navigation schemes which depend on the cooperation between mobile nodes and the sensor network rather than on the GPS data.

Routing is the most important aspect of MWSNs. Generally, routing protocols for MWSNs are inspired from those that are used in static WSNs and mobile ad hoc networks (MANETs). However, routing protocols based on WSNs cannot handle mobility while MANET based protocols are not designed for one-way communication, which is usually the case in sensor networks. Moreover, most of the solutions use GPS for the estimation of a node's location, which in most of the cases might not be available to real-world applications [10].

In order to improve efficiency in an event-triggered WSNs, the work in [28] proposes and evaluates current mobility management strategies. They considered mobility to maximize the coverage and load balancing. By conducting experiments that make use of different network configurations, a joint evaluation scheme to compare the performances of different approaches is presented. The conclusion is that when nodes are deployed in a mesh structure, load balancing techniques will achieve the expected performance related goals such as increased battery lifetime with a considerable increase in the number of sensed events. But these strategies become ineffective and lose efficiency in random deployment scenarios. Moreover, this research suggests that the advanced load balancing techniques must include artificial intelligence (AI) based mechanisms for them to be resilient.

We know that not many routing protocols have been proposed to support the mobility in MWSNs. In [29], Achour *et al.* summarized a few types of protocols as extensions of MIPv6 based on 6LoWPAN, which are Fast Handovers protocol for MIPv6 (FMIPv6), Hierarchical Mobile IPv6 (HMIPv6), Proxy Mobile IPv6 (PMIPv6), and Network mobility (NEMO). Although these protocols are easy to deploy, they still have some gaps. Sabor *et al.* [30] show that the hierarchical-based protocols outperform their counterparts in saving energy, scalability, and extending lifetime of MWSNs. Therefore, they focused on reviewing hierarchy-based routing protocols and divided them into two broad groups, namely, classical-based and optimized-based. They provided a detailed classification based on a list of metrics and discussed comparative advantages and limitations of each protocol in terms of various attributes such as energy-efficiency.

Unlike most existing studies such as [10] that summarize WSNs into six characteristics as depicted in Table 1, we introduce and build a clear map of classification based on a quadruple specified in Equation 1, wherein we select three characteristics of MWSNs derived from Table 1 and upgrade it by adding a new feature "Ai" as presented in Figure 2.

The Quadruple C is defined as follows and as shown in Table 2.

Let Class C be a Quadruple:

$$C = (Lc, Dt, Co, Ai). \tag{1}$$

As the value of each element in quadruple C can be either 0 or 1, each combination of values will represent a

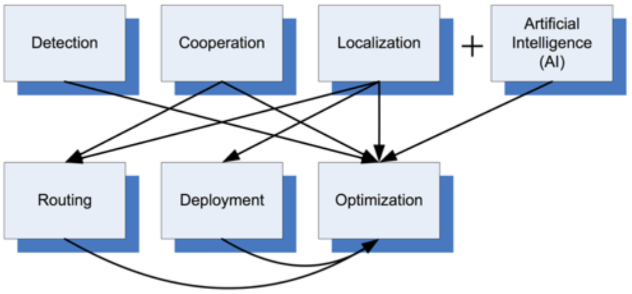


FIGURE 2. Derived Quadruple.

TABLE 2. Notation table in Quadruple *C*.

Notation (value= 0 or 1)	CHARACTERISTICS	Description
Lc	Localization	Using distance, Received Signal Strength (RSS), angle or GPS
Dt	Detection	Discover and identify mobile nodes and network structure
Co	Cooperation	Cooperation between mobile and static nodes
Ai	Artificial Intelligence (AI)	Intelligent Algorithms

TABLE 3. Full classes of Quadruple *C*.

CLASS	Quadruple (*Lc, Dt, Co, Ai*)
C1	(0,0,0,1)
C2	(0,0,1,0)
C3	(0,0,1,1)
C4	(0,1,0,0)
C5	(0,1,0,1)
C6	(0,1,1,0)
C7	(0,1,1,1)
C8	(1,0,0,0)
C9	(1,0,0,1)
C10	(1,0,1,0)
C11	(1,0,1,1)
C12	(1,1,0,0)
C13	(1,1,0,1)
C14	(1,1,1,0)
C15	(1,1,1,1)

single class. So, there will be $2^4 - 1 = 15$ classes in total as shown in Table 3 below. We map the studies in the literature into the classes of Quadruple C.

The work in [31], conducts a comprehensive search on websites and scientific databases such as Google Scholar, IEEE Xplore, Scopus, Science Direct and Web of Science to find the relevant papers written in English. The keywords that we use to search for the relevant research papers are, "wireless sensor networks", "mobile", "mobility management", "localization", "detection", "cooperation", "artificial intelligence", "movement", "mobile sensor", "node repositioning". The time span for the search was defined from 2010 till 2017.

TABLE 4. Literature distribution based on classification of Quadruple C.

Class	QUADRUPLE	Class Title
C3	(0,0,1,1)	AI based Cooperation Solutions
C4	(0,1,0,0)	Enhanced Detection Solutions
C5	(0,1,0,1)	AI based Detection Solutions
C6	(0,1,1,0)	Cooperation based Detection Solutions
C8	(1,0,0,0)	Improved Localization Solutions
C10	(1,0,1,0)	Cooperation based Localization Solutions

For example, in Scopus a particular query used was "TITLE-ABS-KEY (wireless AND sensor AND network+mobile) AND (LIMIT-TO (PUBYEAR, 2018) OR LIMIT-TO (PUBYEAR, 2017) OR LIMIT-TO (PUBYEAR, 2016) OR LIMIT-TO (PUBYEAR, 2015) OR LIMIT-TO (PUBYEAR, 2014) OR LIMIT-TO (PUBYEAR, 2013) OR LIMIT-TO (PUBYEAR, 2012) OR LIMIT-TO (PUBYEAR, 2011) OR LIMIT-TO (PUBYEAR, 2010))"

After executing comprehensive exhaustive search with all the possible queries, around 3,305 records were found, and upon further filtering out some more irrelevant papers, the final result was a total of 478 papers. After reading the titles, abstracts and conclusions of these 478 papers, we followed it by examining the introduction, results and analysis sections of those papers that had a strong relevance to this study. These papers were selected and were classified as core papers. Rest were discarded. Some key parameters that were used to select these papers are state of the art, citations, most recently published, proof of concept, and strong analysis backed up by experimental results as strong evidences. As a result, 19 research papers in MWSNs field were considered for classification. After carefully reviewing these papers and studies, we placed them into six classes selected from those in Table 3, and calculated their distribution as given in Table 4, wherein we set a title for each corresponding class. Every class is based on papers according to the relevance, as *C3* is based on 1, *C4* on 1, *C5* on 5, *C6* on 6, *C8* on 5, and *C10* on 1 as summarized in Table 6.

A. CLASSIFICATION OF MOBILITY MANAGEMENT ISSUES IN MWSNs

This subsection introduces the six classes selected in our classification and discusses the papers in each class in more detail.

1) AI BASED COOPERATION SOLUTIONS (C3)

Hu *et al.* [32] proposed a protocol called immune orthogonal learning particle swarm optimization algorithm (IOLPSOA) for the recovery of routing process from path failures between the source and the sink due to the movement of sensors and the sink nodes in the network. As opposed to other popular protocols such as the AODV, the proposed protocol in [32] facilitates a local path recovery mechanism within a small region thereby providing a relatively better energy consumption model. In this protocol, each node in the network is considered as a particle and the sequence of particles from the source to the sink forms a path. Such a sequence of particles along the path is optimized by using IOLPSOA for finding the optimal path between the source and the sink. The IOLPSOA is evaluated using four well-known benchmark optimization functions such as Schwefel [33], [34], Griewank [34], [35], Rosenbrock [34], and Rastrigrin [35] and compared to standard particle swarm optimization (PSO), cooperative particle swarm optimization (PSOA)/CPSO [36] and OLPSOA-L [37]. An experimental evaluation conducted on the selected four functions shows that IOLPSOA provides the best solution when compared to the rest of the algorithms. Moreover, for performance analysis, IOLPSOA is combined with AODV and compared to AODV and AODV-SMS (simple sink mobility support) in terms of energy efficiency, packet loss ratio and packet delivery latency; the results show that IOLPSOA-AODV outperforms the other two on these aspects.

2) ENHANCED DETECTION SOLUTIONS (C4)

In order to solve the connectivity problem of the network, a fault detection and recovery scheme (FDRS) was proposed in [38], where an agent packet is generated by the sink, and such an agent builds a query link reaching a dead or a faulty node. The receiving node makes a decision randomly on whether to forward the packet or not in order to detect the dead or faulty nodes. Then the scheme will use the Least-Disruptive Topology Repair (LeDiR) algorithm to replace the target nodes with block movement. Their simulation shows that the proposed FDRS algorithm is superior to several existing algorithms such as LeDiR and Fault-Tolerant Service (FTS) in terms of metrics like delivery ratio and energy consumption. Such combinatorial schemes normally use localization and routing techniques to generate the optimal value; this has become a trend in recent research.

3) AI BASED DETECTION SOLUTIONS (C5)

Okazaki and Fröhlich [39] proposed an ant-based dynamic hop optimization protocol (ADHOP) for dynamic WSNs that incorporates an ACO algorithm for route discovery and maintenance. The focus of this work is mainly on mitigating the routing overhead in the WSNs and improving the data delivery ratio. ADHOP is a self-reconfiguring and multi-hop reactive routing protocol based on HOPNET, an ACO based protocol for MANETs. ADHOP differs from HOPNET in that it explicitly determines the next hop node dynamically rather than through the use of fixed size zones, as is the case with HOPNET. The constraints of WSNs are taken into account while designing the ADHOP architecture. However, the ADHOP algorithm is not evaluated in a WSN environment, rather in ad hoc wireless network environments. The performance of ADHOP is better than that of HOPNET in terms of routing overhead, congestion avoidance and the data delivery ratio in dynamic topology environments. On the other hand, solutions based on cross layer design are promising and energy efficient in WSNs. However, most of the solutions in the literature fail to include the complete range of mobility features.

Hoeller *et al.* [40] proposed that the transmission power of radio links between mobile nodes in mobile Ad-Hoc WSNs can be optimized by exploring the ACO method of ADHOP. ADHOP with power selection involved, i.e., ADHOP-PS, minimizes the energy consumption due to the transmission power with no effect on connectivity and with no significant influence on the packet delivery rate. A comparative analysis of ADHOP-PS with original ADHOP, AOER and AODV algorithms shows better results than the original ADHOP and AODV; however, AOER outperforms ADHOP-PS.

Zhang *et al.* [41] proposed a bio-inspired trusted routing protocol (B-iTRP) for trusted and energy efficient multi-hope routing in MWSNs. B-iTRP integrates AIS, ACO and physarum optimization (PO) algorithms to reliably assess the nodes along a path, to create an effective routing strategy from the source to the sink and for the assessment of route discovery and optimization of local routing, respectively. The AIC component of the protocol monitors the behavior of the neighboring nodes in real-time for the detection and identification of selfish and malicious nodes; since such nodes could expose MWSNs to malicious attacks. The simulation results show that B-iTRP performs better in terms of end-to-end packet delay and end-to-end packet delivery ratio when compared to AODV, TGRP and Ant Hoc Net protocols. However, B-iTRP incurs more communication control overhead when compared to the rest of the three protocols. In order to reduce the communication overhead, end-to-end delay, packet loss and energy consumption in WSNs and to improve the overall lifetime of WSNs, Saleem *et al.* [13] proposed an improved ant colony optimization (IACO) algorithm for the estimation of an optimal route based on the end-to-end delay, the link packet reception rate (PRR) and the remaining battery power of the sensor nodes. While IACO shows acceptable results in both simulations and implementation on a real test bed, it lacks the support for mobility and security, which are critical to the overall resilience of WSNs.

4) COOPERATION BASED DETECTION SOLUTIONS (C6)

In order to conserve the energy of sensor nodes in WSNs and reduce the latency in mobile data gathering, a polling-based data gathering approach via mobile collectors called bounded relay hop mobile data gathering (BRH-MDG) is proposed in [42]. In this approach, a mobile collector collects the aggregated data from the nodes in a WSN through predefined buffer nodes called polling points, which locally buffer the aggregated data from the affiliated nodes. These polling points are selected using centralized and distributed algorithms, respectively. The centralized algorithm is a shortest path tree based data gathering (SPT-DGA) algorithm whereas the distributed algorithm is apriority based PP selection algorithm (PB-PSA). Moreover, the SPT-DGA and PB-PSA schemes are evaluated against the single-hop data gathering (SHDG) scheme and the controlled mobile element (CME) scheme in terms of energy conservation, i.e., the relay hop count of sensors for local data aggregation, and data gathering latency wherein the tour length of the mobile collector is considered. The results show a comparative improvement in the tour length for small relay hop count. Although this solution improves energy and the mobile data gathering latency in WSNs with static sensor nodes, it might not be an optimal solution for MWSNs with mobile sensor nodes. This is because it considers a specific scenario wherein only the collector node is mobile and rest of the nodes are stationary.

Similarly, in order to optimize the communication power between the nodes of WSNs, Falcon et al., present a hybrid, i.e., controlled mobility and routing, model in [43]. For routing, a protocol called dynamic optimal progress routing (DOPR) is proposed. DOPR is similar to the optimal hop count routing'' (OHCR) protocol. In this work, energy consumption is optimized by moving the intermediate sensor nodes from a Move Directly (MD) scheme to a scheme using a predefined route between the source and the sink. Moreover, in this work, packet delivery is achieved by using a depth in first search (DFS) algorithm in both sparse and dense networks. This algorithm first uses another algorithm called collect-K neighbors routing (CKNR) algorithm to select K ideal hops to the network periphery. The packets are then sent out to any target along this route path. This solution not only solves the problem of energy consumption but also concurrently facilitates the mobility of the relay nodes. The proposed work shows improved results in comparison to other such protocols including NP, greedy, OHCR and MPoPR through various simulation tests.

In a scenario, where mobile sinks collect non-real time data, Rao and Biswas [44] present a framework for the feasibility of multi-hop routing in the network. The objective of this work is to determine the feasibility of the feasibility of the extent to which multi hop routing can be carried out for data collection in WSNs with mobile sinks by considering certain application parameters such as the node density, the data generation rate of nodes, the link capacity between the nodes, the mobility patterns of the sink and its speed. In such a framework, the data is routed from all the nodes in the network using multi-hop routing to a set of predefined designated gateway (DG) nodes. The mobile sink then collects the data from DGs' either on the move or on a stop on demand basis. In order to keep the balance between data collection, throughput, energy consumption, and sink trajectories, the extent of the multi-hop routing is defined through a hop bound factor with threshold values. The proposed framework is simulated in NS2 using the network assisted data collection (NADC) protocol for the validation of the predicted permanence trends of the model. For the identification of the trajectories of a mobile sink, a distributed version of the k-hop minimum dominating set technique is used.

Papadopoulos *et al.* [45] presented an energy efficient routing protocol called virtual infrastructure-based energy-efficient (VIBE) routing for WSNs with support for both static as well as mobile sensor nodes. In this protocol, the messages from the sensor nodes to the sinks are routed in a particular direction over a virtual infrastructure of virtual grids within a sensed area that includes a cluster head node. In order to reduce energy consumption due to communication overhead, the protocol does not use control messages for propagating the positions of the nodes to the neighboring nodes. The sensor nodes determine the positions in the field using the virtual grid mechanism. All nodes in the field could be mobile except the sink node and they are all location aware. Moreover, the performance of VIBE is evaluated in terms of energy efficiency through experiments and compared with those of other well-known protocols such as LEACH, MECH, greedy forwarding, and directed flooding protocol. The VIBE fairs comparatively better in terms of energy savings.

Maia *et al.* [46] developed a protocol called proFlex for data gathering in a distributed fashion in large-scale heterogeneous WSNs with mobile sinks. In this protocol, a set of powerful nodes with rich resources are used for data storage from where the mobile sink collects the data. ProFlex efficiently collects the data in the sensor field due to its ability of efficiently replicate the data among the selected storage nodes in the field and by avoiding data loss or failures as it might be the case with other protocols with similar powerful storage nodes in the network. In performance evaluation, simulations show satisfactory results for proFlex in terms of communication overheads, with decreasing incidence of energy hole vulnerability in the network and with stronger resilience against failures and message losses when compared to other storage protocols like, Supple, RaWMS, and Deep protocols [46]. Moreover, in WSNs, the transmission power of radio devices incurs most of the energy consumption [46].

In [47], a real-time mobility aware and load distribution (RTMLD) protocol is proposed. In this protocol, for data forwarding to a mobile sink in real-time and for routing management, a corona uniform model is incorporated instead of location-based routing. Moreover, RTMLD uses a backward corona mechanism to overcome the routing hole problem due to hidden nodes. In RTMLD, the optimal forwarding nodes in the network are determined through certain parameters such as the remaining power of the sensors, RSSI, and the delay incurred by the packets over one hop and then the traffic load is distributed among the neighboring nodes along the sink path thereby prolonging the lifetime of individual WSN nodes. The RTMLD achieves a high packet delivery ratio and low power consumption with minimum end-to-end delay in both MWSNs and WSNs. However, in the initial stage of neighbor discovery, RTMLD incurs communication overhead due to the identification of optimal forwarding nodes. RTMLD is evaluated against two static WSN protocols, namely MM-SPEED and RTLD, and a MWSN protocol called RACE. The simulations show that RTMLD has better performance in terms of packet delivery ratio, end-to-end delay and energy consumption; nevertheless, it has a higher packet overhead as compared to the rest of protocols. In addition, RTMLD is also implemented on a real experimental testbed and is shown to achieve satisfactory results. Combinatorial optimization methods have become more and more popular since they may show distinctive performance in terms of metrics that are encapsulated by another quadruple set as introduced in Eq. 2 (see below).

5) IMPROVED LOCALIZATION SOLUTIONS (C8)

Madani *et al.* [48] proposed an energy efficient cluster based power control routing (PCR) protocol and its enhanced version EPCR for MWSNs along with a packet loss recovery mechanism. In PCR, the nodes in a MWSN are associated with the cluster head via their weights, and this leads to a mapping problem particularly when a node is in the transmission range of more than one cluster-head and on the border of the transmission range of a potential cluster-head. In such a scenario, one possible solution could be the node going out of the transmission range of the potential cluster head. The EPCR protocols tackle this problem by using distance as a metric to associate nodes with a cluster head. PCR is based on the distributed efficient multi hop clustering protocol (DEMC) with the differences in cluster operation time, transmission power and recovery mechanism. PCR and EPCR are designed to work well for both mobile and static networks and achieves high throughput, longer network lifetime, and high packet delivery ratio. Moreover, in these protocols, the transmission power of the nodes is kept fixed during the clustering, inter-cluster communication and recovery phases. On the other hand, during the transmission of data by the nodes to their cluster-head, they change the transmission power according to their distance from their cluster-head since variable transmission power levels does not necessarily mean or lead to reduced signal strength [49]. In these protocols, the distance of a node from a cluster-head is determined through the use of the received signal strength indicator (RSSI) instead of GPS. Furthermore, PCR and EPCR are evaluated through simulations and in comparison to DEMC and Hybrid Energy efficient protocols (HEED) show satisfactory results.

Awwad *et al.* [50], proposed a cross layer design for routing in mobile wireless sensor networks. This work gets its inspiration from low energy adaptive clustering hierarchy (LEACH-mobile) protocol and principally aims to address issues that relate to packet delivery ratio and energy consumption. The solution proposed is a cluster based routing protocol for mobile sensor nodes (CBR-Mobile), which is based on cross layer optimization between medium access control (MAC) and network layers. In this solution, the routing decisions are made by collaborating with mobile nodes that use a hybrid MAC protocol and manage their schedule based and contention-based timeslots using TDMA. In the setup phase, carrier sense multiple access with collision avoidance (CSMA/CA) MAC protocol is used. For mobility, random waypoint mobility model is used. In CBR-Mobile, energy consumption is reduced by restricting the idle listening time and overhearing while the packet delivery ratio is improved by providing fast registration to the disconnected nodes. Moreover, in this protocol, the data is sent to the cluster-head in an efficient manner by using the received signal strength. Each cluster-head is equipped with a database to record and store the updates received from other nodes. Simulations show that the performance of CBR-Mobile is better than those proposed for LEACH-Mobile and AODV protocols in terms of packet delivery ratio, energy consumption, delay and fairness in the mobility environment.

In some situations, a sensor node may need to change its position. To address this case, an Energy Efficient Geographical Key Management (EEGKM) algorithm was introduced in [51]. In this approach, the cluster will first have to be divided, and then the node's motion is associated with the angles it makes with the sector heads. Simulation results show that such a scheme consumes low energy while increasing throughput when compared with other such algorithms like multi-level dynamic key management (MDKM) and energy efficient dynamic key management (EEDKM). More recently, hybrid methods have also become popular.

In [52], Abuarqoub *et al.* proposed a self-organizing and adaptive Dynamic Clustering (DCMDC) algorithm to balance the load and energy consumption in WSNs. The algorithm is a kind of a Routing Optimization method; it divides the network into clusters called Service Zones (SZs) to reduce the signaling overhead, to minimize route set up delay, and to improve bandwidth utilization. The experimental evaluation showed that DCMDC reduces mobility management cost, end-to-end delay, and energy consumption while increasing the network lifetime and packet delivery ratio when compared with other algorithms such as Mobile Data Collectors (MDCs).

Energy efficiency and tracking accuracy are two important factors in target tracking applications. Because of the special characteristic of WSNs, there exists a balance between energy consumption and tracking accuracy. Hirpara and Rana [53] proposed a hybrid Energy-Efficient Constant Gain Kalman Filter based Tracking (EECGKFT) algorithm to provide a perfect balance by integrating clustering and prediction techniques. The simulations showed that the proposed algorithm outperforms the existing algorithms. Analysis of results validates that EECGKFT increases energy efficiency by reducing the transmission of unnecessary data in the sensor network environment and also provides good tracking results. More recently new proposals have appeared that outline similar solutions.

6) COOPERATION BASED LOCALIZATION SOLUTIONS (C10)

Gaddour *et al.* [54] addressed the lack of mobility in an already existing IETF standard protocol for low power and lossy networks (RPL) by extending RPL to support the mobility of nodes in WSNs. This extension is called Co RPL. Co-RPL incorporates the corona architecture for mobility support in RPL. In Co-RPL, the network is divided into different circular layers called coronas around the static directed acyclic graph (DAG) roots, i.e., sinks, for better localization of mobile nodes with respect to the sinks. Simulation results reported in [54] show that Co-RPL reduces the packet loss ratio, end-to-end delay and energy consumption to a greater extent when compared to the standard RPL.

In order to access the efficiency of the proposed solutions we have introduced six tuple which is based on some performance related metrics that we obtained from the existing literature.

Let Metrics M be a six-tuple:

$$M = (Nc, Lf, Re, Tp, La, Ca) \tag{2}$$

as shown in Table 5.

TABLE 5. **Notation table in six-tuple *M*.**

Notation (VALUE=0 OR 1)	Performance Metric
Nc	Network Cost
Lf	Lifetime
Re	Reliability
Tp	Throughput
La	Latency
Ca	Capacity

The performance metrics are defined as:

- Network cost is the first and foremost metric of interest. The network cost increases and become more complex by adding more resources and vice versa.
- Lifetime can be defined as the time span from the deployment to the instant when the network/node is considered non-functional.
- Reliability can be defined as the probability of delivering message or data till the destination.
- Throughput is the rate of successful message delivered in a specified amount of time.
- Latency is the time a packet takes to travel from source to destination and sometimes the round-trip time.
- Capacity is the maximum number of bits that a link can accommodate.

Let f be the solution under consideration, then we have

$$M = f(C). \tag{3}$$

Where, the f is a guidance factor for the future research that can guide the researchers to design their own algorithms or build strategies and map the combination C of algorithms or strategies (many items in Quadruple) to get a concerned optimal result M.

In this paper, the proposed classification is based on Eq. 1, while the mobility management solutions comparison in terms of performance metrics are performed with the help Eq. 2.

B. MOBILITY ISSUES RELATED LITERATURE COMPARISON

According to the classification of mobility related issues based on 19 key papers, a comparison in Table 6 of the existing techniques is performed in terms of location awareness, energy efficiency, the use of GPS, clustering, the use simulation/experimental testbed using, type of simulators used, and security considerations.

IV. OPEN ISSUES AND CHALLENGES

Based on our literature study and its subsequent analysis, we highlight the important issues that need to be addressed, and also provide a concise summary of emerging research trends and challenges.

A. OPEN ISSUES

The following are the issues that need to be addressed in the near future.

1) NODE SECURITY SUPPORT IN MWSN

We have not come across any scheme addressing mobile nodes with pre-consideration for data losses or privacy breaches. In the Internet of Things (IoT) paradigms, where MWSNs will be an integral part of the infrastructure, data can be lost or compromised in myriad, and planning against privacy threats must be undertaken before executing an event.

2) MIPv6 SUPPORT IN MWSN

The bulk of the schemes reported in the literature on IP based WSNs use Internet Protocol version 4, which has limited support for node mobility. A handful of schemes have been developed that are fully compliant with 6LoWPAN mobility support features such as some extended protocols of MIPv6. Although these protocols are easy to deploy, they still have some limitations. When considering routing related issues such as resource-based routing support, host-based routing support, Home Address (HA) and Care-of-Address (CoA) support, proposed solutions must aim to mitigate path and address the underlying route construction and coverage related issues in a holistic manner. All these exceptions in the literature are addressed in static, but not all anomalous conditions are addressed.

3) DATA SECURITY AND NETWORK INTEGRITY IN MWSN

As discussed above, security and privacy are together considered as a separate and atomic feature in WSNs, which is only triggered reactively for the identified threats and proactively for the known threats. In instances when zero-day attacks are launched against the network, the defense mechanisms that are deployed will not take appropriate measures to stop it since these mechanisms are unable to discover such attacks in the first place.

The discovery of network attacks is intrinsically linked to anomaly detection. Network traffic variables such as packet latency, packet structure, bandwidth, and data flow are typically fingerprinted and any variation in the normal ranges of the variables is treated as an anomaly. A typical anomaly requires human analysis and intervention. Once an

TABLE 6. **MWSNs state-of-the-art literature comparison.**

Scheme	Class	Location aware nodes	Energy efficiency	GPS	Clustering	Simulation/ Experiment	Simulator used	Security	*M (Nc, Lf, Re, Tp, La, Ca)*
Hu et al., [32]	*C3*	No	Yes	No	No	Simulation	MATLAB (future work aims at its integration into Zigbee and TinyOs)	N/A	(1,1,1,0,1,0)
Yuvaraja et al., [38]	*C4*	No	Yes	No	Yes	Simulation	NS2 version 2.32	Yes (identification of abnormal nodes)	(1,1,1,0,1,0)
K. Saleem et al., [13]	*C5*	No	No	No	No	Simulation + experimental test bed	NS2 + real WSN test bed based on TelosB mode with TOSSIM framework	Yes (identification of self and non-self data packets)	(1,1,1,0,1,1)
A. González et al., [28]		Yes	Yes	No	Yes	Simulation	Eboracum Simulator	N/A	(1,1,0,0,0,0)
Okazaki & Fr¨ohlich[39]		No	No	No	No	Simulation	GloMoSim	N/A	(0,1,1,0,1,1)
A Hoeller et al., [40]		No	Yes	No	No	Simulation	OMNeT++ simulator	N/A	(1,1,0,0,0,0)
M. Zhang et al., [41]		No	Yes	No	No	Simulation	NS2 version 2.34	Yes (identification of selfish and malicious nodes)	(0,1,1,0,1,0)
Zhao & Yang [42]	*C6*	No	Yes	No	No	Simulation	CPLEX	N/A	(1,1,0,1,1,0)
Falcon et al., [43]		Yes (relay nodes are calculated)	Yes	Yes (Source node)	No	Simulation	MATLAB	N/A	(1,1,1,0,0,0)
J. Rao & S. Biswas [44]		No	Yes	No	No	Simulation (a framework model)	NS2	N/A	(1,1,1,0,1,0)
Papadopoulos et al., [45]		Yes	Yes	No	Yes	Simulation	N/A (a prototype was implemented in TinyOS2.x)	N/A	(1,1,0,0,0,0)
G. Maia et al., [46]		No	Yes	No	No	Simulation	Sinalgo simulator version 0.75.3	N/A	(1,1,1,0,0,0)
A A. Ahmed & N. Fisal [47]		No	Yes	No	No	Simulation + experimental test	NS2 + (TelosB motes is used as a test bed)	N/A	(1,1,1,0,1,0)
Khan et al., [48]	*C8*	No	Yes	No	Yes	Simulation	OMNET++ v4.0 (INET)	N/A	(0,1,1,1,0,0)
Awwad et al., [50]		No	Yes	No	Yes	Simulation	MATLAB	N/A	(0,1,1,0,1,0)
G. Rohini et al., [51]		No	Yes	No	Yes	Simulation	NS2 simulator	Yes (key transmission guaranteed)	(0,1,0,0,0,0)
A. Abuarqoub et al., [52]		Yes	Yes	Yes	Yes	Simulation	NS3 simulator	N/A	(0,1,1,0,1,0)
KirtiHirpara et al., [53]		Yes	Yes	Yes	Yes	Simulation	MATLAB	N/A	(0,1,0,0,0,0)
O. Gaddour et al., [54]	*C10*	No	Yes	No	No	Simulation	Contiki / Cooja simulator	N/A	(0,1,1,0,1,0)

incoming traffic flow is classified as a threat, appropriate countermeasures can then be developed to safeguard against such attacks.

Mobility brings uncertainty in the network topology. In order to cope with uncertainty, specific mobility management schemes have been proposed. The issues of privacy preservation were left out from the list of considered issues. Presumably, every action in the network may lead to a privacy breach. Node mobility being a major event in the network may lead to data leakage, hence it should be addressed by using mechanisms based on data encryption, or obfuscation techniques.

4) SIMULATION-BASED VS TESTBED-BASED EMPIRICAL STUDIES OF MWSN

When designing a simulation environment, certain topological assumptions are made. Furthermore, in a simulation environment, the movement pattern of a mobile node is often found to be pseudo random. Many experiments involving a test bed implementation consider a specific MWSN. The application specific constraints need to be considered in the development phase. Due to this discrepancy, a difference in the performance is observed when conducting simulations over different WSN set ups. The deployed solutions show skewness from the expected results and these results are then presented in the literature without a clear awareness of the limitations.

5) LACK OF AUTONOMOUS AND PLUG-AND-PLAY SUPPORT FOR OPTIMAL SOLUTIONS IN MWSNs

The proposed solutions to mobility management require an intensive configuration that often requires manual labor. In an ubiquitous network paradigm, the node down time is directly proportional to loss in revenue. In all the solutions that were reviewed, we have not come across any scheme that supports plug and play solutions.

B. TRENDS AND CHALLENGES

From the distribution of the studies shown in Table 4, we can conclude that the classification of recent studies does not obey a uniform distribution as shown in Table 7.

TABLE 7. Literature distribution analysis.

Technique (s) used in Quadruple C	NO. OF STUDIES	Real Ratio of Studies	Ratio of Classes in a Uniform Distribution (15 classes totally)
Single Technique	7	7/19 = 37%	4/15 = 27%
Multiple Techniques	12	12/19 = 63%	6/15 = 40%

Table 3 shows 4 classes that use a single technique, and 6 classes that use multiple techniques. Since we have selected 19 papers out of a total of 478, and the selection criteria did not have anything to do with the number of techniques that a proposal used, we can safely conclude that the selection process as arbitrary and random as illustrated in the table. It is clearly shown in Table 7 that 63% of the total schemes studied use hybrid techniques as opposed to 40 % that are based on a single technique, a recent trend currently prevalent in mobility management of MWSNs.

MWSNs also introduce significant challenges, such as those that relate to [10], which are Scheduling, Reliability, Mobility, Localization, Dynamic Network Topology.

Moreover, since we have entered into the realm of Big data and AI [55], it is essential for us to leverage technologies and algorithms based on these paradigms to empower mobility management. As a result, the vision for futuristic mobility management solutions must be expanded to accommodate these novel approaches. Quadruple C in Eq. 1 should be extended to a more complex five-tuple, by adding Dimension & Security elements in it. The combination of single or hybrid solutions has potential to become the mainstream in future research. In future, intelligence, complexity and performance would be expected to gain more prominence. Moreover, the increasing complexity of the proposed algorithms and security would become the most important challenges in MWSNs.

V. CONCLUSIONS AND FUTURE WORK

In this paper, we have presented a critical analysis on mobility management related issues in MWSNs for cyber physical systems. The aim of the paper is to highlight the important issues and to reveal the recent trends and current challenges that can provide the guidance to the future research endeavors in the area/field. We have explored the recent state of the art literature on mobility management in MWSNs and suggested a novel classification method to classify these schemes based on the techniques that they use. Our classification uses one quadruple set C and six-tuple M in order to offer a solution for further analysis.

Our review shows that indicators like location awareness among mobile nodes brings a sense of relevant movement, and hence results in graceful handoff in MWSNs. This becomes an important issue when the leaving node is a cluster head. In addition, energy efficiency has been addressed abundantly due to the assumption that the nodes in a MWSN have a very limited lifetime, a key issue that requires further investigation.

Furthermore, we have also discovered that mobility supported protocols still have limitations due to real-time constraints. Moreover, we have found that most of the reported test beds are custom built rather than being plug and play hence lack self-configuration features. Besides, MWSN nodes are not assumed to have Global Positioning System (GPS) capabilities except for certain high power nodes that play the role of a cluster head. As the GPS technology has become more accessible, this assumption needs to be reconsidered. Another point which is found to be noteworthy is that while clustering is the most popular and almost ubiquitous aggregation method among MWSNs, security remains the least considered issue among all other issues for MWSNs.

Thus, we believe that the discussion of the recent trends and current challenges in this analysis will provide further guidance for future research in MWSNs.

ACKNOWLEDGMENT

(JALAL AL-MUHTADI and MA QIANG are co-first authors.)

REFERENCES

[1] A. Gawanmeh and K. Saleem, “Introduction to the special issue on communication, computing, and networking in cyber-physical systems,” *Scalable Comput., Pract. Experim.*, vol. 18, no. 4, p. 3, 2017.

[2] K. Saleem, Z. Tan, and W. Buchanan, "Security for cyber-physical systems in healthcare," in *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*, C. Thuemmler and C. Bai, Eds. Cham, Switzerland: Springer, 2017, pp. 233–251.

[3] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.

[4] M. Yaseen *et al.*, "Secure sensors data acquisition and communication protection in eHealthcare: Review on the state of the art," *Telematics Inform.*, to be published. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0736585316304968

[5] M. S. Kamal, S. Parvin, K. Saleem, H. Al-Hamadi, and A. Gawanmeh, "Efficient low cost supervisory system for Internet of Things enabled smart home," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC)*, May 2017, pp. 864–869.

[6] X. Xu, W. Liang, X. Jia, and W. Xu, "Network throughput maximization in unreliable wireless sensor networks with minimal remote data transfer cost," *Wireless Commun. Mobile Comput.*, vol. 16, no. 10, pp. 1176–1191, 2016.

[7] K. Saleem, "Biological inspired self-organized secure autonomous routing protocol for wireless sensor networks," Doctor Philosophy, Faculty Elect. Eng., University of Technology, Malaysia, Johor Bahru, Malaysia, 2011.

[8] D. Yuan, S. S. Kanhere, and M. Hollick, "Instrumenting wireless sensor networks—A survey on the metrics that matter," *Pervasive Mobile Comput.*, vol. 37, pp. 45–62, Jun. 2017.

[9] M. Bouaziz and A. Rachedi, "A survey on mobility management protocols in wireless sensor networks based on 6LoWPAN technology," *Comput. Commun.*, vol. 74, pp. 3–15, Jan. 2016.

[10] A. Sayyed and L. B. Becker, "A survey on data collection in mobile wireless sensor networks (MWSNs)," in *Cooperative Robots and Sensor Networks*. New York, NY, USA: Springer, 2015, pp. 257–278.

[11] M. Amadeo *et al.*, "Information-centric networking for the Internet of Things: Challenges and opportunities," *IEEE Netw.*, vol. 30, no. 2, pp. 92–100, Mar./Apr. 2016.

[12] F. Ren, H. Zhou, L. Yi, Y. Qin, and H. Zhang, "HMMCCN: A hierarchical mobility management scheme for content-centric networking," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 22, no. 3, pp. 139–152, 2016.

[13] K. Saleem, N. Fisal, and J. Al-Muhtadi, "Empirical studies of bio-inspired self-organized secure autonomous routing protocol," *IEEE Sensors J.*, vol. 14, no. 7, pp. 2232–2239, Jul. 2014.

[14] G. Han, J. Jiang, C. Zhang, T. Q. Duong, M. Guizani, and G. Karagiannidis, "A survey on mobile anchor node assisted localization in wireless sensor networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2220–2243, 3rd Quart., 2016.

[15] J. A. Chaudhry, U. Tariq, M. A. Amin, and R. G. Rittenhouse, "Sinkhole vulnerabilities in wireless sensor networks," *Int. J. Security Appl.*, vol. 8, no. 1, pp. 401–410, 2014.

[16] S. Ali, A. Naveed, M. A. B. Ngadi, and J. A. Chaudhry, "Interference nomenclature in wireless mesh networks," *Wireless Pers. Commun.*, vol. 75, pp. 1983–2003, Apr. 2014.

[17] W. Tang, X. Ma, J. Huang, and J. Wei, "Toward improved RPL: A congestion avoidance multipath routing protocol with time factor for wireless sensor networks," *J. Sensors*, vol. 2016, Jun. 2016, Art. no. 8128651. [Online]. Available: https://www.hindawi.com/journals/js/2016/8128651/

[18] T. Winter, "RPL: IPv6 routing protocol for low-power and lossy networks," Internet Eng. Task Force, Fremont, CA, USA, Tech. Rep. RFC: 6550, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6550

[19] K. Saleem and N. Fisal, "Energy efficient information assured routing based on hybrid optimization algorithm for WSNs," in *Proc. 10th Int. Conf. Inf. Technol., New Generat.*, 2013, pp. 518–524.

[20] A. A. Ahmed and N. F. Fisal, "Secure real-time routing protocol with load distribution in wireless sensor networks," *Secur. Commun. Netw.*, vol. 4, no. 8, pp. 839–869, Aug. 2011.

[21] E. Amiri, H. Keshavarz, M. Alizadeh, M. Zamani, and T. Khodadadi, "Energy efficient routing in wireless sensor networks based on fuzzy ant colony optimization," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 7, p. 768936, 2014.

[22] R. Singh, J. Singh, and R. Singh, "Fuzzy based advanced hybrid intrusion detection system to detect malicious nodes in wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2017, Apr. 2017, Art. no. 3548607. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/3548607/

[23] X. Zhang, X. Dong, J. Wu, Z. Cao, and C. Lyu, "Fault activity aware service delivery in wireless sensor networks for smart cities," *Wireless Commun. Mobile Comput.*, vol. 2017, Sep. 2017, Art. no. 9394613. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/9394613/

[24] B. A. Attea and E. A. Khalil, "A new evolutionary based routing protocol for clustered heterogeneous wireless sensor networks," *Appl. Soft Comput.*, vol. 12, no. 7, pp. 1950–1957, 2012.

[25] D. Karaboga, S. Okdem, and C. Ozturk, "Cluster based wireless sensor network routing using artificial bee colony algorithm," *Wireless Netw.*, vol. 18, no. 7, pp. 847–860, 2012.

[26] U. Pervez, A. Mahmood, O. Hasan, K. Latif, and A. Gawanmeh, "Formal reliability analysis of device interoperability middleware (DIM) based E-health system using PRISM," in *Proc. 17th Int. Conf. e-Health Netw., Appl. Services (HealthCom)*, Oct. 2015, pp. 108–113.

[27] Y.-C. Wang, F.-J. Wu, and Y.-C. Tseng, "Mobility management algorithms and applications for mobile sensor networks," *Wireless Commun. Mobile Comput.*, vol. 12, no. 1, pp. 7–21, 2012.

[28] A. V. González, L. Brisolara, and P. R. Ferreira, "Efficiency evaluation of strategies for dynamic management of wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2017, Jan. 2017, Art. no. 5618065. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/5618065/

[29] A. Achour, L. Deru, and J. C. Deprez, "Mobility management for wireless sensor networks a state-of-the-art," *Proc. Comput. Sci.*, vol. 52, pp. 1101–1107, Jan. 2015.

[30] N. Sabor, S. Sasaki, M. Abo-Zahhad, and S. M. Ahmed, "A comprehensive survey on hierarchical-based routing protocols for mobile wireless sensor networks: Review, taxonomy, and future directions," *Wireless Commun. Mobile Comput.*, vol. 2017, Jan. 2017, Art. no. 2818542. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/2818542/

[31] S. Hamrioui *et al.*, "A systematic review of security mechanisms for big data in health and new alternatives for hospitals," *Wireless Commun. Mobile Comput.*, vol. 2017, Dec. 2017, Art. no. 2306458. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/2306458/

[32] Y. Hu, Y. Ding, K. Hao, L. Ren, and H. Han, "An immune orthogonal learning particle swarm optimisation algorithm for routing recovery of wireless sensor networks with mobile sink," *Int. J. Syst. Sci.*, vol. 45, no. 3, pp. 337–350, 2014.

[33] T. Bäck and H.-P. Schwefel, "An overview of evolutionary algorithms for parameter optimization," *Evol. Comput.*, vol. 1, pp. 1–23, Dec. 1993.

[34] M. A. Potter and K. A. De Jong, "A cooperative coevolutionary approach to function optimization," in *Parallel Problem Solving From Nature*, Y. Davidor, H.-P. Schwefel, and R. Männer, Eds. Berlin, Germany: Springer, 1994, pp. 249–257.

[35] W. Jiao, G. Liu, and D. Liu, "Elite Particle Swarm Optimization with mutation," in *Proc. Asia Simulation Conf. 7th Int. Conf. Syst. Simulation Sci. Comput.*, 2008, pp. 800–803.

[36] F. van den Bergh and A. P. Engelbrecht, "A cooperative approach to particle swarm optimization," *IEEE Trans. Evol. Comput.*, vol. 8, no. 3, pp. 225–239, Jun. 2004.

[37] Y. F. Hu, X. M. Wu, F. Q. Wang, and H. Han, "A particle swarm algorithm based routing recovery method for mobile sink wireless sensor networks," in *Proc. 26th Chin. Control Decision Conf. (CCDC)*, 2014, pp. 887–892.

[38] M. Yuvaraja and M. Sabrigiriraj, "Fault detection and recovery scheme for routing and lifetime enhancement in WSN," *Wireless Netw.*, vol. 23, pp. 267–277, Jan. 2017.

[39] A. M. Okazaki and A. A. Fröhlich, "Ant-based dynamic hop optimization protocol: A routing algorithm for mobile wireless sensor networks," in *Proc. IEEE GLOBECOM Workshops (GC Wkshps)*, Dec. 2011, pp. 1139–1143.

[40] A. Hoeller, P. Oliveira, and A. A. Frohlich, "Dynamic adjustment of transmission power of mobile ad-hoc wireless sensor networks," in *Proc. Brazilian Symp. Comput. Syst. Eng. (SBESC)*, 2013, pp. 167–168.

[41] M. Zhang, C. Xu, J. Guan, R. Zheng, and H. Zhang, "A novel bio-inspired trusted routing protocol for mobile wireless sensor networks," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 1, pp. 74–90, 2014.

[42] M. Zhao and Y. Yang, "Bounded relay hop mobile data gathering in wireless sensor networks," *IEEE Trans. Comput.*, vol. 61, no. 2, pp. 265–277, Feb. 2012.

[43] R. Falcon, H. Liu, A. Nayak, and I. Stojmenovic, "Controlled straight mobility and energy-aware routing in robotic wireless sensor networks," in *Proc. IEEE 8th Int. Conf. Distrib. Comput. Sensor Syst. (DCOSS)*, May 2012, pp. 150–157.

[44] J. Rao and S. Biswas, "Analyzing multi-hop routing feasibility for sensor data harvesting using mobile sinks," *J. Parallel Distrib. Comput.*, vol. 72, no. 6, pp. 764–777, 2012.

[45] A. Papadopoulos, A. Navarra, J. A. McCann, and C. M. Pinotti, "VIBE: An energy efficient routing protocol for dense and mobile sensor networks," *J. Netw. Comput. Appl.*, vol. 35, no. 4, pp. 1177–1190, 2012.

[46] G. Maia, D. L. Guidoni, A. C. Viana, A. L. L. Aquino, R. A. F. Mini, and A. A. F. Loureiro, "A distributed data storage protocol for heterogeneous wireless sensor networks with mobile sinks," *Ad Hoc Netw.*, vol. 11, no. 5, pp. 1588–1602, 2013.

[47] A. A. Ahmed and N. Fisal, "A real–time routing protocol with mobility support and load distribution for mobile wireless sensor networks," *Int. J. Sensor Netw.*, vol. 15, no. 2, pp. 95–111, 2014.

[48] A. R. Khan, S. A. Madani, K. Hayat, and S. U. Khan, "Clustering-based power-controlled routing for mobile wireless sensor networks," *Int. J. Commun. Syst.*, vol. 25, no. 4, pp. 529–542, 2012.

[49] S. Max and T. Wang, "Transmit power control in wireless mesh networks considered harmful," in *Proc. 2nd Int. Conf. Adv. Mesh Netw. (MESH)*, 2009, pp. 73–78.

[50] S. A. B. Awwad, C. K. Ng, N. K. Noordin, and M. F. A. Rasid, "Cluster based routing protocol for mobile nodes in wireless sensor network," *Wireless Pers. Commun.*, vol. 61, pp. 251–281, May 2011.

[51] G. K. Chella Thevar and G. Rohini, "Energy efficient geographical key management scheme for authentication in mobile wireless sensor networks," *Wireless Netw.*, vol. 23, pp. 1479–1489, Jul. 2017.

[52] A. Abuarqoub, M. Hammoudeh, B. Adebisi, S. Jabbar, A. Bounceur, and H. Al-Bashar, "Dynamic clustering and management of mobile wireless sensor networks," *Comput. Netw.*, vol. 117, pp. 62–75, Apr. 2017.

[53] K. Hirpara and K. Rana, "Energy-efficient constant gain Kalman filter based tracking in wireless sensor network," *Wireless Commun. Mobile Comput.*, vol. 2017, Apr. 2017, Art. no. 1390847. [Online]. Available: https://www.hindawi.com/journals/wcmc/2017/1390847/

[54] O. Gaddour, A. Koubaa, R. Rangarajan, O. Cheikhrouhou, E. Tovar, and M. Abid, "Co-RPL: RPL routing for mobile low power wireless sensor networks using Corona mechanism," in *Proc. 9th IEEE Int. Symp. Ind. Embedded Syst. (SIES)*, Jun. 2014, pp. 200–209.

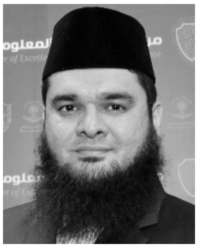
[55] M. Lytras, V. Raghavan, and E. Damiani, "Big data and data analytics research: From metaphors to value space for collective wisdom in human decision making and smart machines," *Int. J. Semantic Web Inf. Syst.*, vol. 13, no. 1, pp. 1–10, 2017.

JALAL AL-MUHTADI received the Ph.D. and M.S. degrees in computer science from the University of Illinois at Urbana–Champaign, USA. He is currently the Director of the Center of Excellence in Information Assurance, King Saud University, and also a Faculty Member with the Department of Computer Science, King Saud University. He has published over 50 scientific papers in the areas of cybersecurity and the Internet of Things. His areas of expertise include cybersecurity, information assurance, privacy, and Internet of Things.

MA QIANG received the M.S. degree in computer science from Lanzhou University, China, in 2009, and the Ph.D. degree in computer science from King Saud University, Saudi Arabia, in 2016. He is currently with the Center of Excellence in Information Assurance, King Saud University. His research interests include artificial intelligence and network security.

KHAN ZEB received the B.Sc. degree in telecommunication engineering from the University of Engineering and Technology, Peshawar, Pakistan, in 2010, and the M.S. degree in electrical engineering from King Saud University, Riyadh, Saudi Arabia, in 2015. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC, Canada. He was a Researcher with the Center of Excellence in Information Assurance, King Saud University, from 2015 to 2016. His research interests include wireless networks, optical networks, fronthaul, RoF, C-RAN, cyber security, anomaly/intrusion detection, e-healthcare/m-healthcare systems, and IoTs.

JUNAID CHAUDHRY has a career which has so far led him on a journey through academia, law enforcement and industry. Past roles have been leading security researchers with Duja Inc., and holding positions with the University of Amsterdam, Qatar University, University Technology Malaysia, the University of Hail, the University of Trento, and the University of South Pacific. He was also with Al-Jazeera, the State of Qatar, Qatar Foundation, and FBK-Italy as a Consultant. He is currently an Assistant Professor with the College of Security and Intelligence, Embry-Riddle Aeronautical University, Prescott, AZ, USA. He is also currently focused on researching context aware security in medical informatics while also having an interest in digital forensics, network security, and interdisciplinary research in cyber security. With over 50 published papers, authorship of three international books, two patents, and 15 technical reports, he frequently volunteers in organizing conferences, reviewing research reports for scientific journals, editing special issues, and community outreach programs.



KASHIF SALEEM received the M.E. and Ph.D. degrees in electrical engineering from University Technology Malaysia, in 2007 and 2011, respectively. He has been an Assistant Professor with the Center of Excellence in Information Assurance, King Saud University, since 2012, and a Visiting Fellow with the Department of Computing, Faculty of Science and Engineering, Macquarie University, Sydney, Australia. He has authored and co-authored over 90 papers in refereed international journals and conferences. His research interests include telecommunications, computer security, wireless communication, wireless security, artificial intelligence, and bioinformatics. He has also served as a TPC member of numerous international conferences and workshops. He is an Associate Editor and Reviewer for over 30 reputed international journals. He has organized International and local events as Reliability of eHealth Information Systems, Security and Privacy in Next Generation Networks, International Symposium on Health Informatics, and International Workshop on Networks of Sensors, Wearable, and Medical Devices. He acquired several research grants in KSA, EU, and the other parts of the world.

ABDELOUAHID DERHAB received the engineering, master's, and Ph.D. degrees in computer science from the University of Sciences and Technology Houari Boummediene, Algiers, in 2001, 2003, and 2007, respectively. He was a Computer Science Engineer and a Full-Time Researcher with CERIST Research Center, Algeria, from 2002 to 2012. He is currently an Assistant Professor with the Center of Excellence in Information Assurance, King Saud University. His research interests include network security, intrusion detection systems, malware analysis, mobile security, and mobile networks.

MEHMET A. ORGUN (SM'96) received the B.Sc. and M.Sc. degrees in computer science and engineering from Hacettepe University, Ankara, Turkey, in 1982 and 1985 respectively, and the Ph.D. degree in computer science from the University of Victoria, Canada, in 1991. He is currently a Professor with the Department of Computing, Macquarie University, Sydney, Australia. His professional service includes editorial and review board memberships of several leading journals and program committee and senior program committee memberships of numerous national and international conferences. His current research interests include knowledge discovery, multi-agent systems, and trusted and secure systems. Recently, he was the Program Co-Chair of the 14th Pacific-Rim International Conference on Artificial Intelligence in 2010; and Conference Co-Chair of the 7th and 8th International Conferences on Security of Information and Networks in 2014 and 2015.

RAJAN SHANKARAN received the M.B.A. (MIS) degree in information systems from the Maastricht School of Management in 1994, and the M.Sc. degree (Hons.) and the Ph.D. degree in network communications and security from the University of Western Sydney in 1999 and 2005, respectively. He is currently a Senior Lecturer and the Deputy Director (PG studies) with Macquarie University, Sydney, Australia. He mainly works in the areas of D2D communications, medical implant security, network security, and trust in mobile networks. He has served as a program committee member for a number of conferences in computer networking and security. More recently, he has served as a Technical Program Committee Member for WMNC 2017, Mobility 2017, and WCNC 2018. He was also recently on the organizing committee of IEEE/IFIP NOMS 2017 and CNSM 2017.

MUHAMMAD IMRAN is currently with King Saud University and is a Visiting Scientist with Iowa State University. He has published a number of research papers in refereed international conferences and journals. His research interests include MANETs, WSNs, WBANs, M2M/IoT, SDN, and security and privacy. He serves as a Co-Editor-in-Chief for EAI Transactions and an Associate/Guest Editor for IEEE ACCESS, IEEE *Communications Magazine*, COMPUTER NETWORKS, SENSORS, IJDSN, JIT, WCMC, AHSWN, IET WSS, IJAACS, and IJITEE.

MARUF PASHA received the M.Sc. degree from the National University of Sciences and Technology, Pakistan, and the Ph.D. degree from the University of South Brittany, France. He is currently associated with the Department of Information Technology, Bahauddin Zakariya University, Pakistan. His areas of interest include agent programming, semantic web services, and computer security. He is involved in various funded projects and is also an HEC approved supervisor for doctoral and graduate studies in Pakistan.

• • •