jet INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2021, VOL. 67, NO. 3, PP. 483-496
Manuscript received September 10, 2020; revised July, 2021 DOI: 10.24425/ijet.2021.137838

A Comprehensive Survey on Routing and Security in Mobile Wireless Sensor Networks

Ahmed Al-Nasser, Reham Almesaeed, and Hessa Al-Junaid

***Abstract*—With the continuous advances in mobile wireless sensor networks (MWSNs), the research community has responded to the challenges and constraints in the design of these networks by proposing efficient routing protocols that focus on particular performance metrics such as residual energy utilization, mobility, topology, scalability, localization, data collection routing, Quality of Service (QoS), etc. In addition, the introduction of mobility in WSN has brought new challenges for the routing, stability, security, and reliability of WSNs. Therefore, in this article, we present a comprehensive and meticulous investigation in the routing protocols and security challenges in the theory of MWSNs which was developed in recent years.**

***Keywords*—WSN, routing, security**

I. Introduction

WIRELESS Sensor Network (WSN) refers to the network consisting of multiple computational units with the ability to sense specific physical properties of the environment. The computational units which are called sensor nodes are connected together through wireless links to each other and a special node called base station or sink [1]. The sensor node is a small device with tiny sensors that can be deployed either inside the parameter of the phenomenon which is required to be monitored or deployed close to it. Sensor nodes can be equipped with different types of sensors and can monitor various properties and phenomena. The types of sensors include vibration sensors which monitor earthquakes, thermal sensors for monitoring temperatures and climate changes, acoustic sensors for sensing sound waves and noise levels, visual sensors to measure lightening condition, infrared and radar sensors to sense the presence or absence of objects, and vehicular movement, speed, and directions sensor to measure mobility. Sensor nodes contain sensing components and a transceiver unit to send and receive data from a central processing station. Many applications of WSN require the sensor node to conduct data collection, data analysis, and correlation of the data collected by the node sensors. To achieve the required tasks, sensor nodes are equipped with sensors, processing capabilities, communication units, and onboard storage [2].

While the interest in the WSN applications is rapidly emerging nowadays, the technology of using sensors for special proposes can be traced back to older times. In the mid-1950s and during the Cold War, The United States Navy installed a big network of underwater sensors that can detect Soviet submarines that are using quiet technologies. The project was called the Sound Surveillance System (SOSUS), which is used today for scientific purposes such as monitoring whales and oceans temperature. Similar to the underwater monitoring system, Air Defense deployed monitoring systems by using sensors installed on aerostatic balloons. In 1980, the Defense Advanced Research Projects Agency started the Distributed Sensor Networks (DSN) project, which is considered the actual beginning of the WSNs [3] [4]. One of the major advancements in the WSN field is the introduction of the Mobile Wireless Sensor Network (MWSN). In the MWSN, the sensor nodes are mobile which makes the sensor network applications more versatile compared to the static nodes. The mobile nodes' movement can be either dependent or independent of each other. Some applications in the fields of healthcare, military, transportation, and industry require the mobility of sensor nodes to support the mobility of the sensed objects [5][6]. The mobility introduces new challenges to the sensors network such as the network coverage and reliability of communication as well as introducing new security challenges.

The remainder of the article is organized as follows: In Section 2, we present an overview of wireless sensor networks structure, topologies and applications. In section 3 we discuss routing in WSN, in particular, we present the routing challenges and intensive discussion of the routing protocols classifications which proposed in the literature. Section 4 provides detail investigation in the security aspects of WSN, and the proposed state-of-art routing mechanisms in the literature. Finally, section 5 concludes the article.

II. Overview of Wireless Sensor Networks

MWSNs are an advanced type of Wireless Sensor Networks (WSN), which present mobility as a new factor for both sensor nodes and the base station. Because the mobility introduces new challenges to the network such as reliability and security challenges, MWSNs require considerations in regard to the network topology, routing protocols, physical security, and information security.

A. MWSN Network Topology

In MWSN, a network is considered effective if both data collection and topology management are reliable. The network topology should provide guaranteed quality of the service regarding the mobility, traffic, and network connection stability Network topology management is the task responsible for managing the membership of sensor nodes group by managing the new and withdrawn members. Depending on the nature of the MWSN, in order to achieve the best performance and to

Authors are with University of Bahrain College of Information technology, Bahrain (e-mail: ralmesaeed@uob.edu.bh).

ensure reliable data gathering. different types of network topologies are deployed. Such as: flat or unstructured, chain, mesh, tree, clustered, and hybrid [7].

B. Routing in MWSN

Routing protocols for MWSN require consideration of the mobility nature of the nodes as well as the changes in the network topology. In static approaches of WSNs, the nodes and the base stations are stationary and the distances, signal ranges, and neighbour nodes are known to each member of the network. Unlike stationary approaches, mobility approaches should consider all types of applications of MWSNs. There are three mobility approaches: (a) Static base station and moving nodes, (b) Moving base station and static nodes, and (c) moving base station and moving sensor nodes. Routing protocols in MWSN are inspired by both its predecessor the Wireless Sensor Network and the Mobile Ad hoc Network (MANET). While MANET protocols are designed to support mobility, there are several considerations to be made regarding the variations between MANET and MWSN. While the main objective of the MWSN is to collect information from sensor nodes, MANET is designed to manage distributed computing units. MWSN networks can be much bigger in coverage and in the number of sensing nodes that are needed to study a phenomenon. MWSN nodes mainly communicate by broadcast data and mainly toward the sink node while MANET nodes use point to point two-way irregular communications. Because of their unattended operations, cost, and size, sensor nodes in MWSN have limited resources and computational power comparing to the counterparts in MANET [8] [9] [10]. Routing protocols in WSN are categorized based on several properties. Depending on the network structure, routing protocols are classified as (a) Flat based routing protocols where all nodes are assigned similar roles, (b) hierarchical based routing where nodes have different roles, and (c) location-based routing where the location of the nodes is used for routing. Furthermore, routing protocols are classified based on the process performed to find the route to the destination. In this classification, there are three categories which are (a) Proactive routing where the routes are pre-calculated and pre-determined, (b) Reactive routing where the routing paths are determined on request, and (c) Hybrid routing where both proactive and reactive routing is used. When the nodes are stationary, the preferred approach is to precompute the routing paths rather than calculating the routing paths on demand. Energy and computational limitations add more resource challenges as a significant amount of energy are consumed during proactive computations of routing paths. From an operation perspective, the routing protocols can be classified into (a) negotiation-based routing protocols, where the routing protocol preserve the energy by reducing the data redundancy during communication, (b) query-based routing protocols where the sink node broadcasts queries regarding the nodes sensing task and the associated sensing node uses the reverse routing path to send the collected data back, (c) multipath-based routing protocols which uses deferent alternative paths to enhance the availability and security, (d) QoS-based routing protocols which benefits from controlling the congestion and satisfying the quality of service requirements such as bandwidth and delay [11], and (e) coherent-based routing protocols where the nodes perform minimum data processing and the data is sent to the upper levels for more processing [12] [13] [14] [7]. Figure 1 shows the routing protocols classifications in MWSNs.

III. State-of-the-art MWSN Routing protocols

In this section, well known state-of-the-art MWSN routing protocols and their enhanced variants are discussed. The section focuses on the functionality and the security mechanism of the routing protocols that are suitable for MWSN.

A. LEACH Family

Low-energy adaptive clustering hierarchy (LEACH) routing protocol is one of the most popular hierarchically clustered routing protocols for WSNs [7]. The protocol is designed for distributed networks and does not require global network knowledge. LEACH is considered Time-division multiple access (TDMA) which allows transmission over the same channel with different time slot per transmitter. LEACH offers low energy consumption by allowing nodes to use minimal transmission power to reach cluster heads by activating their transceivers during scheduled time slots only. In LEACH, data transmission is divided into fixed time intervals or rounds. There are two phases in each round, which are the setup phase and the steady-state phase. During the setup phase, cluster heads will be chosen with an equal probability based on the nodes' signal strength and residual energy. If the node became a cluster head, it cannot become a cluster head again until all nodes have been chosen. Also, multi-hop communications are established between the cluster heads and the base station during the setup phase. During the steady-state phase, data is collected from cluster members by the cluster heads in communication called intra-cluster transmission. After that, the aggregated data will be comprised and forwarded to the base station in communication called the inter-cluster transmission. LEACH protocol is very efficient in extending the lifetime of the static nodes in WSN however, its efficiency degrades for large mobile networks which triggered the design of LEACH variants such as TLEACH, LEACH-mobile, and LEACH-mobile-enhanced [7]. LEACH has some limitations such as random and uneven cluster heads distribution all over the network and the selection process considers only remaining energy for selecting cluster heads. There are situations when one-hop communication between cluster heads and the base station is not energy efficient. The inefficient randomization process of the cluster head formations is another limitation of LEACH [15].

Because LEACH protocol does not account for the movement of the nodes after each round, there will be serious data loss in MWSN where nodes are frequently moving. LEACH-mobile was proposed by Kim and Chung to solve the nodes' mobility issues [16]. Unlike in the LEACH protocol where nodes will be communicating with their cluster heads, LEACH–mobile solve the communication by allowing the nodes that cannot connect to their cluster heads during two consecutive TDMA schedules to request joint another cluster head by broadcasting cluster head joint request. The approach enhances the connectivity of mobile nodes moving outside the radio range of their cluster heads [17] [7] [18]. LEACH-mobile assumes that cluster heads are stationary and therefore mobile cluster heads may cause some data loss. To overcome this issue, Kumar et al. proposed an enhancement to the LEACH-mobile protocol [19] called LEACH-mobile-enhanced (LEACH-ME). LEACH-ME considers the mobility factor in the cluster heads' selection process.

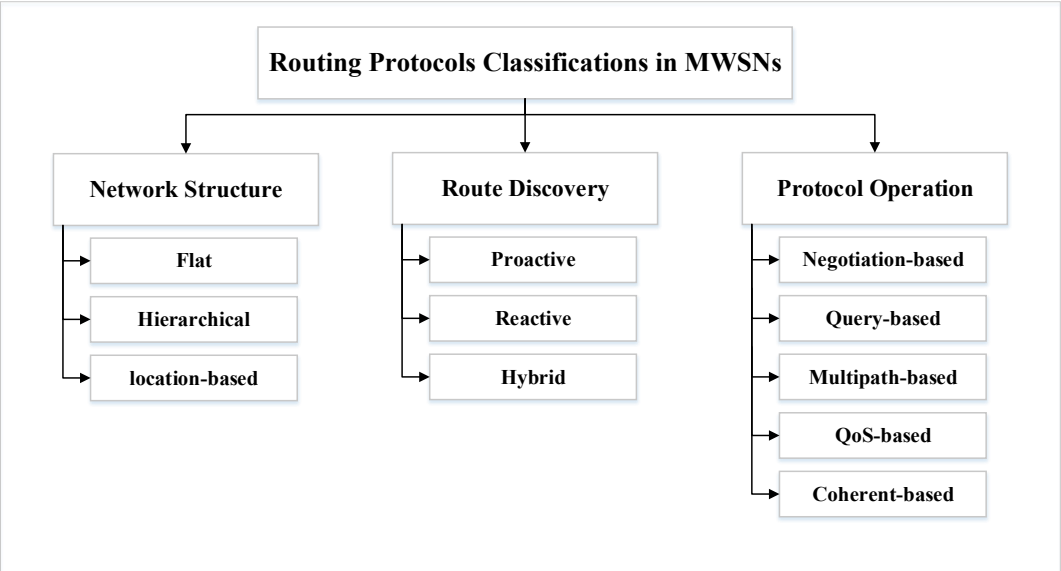

Fig. 1. Classification of routing protocols.

The mobility factor is calculated in each time frame, based on the velocity of the node and the amount of time the node takes to move between two locations. Although LEACH-ME is more reliable for MWSNs, the calculation of the mobility factor for each node in each frame consumes a significant amount of energy [18].

TLEACH was proposed by Qi and Min to address the mobility of all nodes in MWSNs. The protocol enhances the power consumption and packets delivery rate by using tree-based routing, power control, and multi-hop transmission. Due to the enhancements the protocol provides, it can handle large MWSNs and uneven distributed mobile nodes [20].

TLEACH consists of two phases, which are the topology construction and the topology maintenance stages. In the topology construction phase, a data aggregation tree is constructed as well as the cluster structure and multi-hop mechanism. In the topology maintenance phase, the network is maintained based on multi-hop transmission, mobility reactions of the nodes, and mobile cluster reactions. In comparison with LEACH and LEACH-mobile [20], TLEACH was observed to provide more effectively established and maintenance of the topological structure of large and uneven mobile network in terms of energy consumption and delivery rate [7].

"Optimizing LEACH protocol" was introduced by Mottaghi and Zahabi Based on LEACH and influenced by the mobile sink and rendezvous points. The protocol follows the same LEACH structure with modification to include a rendezvous node schedule for collecting data [21].

B. Mobile Sink-Based Routing Protocol (MSRP)

In MWSN, nodes near the base station are required to forward significantly more traffic than the rest of the nodes and therefore consume more energy and die sooner. This creates hotspots in the network. Several protocols have addressed this issue such as MSRP. MSRP is a hierarchically clustered protocol that was designed to address the problem of hotspot or energy holes that form near the base station and therefore prolong the lifetime of the network. MSRP is based on a moving sink approach that collects the data from the cluster heads. The movement of the sink is related to the residual energy of the cluster head where the sink will move toward the cluster head with the higher energy to keep the nodes near sink connected as long as possible. The protocol has two phases which are the setup phase and steady-state phase. In the setup phase, the cluster heads are selected and the sink advertised its location. The sink then broadcast Time-division multiple access (TDMA) schedule to the cluster heads during the steady-state phase. Once the sink collects the information from a cluster head, it moves to the next cluster head with the highest remaining energy [22] [18].

C. Ad Hoc On-Demand Distance Vector (AODV)

MWSN inherits routing protocols from MANETs and WSN. In most cases, MANET protocols are much efficient than WSN for mobility. AODV is one of the MANET routing protocols, which are design for both wireless and mobile communication scenarios. AODV is an on-demand protocol that builds routing paths only if demanded by the communication parties in the network. Because AODV creates routes on demand and these routes will be kept as long as needed, the need for RREQ and RREP communications are reduced to the minimum, which helps in reducing the consumption of energy, and allowing nodes to enter power-saving modes. To ensure route information freshness, AODV utilizes sequence numbers. When a node requests a routing to a destination, the node will broadcast the request to its neighbours. Neighbour nodes will forward the message and will create temporary routes to the requester node. The requester node will receive back the route to the destination and will keep the route with the least number of hops. All routing entries produced from the route request will be purged when not required. Multicast in AODV will benefit from the same routes caches processes, QoS, address aggregation, and auto-configuration. AODV is shaped from the Destination-Sequenced Distance-Vector (DSDV) routing protocol with on-demand consideration. Although DSDV is considered an effective protocol given that all the nodes in the network involved in all changes, DSDV requires massive numbers of broadcast updates and therefor will consume more traffic and more energy resources. Unlike DSDV, AODV broadcasts are minimal. When a link between nodes breaks, only involved nodes will communicate where in DSDV, this event requires routing broadcast to all nodes [23] [24].

D. Dynamic Source Routing (DSR)

DSR is one of the purest on-demand routing protocol where any communication is only triggered by node request. DSR uses source routing where the routed packets will contain the address of all nodes in the path for the destination. For mobile nodes, the packet routing information will be updated at each node. For long paths or large sets of addresses, there will be high overhead since the packets have to carry the information related to the full path.

DSR contains two main mechanisms which are route discovery and route maintenance. During the route discovery, multiple paths will be generated toward the same destination. During the route maintenance phase, the protocol is unable to locally repair broken paths. While DSR is a simple and efficient protocol, it is designed originally for MANETs and has a limited efficiency when it is used for a large number of nodes in MWSN [23] [25].

E. Artificial Bee Colony (ABC) Based Routing Protocol

ABC algorithm was proposed by Karaboga and Basturk [26] for the optimization of the numerical functions. The algorithm is based on swarm intelligence and benefits from the bee colonies' studies. ABC divide the bees into three groups, which are employed bees, onlookers, and scouts. The onlooker bees are the bees waiting to make a decision regarding the food source. The employed bee is the bee that is going to the food source, which has been visited by the same bee before. A scout bee is a bee carrying random searches. The ABC algorithm colony consists of two halves. The first half contains the employed bees and the second half contains the onlooker bees. There is only one food source per bee. When the bee's food source is exhausted, the bee becomes a scout [26] [7] [18].

The ABC algorithm was used to enhance routing in WSNs and MWSNs by researchers. Yue et al. proposed an optimized-ABC-based algorithm for data collection in large-scale MWSNs. They based the optimization on choosing the optimal path for the sink node movement, the cluster heads, and the routing shortest paths in order to collect information from nodes [27].

F. Mobility adaptive cross-layer routing (MACRO)

Cakici et al. proposed a routing protocol to overcome the existing packet delay, energy consumption, and end-to-end reliability issues in mobile sensor networks. The protocol is based on the interaction of the five reference layers, which are physical, media access, network, transport, and application layers. The proposed protocol accounts for the available routing path as well as the routing reliability, which is affected by topology changes. Channel conditions such as congestions and failures of the nodes are adapted to preserve the reliability while adapting to the possible topologies' changes. MACRO protocol consists of route discovery, route management, and data forwarding algorithms. In large MWSNs with frequent topology changes, the route discovery process may cause large packet delay [28]. MACRO is proven to provide better packet delivery ratio and lower end-to-end delay when benchmarked against LEACH-mobile and the cluster-based cross-layer routing protocol (CBR-mobile) [29] [7].

G. Energy Management with Multiple Sinks (EMMS)

In many WSN routing protocols, the routing protocol is based on single sink deployment. EMMS proposed by Shi et al. to benefits from multiple mobile sink nodes to prolong the network lifetime by reducing the energy consumption [30]. The proposed protocol addresses the challenge of managing the movement of the mobile sink nodes to balance the sensors' data collection workload among the different sinks. The movement of the sink is a closed tour of trajectory roads in the network area. The proposed algorithm consists of two stages, which are finding a close tour as the first stage and determining the sojourn locations of the mobile sink in the second stage. In the first stage, the algorithm will find a close tour with almost equal length for each sink. In the second stage, the algorithm will determine sojourn locations and build the routing tree for each location and for each sink considering the sink stopover time in each location for collecting the data from nodes. EMMS improves the residual energy utilization as well as the transmission quality for MWSNs [30] [7] [18].

H. Mobility-Based Clustering (MBC) Protocol

MBC protocol was proposed by Deng et al. to address the mobility and other performance issues in MWSN [31]. Similar to LEACH, MBC is a hierarchal-based cluster protocol. The nodes will be elected as cluster heads based on the residual energy and the mobility with equal probability for each node to be a cluster head. The operation of the protocol is divided into two stages, which are the setup stage and the steady-state stage in each round. In the setup stage, cluster heads will be selected with consideration to the connection time between the nodes in a cluster and their cluster head for more reliable and stable routing paths. In the steady-state stage, the data transfer to the cluster head in intra-cluster communication and from the cluster head to the sink in inter-cluster communication in each round. While the operations of MBC and LEACH are similar, MBC provides more stability and better performance in mobile-based applications because LEACH is not effective in large mobile networks. However, MBC may face some issues related to packet dropping, link breakage, and reduced network utilization due to its failure to address the problem of critical node occurrence [7] [18].

I. Cluster-Based Routing Protocol for MWSN (CBR–MWSN)

CBR-MWSN is a cluster-based routing protocol that was proposed by Awwad et al. to address the mobility of nodes and energy consumption [29]. CBR-MWSN is round free and uses the adaptive Time Division Multiple Access (TDMA) approach. In CBR-MWSN the cluster head will collect the data from its member nodes as well as other nodes that lost their connection to their allocated cluster heads and just entered its radio range, subject to the availability of free time slot in its schedule. Cluster heads take a turn to be free and they adaptively change their TDMA schedule according to the mobility and traffic. The simulation result of CBR-MWSN showed a reduction in the data packet loss by 25% comparing to LEACH-mobile. However, CBR-MWSN will consume more energy due to the operational overhead compared to LEACH-mobile [29] [18].

J. Power-Efficient Gathering in Sensor Information Systems (PEGASIS) & Mobile Sink Improved Energy-Efficient PEGASIS-Based Routing Protocol (MIEEPB)

PEGASIS was proposed by Lindsey and Raghavendra to prolong the lifetime of the network [32]. PEGASIS developers were influenced by the LEACH protocol. PEGASIS use chain-based communication to distribute the workload of transmitting to the base station among the sensor nodes. Similar to the idea of cluster heads in LEACH, neighbor nodes in PEGASIS will form groups between them and will take a turn to send the collected data from the group. Only one node from the group will communicate with the base station at each round. The assumption given in the PEGASIS proposal is that the base station is located far away from all nodes and it has a fixed location. During the simulation, PEGASIS showed improvement from 100% to 300% in prolonging the lifetime of the network over LEACH [32] [33]. Although PEGASIS enhances the power consumption, the protocol does not account for the mobility of nodes and the mobility of the base station, with the performance improvement is limited to the assumption of the base station being located far away from nodes.

An enhancement to the PEGASIS was proposed by Jafri et al. to account for the mobility and to provide efficiency of power consumption in MWSNs. The proposed protocol called Mobile Sink Improved Energy-Efficient PEGASIS-Based Routing Protocol (MIEEPB). In MIEEPB, the field will be divided into four zones and smaller chains will be formed at each zone. The leader node of each chain will be selected by accounting for the distance from the sink and the residual energy. The mobile sink will make scheduled stopovers to each zone to ensure data collection and reduce power consumption needed to transmit the data [33] [18].

K. Other State-of-the-Art Routing Protocols

In the previous list of routing protocols, the discussion focused on well-known and most researched protocols with different approaches. In addition, there are many other protocols that are influenced by these well-known state-of-the-art protocols and some of them will be briefly discussed below.

Velmani and Kaarthick proposed two routing protocols with the purpose of improving network efficiency and reducing power consumption. The protocols are Velocity Energy-efficient and Link-aware Cluster-Tree (VELCT) [34] and Cluster Independent Data Collection tree (CIDT) [35].

Enhanced Cluster-Based Routing Protocol (ECBR-MWSN) was proposed by Anitha and Kamalakkannan based on the influence of both CBR-Mobile and LEACH-Mobile [36]. The proposed protocol uses five stages including re-clustering and rerouting phases. The selection of cluster heads is based on three factors, which are residual energy, mobility, distance from the base station [18].

Proactive Highly Ambulatory Sensor Routing (PHASeR) was proposed by Hayes and Ali for MWSNs. The PHASeR protocol uses global Time-division multiple access in the Medium access control (TDMA-MAC) layer to assign time slots for each node [37].

Ring Routing Protocol was proposed by Tunca et al. with consideration for the energy consumption and network lifetime. The ring protocol consists of forming a virtual ring with an anchor node that is close to the mobile sink to collect the data. The virtual rings change while the mobile sink moves to cover all nodes in the network [38].

Anycast Tree-Based Routing Protocol is another protocol that was designed to reduce energy consumption and minimize traffic. The protocol is part of reactive routing protocols with maintaining the routing information. It is based on unicast messaging and the expansion of ring search in mobile multiple sink nodes [39].

Fuzzy logic, swarm logic, genetic algorithms, and solving nondeterministic Polynomial optimization problems was used to find the optimal solution for the relation of the energy consumption, number of nodes, and lifetime of the network. Genetic Algorithm Based Routing Protocol (GAROUTE) was one of these optimization efforts [40]. Another algorithm is Clustering Algorithm Based on Glowworm Swarm Optimization (CAGM) which was developed by Wang et al. which divides the network to clusters based on the glowworm swarm optimization algorithm [41].

Many other enhanced routing protocols were proposed for optimizing the energy consumption, network reliability, and prolonging the lifetime of the network. All the aforementioned routing protocols did not consider any security measures to protect the routed data or to protect routing functionality from attackers.

IV. Security Requirements in MWSN

MWSN shares many characteristics with the typical computer networks but also has unique security requirements with regards to the nature of the network. The main MWSN security requirements are [13]:

- Confidentiality: in the MWSN, the data should be protected from unauthorized access. The key distribution methods should be secured and certain public information including node identity and public keys should be kept safe from being exposed to unauthorized access [42].
- Integrity: Because MWSNs could be deployed in hostile or outdoor environments, the data collected, processed, or transferred should be protected from manipulations. The integrity of the data is a core requirement of sensor networks. In MWSN, most sensor nodes operate on limited power sources where the recharging may not be an option. Because integrity requires security operations that could heavily affect the limited resources of the sensor nodes, lightweight algorithms are required [43] [44].
- Availability: The availability and reliability of the network are critical to the operation of MWSNs. System failures can lead to serious consequences such as economic losses, environmental damages, or even put humans at risk. The main sources of impact on system availability are security attacks, software and hardware failures, and the lack of structured approaches. The MWSN functionalities should be available even during attacks or faults by implementing redundancy, attack prevention and mitigation, and failure control [45].
- Authentication: Authentication is the process of identifying the source node in MWSN communications and verifying its assumed identity. Because of the

broadcasting nature of the MWSN, verifying the source entities is always a challenge. The authentication can be accomplished by using Message Authentication Code MAC for the communications between nodes. Because sensor nodes in most cases are limited in resources and because authentication operations require high resource consumption, authenticating all income traffic in a network with broadcasting nature is not possible and, in some cases, intentionally ignored to preserve nodes energy. Malicious nodes can create a massive number of packets, disturb the routing functionality, direct the traffic toward itself, and create a denial of service attacks (DoS). Some lightweight authentication algorithms were proposed by researchers such as the Biphase authentication scheme, which offers small-scale authentication and provides resistance against DoS attacks [46].

- Data freshness: The data freshness in MWSN should be ensured by making sure that data is recent, and no old data is being replaced by malicious nodes. Adversaries can carry replay attacks when shared keys are being used in the MWSN. There are two main methods to achieve the data freshness requirement which are: (a) Data Dynamicity where the sequence of data is used by frames but only disclosed to the intended destination. And (b) Delay Tolerance and independent Processing where each packet is verified individually [47].
- Secure localization: The location of the sensed event is crucial information in the setting of sensor networks. The location of events could determine the action required such as in sensing fire hazards. The location information can support functionalities such as geographical routing. The adversary can provide incorrect location information using false localization properties such as signal strength or by replaying packets. Attacks such as Replay, Sybil, and Wormhole attacks could target the localization in MWSN. There are many proposed schemes to protect against localization attacks. A proposed secure localization scheme is proposed by Lazos & Poovendran [48] which is called SeRLoc. SeRLoc is a range-independent and decentralized localization scheme designed for resource-constrained untrusted environments such as MWSN [49].
- Nodes self-organization: With the demand for flexibility and less human intervention and maintenance, required self-organization and self-healing is an essential feature of MWSN. Nodes are deployed without the prior knowledge of each other, but they are required to communicate and exchange data between themselves. Deploying nodes with pre-configured shared keys is not possible in many MWSN applications due to the dynamic nature of the network. Symmetric key pre-distribution schemes were proposed by researchers such as [50] where the researchers used random key distribution based on random graph giant component theories. Moreover, the use of public keys in an efficient manner is essential. Nodes' self-organization should include trust relation, key management, and routing information [51].
- Time synchronization: Time synchronization is a critical requirement in MWSN applications, as well as for security operations. Malicious attacks could break time synchronization by manipulating messages. To ensure network reliability, manipulation attacks should be detected and prevented. In [52] the researchers proposed the "Maximum Consensus-Based Approach" to detect and invalidate malicious manipulation messages. A study by [53] proposed a toolbox of protocols to protect both the nodes within the power range and the nodes, which are multiple hops away.
- Survivability and Self-stabilization: Nodes should have the ability to recover from security incidents independently and without the need for intervention. The node should also survive through the incident and complete the intended tasks even in case of other failures affect the network [54].
- Isolation: Nodes should have the ability to isolate themselves from other malicious nodes in the network and they should have the ability to detect abnormal behaviour of other nodes. Lightweight cryptographic schemes and trust management should help in isolating malicious nodes as discussed in [54].

In their survey, Riaz et al. classified the security aspects of the WSN networks into primary and secondary goals. The primary goal includes confidentiality, integrity, authorization, availability, and access control. Their classification of the secondary goals includes data freshness, route freshness, Self-Organization, Secure Localization, Time Synchronization, and Power Management [55]. Route freshness is the ability to be flexible with the changes of network topology and to ensure the freshness of the routing table data. Attackers may deploy malicious nodes impersonating legitimate nodes and manipulate routing tables. Power management indicates the ability to manage the limited power source of the nodes which can be affected by the attackers. An attack can drain the power source and result in a denial of the service. Such an attack can be carried by forcing critical nodes to participate in unnecessary operations such as routing updates or unnecessary processing.

V. Security Challenges in MWSN

MWSNs are required to be reliable, dependable, available, and the data should be accessed only with proper authorization. Many factors play a major role in increasing the vulnerability of the network and its components. The mobility of the nodes contributes to introducing challenges to the security of MWSN. Mobile nodes have influence over the topology of the network as well as introducing new challenges related to the ability of nodes to change location or position. Mobility also adds more challenges related to the Medium Access Control (MAC) protocols compared to the stationary nodes in WSN. MAC protocols are essential for managing throughput, mobility, security, energy, and protection against collisions [56] [57]. Another factor is the nature of the deployment environment. In most applications on MWSN, nodes are being deployed in unattended environments, hostile environments, or environments with bad conditions where reliability, self-healing, and self-configuration of nodes are challenged. The relationship between nodes such as nodes heterogeneity can also affect network vulnerability [58]. In their Survey on WSN

security attacks and challenges, Riaz et al. listed the WSN challenges that increase the vulnerability of the network as [55]:

- Wireless Medium: MWSNs use wireless communication and wireless broadcasting which increase the accessibility of the attackers and passive eavesdropper.
- Ad-Hoc deployment: Self-healing and self-organizing nodes is an essential feature of a reliable network. This adds to the overhead of the system when the adversary deploys malicious nodes that replace legitimate failed nodes.
- Environment hostility: Attackers may gain physical access to the nodes deployed in hostile or unattended environments. Physical access to nodes may allow access to information and security keys.
- Resource constraints: In most of the applications of the MWSN, the nodes are limited in terms of resources. Security operations demand a high consumption of energy, memory, bandwidth, and processor. Security operations are required to be efficient to preserve nodes and network resources.
- Network Scalability: MWSN can include a huge number of nodes. Securing huge networks requires proper design, proper implementation, and efficient security operations with as little effect as possible on the network resources

VI. MWSN Security Threats and Attacks

According to Jawandhiya et al. [59] security attacks can be classified based on the attacker location as external or internal. In the external attack, the attacker's objective is to disturb the services of the MWSN by targeting availability. On the other hand, the internal attacker's objective is to gain access and target confidentiality and integrity. The internal attacker may use compromised nodes to lunch malicious attacks.

Security attacks can be classified based on the attacker's goals into passive and active attacks. In the passive attacks, the attacker passively monitors the traffic and try to gain access to privileged information. During the passive attack, the attacker avoids detection and does not disturb the network services. Passive attacks may include eavesdropping, traffic analysis, capturing communications, and decryption of encrypted information. On the other hand, active attacks' goal is to take actions against the targeted network by upsetting the services, modifying data, lunching malicious attacks, or gaining control of resources. Most of the active attacks start passive to study the network vulnerabilities and to design the active attack plan [59] [55] [58].

In addition, Yang et al. classified the attacks based on the intention of the attacker as node compromise attacks, repudiation attacks, packet-oriented attacks, protocol-oriented attacks, and denial of service (DoS) attacks which is the hardest to detect, complicated, and destructive [54] [60].

Security attacks in WSN target different layers in the Open Systems Interconnection (OSI) model. For example, the physical layer can be affected by jamming and tampering attacks. The link-layer can be compromised by Collision, Exhaustion, and Unfairness attacks. Attacks on network and routing layer are Neglect and greed, Homing, Misdirection, and Blackholes. The transport layer can be targeted by Flooding and Desynchronization attacks [61].

Sen [13] defined three main categories for the attacks on MWSN based on its target: Attacks on the availability of the network, attacks on privacy and authentication, and the attacks on the integrity of the system. First, attacks on the availability aim to disrupt or parallelize the network and are referred to as DoS attacks. DoS attacks can introduce real-world danger on critical applications such as attacks on health sensors attached to the human body. Second, attacks on privacy and authorization include modification, message replay, spoofing, and eavesdropping. The attacks aim to access privileged information without proper authorization. Using cryptographic methods can protect against these attacks. Finally, the attacks on the integrity aim to falsify data by injecting false data into network nodes.

A. Passive attacks

Passive attacks are designed to be stealthy to achieve the goals of reconnaissance or obtaining confidential information. These attacks usually carried in the form of eavesdropping or traffic monitoring and analysis [59] [62] [58] [55].

- Eavesdropping: the attacker intercepts the wireless connection by conducting overhearing attempts to the MWSN and tries to gain sensitive information such as passwords, cryptographic keys, or unprotected clear text communications. The eavesdropper tries to detect the content of the communication. The eavesdropping activity is usually the initial behaviour of active attacks such as Blackhole and wormhole.
- Traffic monitoring and analysis: The attacker monitors and captures the transmitted packets in the wireless network. Analysis of the captured packets may leak the source and destination addresses and may also give the attacker insight into the structure of the network.
- The homing attack is one of the attacks related to traffic monitoring and analysis. In the Homing Attack, the attacker monitors the traffic and analyses it to determine the critical nodes in the network such as sink or cluster head nodes. The homing attack is used in advance of launching active attacks on critical nodes. Because the attacker studies the traffic and finds the critical node, implementing a prevention method by sending “dummy packets”, which will help in ruining the attacker's findings [54].

B. Active attacks

In the active attacks, the attacker attempts to inflect changes to the data, operations, or availability of the network. The attacker may use the network resources to accomplish the goal of the attack such as replaying old messages, broadcasting false information, or attracting routed packets to malicious nodes. The active attacker may use different types of attacks to disable the operation of the network such as in the denial of service attacks.

DoS attacks family contains various types of attacks with the main purpose of disturbing the entire network or at least a critical part of it. In mobile networks, more types of DoS attacks are available because of the nature of the mobility of network components and the wireless transmission medium. Various types of DoS attacks are discussed in this section.

Kahina Chelli [58] classified active security attacks in WSN as Blackhole, Replay, Sinkhole, spoofing, flooding, jamming, Sybil, overwhelming, wormhole, DoS, fabrication, hello flood, node subversion, man in the middle, selective forwarding, and false node attacks.

Mobile wireless sensor networks and mobile ad-hoc networks MANETs have different properties such as the focus of interaction of the network where MWSN focuses on gathering information from the environment whereas MANET focuses on computational distribution. But MWSNs are much larger, nodes are less equipped, and communication is mostly broadcasted. Despite their differences, they share the security weaknesses and most of the types of attacks because of some unique similarities between both networks [63]. In their survey of MANET attacks, Jawandhiya et al. listed the most known active attacks on MANET as: Jamming attack, Wormhole attack, Blackhole attack, Byzantine attack, Routing Attacks (Routing Table Overflow, Routing Table Poisoning, Packet Replication, Route Cache Poisoning, Rushing Attack), Resource consumption attack, IP Spoofing attack, State Pollution attack, Sybil attack, Fabrication, Modification, Session Hijacking attack, SYN Flooding attack, Repudiation attack, Denial of Service attack, Location disclosure attack, Flooding attack, Impersonation or Spoofing attack, Colluding misrelay attack, Device tampering attack, Grayhole attack, Link spoofing attack, Neighbour attack, Jellyfish attack, Packet dropping attacks, and Sleep deprivation torture.

Yang et al. studied underwater mobile wireless sensors networks (UWSN) security challenges and attacks. UWSNs shares the same attack types with their parent network WSN. In their research, the attacks listed were: Jamming, Collision, Exhaustion, Denial-of-Sleep, Unfairness, Replay, Selective Forwarding, Neglect and Greed, Misdirection, Blackhole/Grayhole, Sinkhole, Wormhole, Sybil, Hello Flooding, Homing, Desynchronization, and Synchronization Flooding Attacks. The following sections discuss, the most known active attacks presented in [59] [13] [64] [58] [55] [54]:

1) Jamming attacks

The jamming attack is considered a physical layer attack. It generates radio interference with other nodes' signal in the MWSNs. Jamming can be done by overwhelming the radio frequency with useless communication which prevents the nodes in MWSN from communicating. Jamming devices can be distributed throughout the network to cripple the whole network communications. Jamming is considered also a DoS attack and can be temporary, intermittent, or continuous. Intermittent jamming attacks can cripple the network similar to the continuous attacks if the network is using time-critical synchronization. Also, targeting critical nodes such as cluster heads, root nodes, or sink node can cripple the entire network. Because of the hostile and unattended nature of MWSN, the jamming attacks are very hard to prevent [65] [13] [54].

Preventing jamming attacks maybe impossible giving that the signal at the physical layer is affected. Del-Valle-Soto et al. proposed two jamming attacks detection methods. The first method depends on sharing performance metrics between neighbour nodes. The second method proposed dividing the network into zones with an information collector node for each zone to compare the collected information with the performance metrics. When a zone is detected, the zone is marked and isolated [66]. The second method requires dedicated nodes to be used as a collector with higher specification and power source than the rest of the nodes to be able to cope with the assigned tasks. This approach introduces more burdens on the MWSNs deployment.

2) Tampering attack

Tampering attack is another example of a physical layer attack. The nature of MWSNs environment is usually hostile, unattended, and distributed. Also, the sensor devices are small in size and are most of the time portable and located outdoor. These features allow attackers to physically access, damage, modify or steal the sensor devices. By physically accessing the sensor devices, the attacker can inject malicious codes or programs, capture the cryptographic keys, and replace sensors. Protection methods typically include physically securing the devices and enhancing cryptographic features of the node to prevent data and keys capture [65] [13] [54].

Protecting against tampering attacks is not trivial and involves many layer protection techniques starting with securing the device from being damaged or stolen to the protection of the devices' information from being revealed. The mobility of the sensor nodes in MWSN adds other challenges comparing to the stationary networks. In their study, Tallez et al. investigated the bootstrap loader brute force attacks on the MSP430 microcontroller units. They found that the attacker could gain passwords in a matter of days and later gain sensitive information about WSN cryptographic keys. They proposed a randomizing method to secure the bootstrap password to protect against reverse engineering the units. In their proposal, they found this method succeeded to increase the difficulty of brute force attacks by increasing the time needed to complete the brute force attack from few days to a matter of decades [67].

3) Wormhole attack

Wormhole attack is considered a network layer attack. The attacker establishes a connection between two portions of the network mostly between two different malicious nodes to connect two parts of the network by creating a wormhole tunnel. The packets captured in one end of the tunnel will be broadcasted to the other end. Wormhole attack can be devastating, hard to detect and not easy to prevent because the attacker can begin the attack without the need to compromise nodes or breakthrough cryptographic defenses. The success rate of the attack is increased if the nodes are a long distance from each other and the tunnel connection is faster and at lower latency than the normal route, which attracts the nodes to use the malicious fast route. The tunnel may use a fast wired or radio-frequency connection between the malicious nodes. The tunnel attracts the packet forwarding and disrupts the normal routing functionalities of the network. Because of the wireless nature of the network and the mobility of the nodes, the attacker is able to capture the packets from one end and send it to another end even if the packets are not routed through the malicious tunnel [65] [13] [54].

Wormhole detection and prevention research has attracted many researchers because of the challenges and the severe effect on the network. Adarkar et al. proposed a detection and prevention method for the wormhole attack using the "packet leach" mechanism. The leaches are information that attaches to the packets containing information about the allowed transmission distance. The proposed method consists of two

types of leaches, geographical and temporal. Geographical leaches depend on the location of the nodes and can use a loosely synchronized clock between the nodes. On the other hand, the temporal leaches depend on the exact time and require the nodes to be tightly synchronized. The proposed solution introduced a protocol "TIK" to achieve instant authentication to prevent wormhole attacks [68].

In addition, Harsányi et al. proposed a new wormhole detection method using spanning trees. Their method depends only on network connectivity information and does not require additional measurements. Their proposed solution depends on the feature of the Wormhole of providing faster and shorter routes. Based on this assumption, the removal of a wormhole will severely affect the shortest path used by nodes close to the wormhole in the network while other nodes' shortest route will remain. Running iterative searches for the changed routes from different nodes will provide information about the affected nodes and Wormhole details [69].

4) Blackhole and Grayhole attacks

The Blackhole attack is classified as a network layer attack. In the Blackhole attack, the attacker will compromise a node or deploy a malicious node to the network. The malicious node will forge and send routing information during the route update or route pathfinding to all nodes falsely pretending to be the shortest and less cost path to destinations. The malicious node then may drop all packets or can selectively forward part of the packets. The Blackhole can be used as a DoS attack when the attacker drops all packets. If the attacker deliberately doped the packets in an intermittent way, the attack will be much harder to detect. This type of Blackhole attack is called a Grayhole attack and is more sophisticated. While the Blackhole attack is part of the DoS attacks, a Grayhole attack is considered part of selective forwarding attacks [65] [13] [54].

Deepak et al. proposed a detection and prevention method for Blackhole and Grayhole attacks using trust-based routing. The proposed solution is based on minimizing the probability of nodes to select the malicious nodes as the best route forwarding option by using trusted route-finding algorithms and elliptic curve cryptography (ECC) for securing data. The encrypted data is verified by the two-stage security mechanism in each node. The routing path is secured by trust route-finding and by sending detection packets through routing paths [70]. While the proposed solution shows promising protection levels, the resource consumption by the encryption, verification, and used searching methods tend to drain the limited resources.

Aslam Khan et al. proposed a solution based on two stages for detecting and prevention for Blackhole attacks. They applied the proposed solution to the Low-energy adaptive clustering hierarchy LEACH protocol. The detection is carried offline during the cluster head setup time. The detection phase depends on the pre-installed agent on the sensor nodes. The agent will listen to the advertising cluster head messages, classified them, and update the cluster head lists. The other stage is the prevention, which is carried during the LEACH protocol setup. The nodes will query the malicious lists created during the detection phase and drop the advertised cluster head request if the node is suspected to be malicious. During the simulation of Blackhole attacks, they found the accuracy of detection is very high with few false positives comparing to the anomaly detection techniques [71]. While the detection accuracy is high, the system has significant requirements to work such as the need for a pre-installed agent, malicious and audit list, and units to perform different tasks. The requirements of the system can significantly affect the performance and resources of the system.

5) Sinkhole Attack

Sinkhole attack is part of network layer attacks. The Sinkhole attacks can be considered a special type of Blackhole attack, which is designed to target the sink node. In the Sinkhole attack, the attacker inserts a malicious node or compromises one of the existing nodes of the network. The compromised node will advertise a fast route to the base station to all neighbour nodes by using forged routing information. Neighbour nodes will choose the compromised node as the preferred routing path to the base station. The scale of the attack depends on the proximity of the compromised node to the sink node. If the compromised node is very close to the sink node, the attacker could attract all the traffic or a large portion of the network traffic, which will be forwarded through the compromised node. The attack will result in granting the attacker control over the captured traffic [13] [55] [54].

A detection method based on hop counts was proposed by Abdulla et al. [72]. The proposed solution applies to stationary nodes with a fixed distance from the base station. The proposed method requires the base station to send a HELLO message containing hop count information. The message will travel from the base toward the more distant node in the network and adding hop counts. Each node then will have a short and long path to the base station. Any advertised route that does not fall into the normal threshold of the route hop count will be considered suspicious. While this proposed solution seems promising in detecting and preventing Sinkhole attacks, the solution can be applied only on stationary node structure with a fixed distance to the base station. With the mobility requirement of MWSN, this solution cannot work without proper enhancement.

6) Byzantine attack

The byzantine attack is related to the network layer. The attack is taking the name from the "Byzantine Generals Problem" where Byzantine generals need to communicate and reach an agreement about a battle plan, but one or more generals are traitors. The problem is used to study the reliability of the computer system in the presence of malfunctioning components [73].

The Byzantine attack involves one or more compromised nodes working in a complicit way to carry-on different type of attacks such as forwarding packets through non-optimal routes, creating routing loops, or selectively drops packets thus degrading the performance of the network, disruption the network routing services, and draining the resources of the network component. The Byzantine attack is not easy to detect because the network does not demonstrate detectable abnormal activities [74] [59] [13] [55].

Anusuya et al. proposed a detection method called "Enhancement cooperative bait detection scheme" for byzantine attack based on sending bait message with a destination address of the neighbour node to lure the malicious node to send RREP messages. The malicious nodes are detected using reverse tracing and then added to the malicious nodes list, which is sent to the nodes participating in the routing of the bait message [75].

7) Routing Attacks

Routing attacks carried through the network layer and targets the routing functionality of the network. There are several types of routing attacks such as Routing Table

Poisoning, Route Cache Poisoning, Routing Table Overflow, Packet replication, and Rushing attacks [59] [13] [55] [54].

Routing Table Poisoning: Malicious nodes in the network attempt to send fake routing updates or change the legitimate routing information in the packets. The attack aims to create network congestion, performance degradation, or major disruption of routing services.

Route Cache Poisoning: While proactive routing protocols rely on the routing tables, reactive routing protocols utilize caches to store recently discovered routes for better performance. The attacker will attempt to overwhelm the cache with fake routes to prevent the creation of new legitimate records.

Routing Table Overflow: Proactive routing protocols tend to create routing entries in advance instead of on-demand route path discovery conducted by reactive routing protocols. This advance creation allows malicious nodes to send excessive fake routing advertisements for non-existence nodes. The malicious node attempts to overwhelm the routing tables to prevent the creation of new legitimate routing entries. Because reactive routing protocols are collecting routing information on-demand bases, they are less affected by this type of attack.

Packet Replication: Malicious nodes will attempt to replicate old messages to confuse the routing functionality to consume bandwidth and power resources.

Rushing Attack: The attack is applicable to the routing protocols that use duplicate packets discard mechanism "duplicate suppression". In the attack, the malicious node, which is located in the routing path of a source node will receive a route request RREQ packets. The malicious node will send the packet quickly "Rush" to the destination node. The destination node will discard the duplicated RREQ from the source node assuming it is a duplicated packet. The source node will continue to use the same routing path including the malicious node because it is unable to discover new routes. The Rushing attack is very difficult to detect in the MWSN networks.

To protect against routing attacks, many researchers proposed enhancement to the existing on-demand routing protocols such as Dynamic Source Routing (DSR) and Ad hoc On-Demand Distance Vector (AODV). Secure routing protocols based on DSR and AODV such as Ariadne, Authenticated Routing for Ad Hoc Networks (ARAN), and Secured SAODV were proposed to fulfill the security requirements of message routing. Although when these secured routing protocols are subjected to Rushing attack, they are unable to discover routes that are more than two hops away [76].

Hu et al. [76] analysed the routing protocols under the rushing attack and proposed the Rushing Attack Prevention RAP protocol. Their proposed solution can be integrated into the secure routing protocols such as Ariadne, ARAN, SADOV. When integrated with the secure routing protocols, RAP will not consume resources unless the node is unable to find a usable route when the network is under a rushing attack. Even though they found RAP is highly effective, they also found that RAP overhead is higher than the standard route discovery protocols [76].

8) Resource consumption attack

Resource consumption attack, sleep deprivation attack [59] [55], resource depletion attack [13], [55], Denial-of-Sleep [54], or resource exhaustion attack [58] [64] all refer to same attack methodology. The attacker attempts to drain and consume the limited resources of sensor nodes. In the resource-constrained environment such as MWSN, battery life is preserved by putting the nodes in sleep or power-saving mode to preserve the battery power. The resource consumption attack will usually consume the battery life, thus taking the node out of service. The attack can be carried using unnecessary forwarded packets, route requests, beacon packets, or false requests. The attack is usually carried through the network layer in the form of route or packet requests but can be carried through the transport layer using Transmission Control Protocol (TCP) unnecessary frequent handshake. This attack could be devastating in WSN by presenting nodes to enter power-saving mode, especially in the networks that are designed and configured for infrequent communication to prolong the battery life [58] [59] [55] [13] [54].

Bhattasali et al. proposed an anomaly detection approach to detect sleep deprivation attacks. The proposed solution is based on normal predefined parameter values comparisons. The model they designed exclude malicious code and reject its communication [77].

9) Sybil attack

Sybil attack is a network layer attack. In the Sybil attack, a malicious node will assume multiple identities to conduct the intended malicious behaviour. The Sybil attack targets unfair voting, attacking routing algorithms, misleading fair resource allocation, and defeat misbehaviour detection. The attack behaves the same way regardless of attack objectives. In the attack against voting mechanism, the multiple identities assumed by one node will create multiple votes, which affect the credibility and fairness of the system. In the attack against the routing algorithms, the multiple identities of a node will create multiple routing paths through the same malicious node [13] [59] [64] [55].

Dhamodharan and Vayanaperumal [78] proposed a detection and prevention method based on a validation list. When new nodes join the network, the base station will send the HELLO message and the new node will be registered. For any new node in the network, a HELLO message and timestamp will be created representing a birth certificate for the node. The system will compare the newly registered node with the base station validation list to detect the malicious nodes. A message authentication process will be used to prevent malicious nodes from sending unicast and multicast messages.

10) Flooding attack

Flooding attacks aim to overwhelm network and nodes resources by sending a massive number of requests to create degradation or denial of the service. Flooding attacks can be carried using different types of methodologies. HELLO-flood attack is one of the network layer flood attacks. In the HELLO attack, the attacker sends a massive number of HELLO packets. The HELLO packets are used by the routing protocol to establish the network topology by discovering neighbour nodes. The attacker may use a strong signal transmitter to falsely present as shortest path route. Nodes that receive HELLO packets will attempt to reply to the sender even if the node is out

of their transmitter range. Route request (RREQ) flooding attack is also a network layer flooding attack. The attacker floods the network with a large amount of RREQ to non-existence destination. Nodes will not reply and will keep forwarding the request which will overwhelm the network and could lead to denial of service. SYN flood attack is another type of flood attack that is related to transport layer attacks. In Transmission Control Protocol TCP, the three-way handshake consists of sending SYN request, receiving SYN/ACK, and returning ACK reply. In the SYN flood attack, the attacker will send SYN requests without replying, which forces the targeted node to wait for the completed handshake communication. Sending a massive amount of SYN request will overwhelm the nodes [59] [64] [13] [64] [55].

Chen et al. proposed a detection and prevention methods for low-rate DoS attacks. They combined the measurement of correlation coefficient and Kolmogorov–Smirnov test to create a trust value for each component. The value is based on the signal produced by the low-rate DoS attack. In order to gain the trust of the system, nodes should satisfy certain evaluation conditions and predefined tolerance values. Otherwise, nodes identified as low trust [79].

11) De-synchronization Attack

De-synchronization is the interruption of an active connection between network nodes. An adversary will send forge communication with fake sequence numbers and control flags to disrupt normal communication between nodes, forcing the nodes to request retransmission of the missed packets. When the attack is timed correctly, it could prevent the nodes from communicating data and instead wasting more energy in trying to recover errors and resynchronized the transmission. De-synchronization attacks can make more damage when combined with other attacks such as wormhole, Sybil, or Replay attacks where these attacks affect the round-trip time between nodes and thus affect the time alignment

Preventing De-synchronization attacks require header or full packet authentication. There are security schemes related to authentication in MWSN such as Sensor Protocol for Information via Negotiation (SPIN), Broadcast Session Key Protocol (BROSK), and Localized Encryption and Authentication Protocol (LEAP). Riaz et al. proposed a solution for authentication based on two phases of authentication called the Biphase Authentication Scheme (BAS). The initial phase requires the new node to register to authentication nodes distributed across the network. If the node is authenticated through the authenticated node, the second phase will require the node to authenticate through the base station [46] [60] [13] [54].

12) Packet Replay Attack

The Packet Replay attack is a network layer attack where the attacker intercepts the transmitted packets from the source node, delay the packets, and send them again to the receiver node. The delay will result in receiving false location as a result of the false time and different signal strength. The attack is more serious for mobile nodes with critical location requirement. Authentication in this case, helps to protect from packet replay attacks [55] [54].

Marigowda et al. proposed a solution for the Replay attacks based on a synchronized incremental counter that is attached to the packets with each transmission. The counter increment with each delay or each hop and will be verified at the receiver side to check if the packet was exposed to the Replay attack. The synchronization solution is built within each node [80].

13) Selective Forwarding Attack

This attack is related to the network layer. During the attack, malicious or compromised node attackers will perform normal tasks and will forward packets normally for most of network but will selectively drop some packets. The main goal of the attack is to suppress or modify intended packets for specific nodes. This intended targeting makes the attack difficult to detect.

Neglect and Greed attacks are special cases of selective forwarding. In the Neglect attack, the attacker will selectively drop the packets but will still acknowledge the source node. In Greed attacks, the attacker will give priority to specific packets or its own [64] [54].

To protect from selective forwarding attack, redundancy of messages and alternative routes methods should be used. Chung and Cho proposed a multi-path routing determination algorithm based on fuzzy logic to detect selective forwarding attacks in MWSNs. They compared their solution with the multi-hop extension of Ad-hoc On-demand Distance Vector (AODV) called AOMDV and found that using the fuzzy logic saved around 10% of the energy [81].

14) Data Modification Attacks

Modification of the data or injecting false information are attacks aiming to compromise the integrity of the system. These attacks can be carried at different layers of the network and using different methods. The attacker may have physical access to the node or to the sensing area of the node. Data integrity can be compromised if the attacker injected false data into the sensor readings such as exposing a thermal sensor to false temperatures. Other types of data modification could be carried by much-sophisticated attacks targeting the data aggregation operation across the entire sensor network such as packet misrouting and impersonation attacks [59] [58] [55].

Cui et al. proposed a solution for the confidentiality and integrity of data aggregation in WSNs. Their solution uses end-to-end lightweight encryption based on Okamoto-Uchiyama homomorphic encryption algorithm and using a lightweight homomorphic message authentication code (MAC) algorithm for data integrity [82].

Figure 2 shows the different types of the security attacks in MWSN.

VII. Conclusion

With the rapid development in IoT and information technology, new challenges have arisen with regards to routing and security in MWSNs, therefore, this article presented in detail the researches carried on MWSN. It analysed the major technical challenges related to routing and security, as well as, discussed most of the existing literature works in MWSNs that aim at providing efficient routing and secure communication in MWSNs. The article reviewed well-known state-of-art routing protocols that are suitable for MWSNs and discussed their functioning and security mechanism. In addition, we reviewed most security threats that targets WSNs, and the proposed solutions for these threats in the literature.

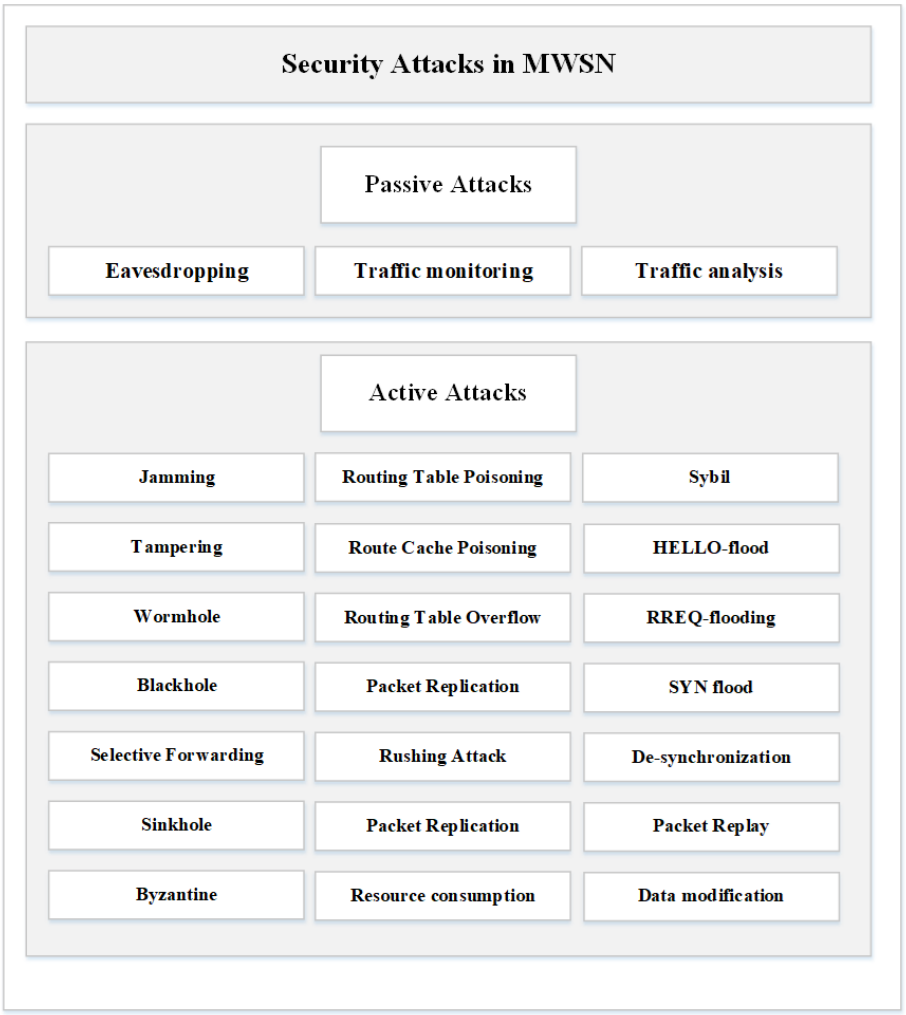

Fig. 2. Classifications of security attacks.

REFERENCES

[1] A. Forster, Introduction to wireless sensor networks, John Wiley & Sons, 2016.

[2] A. Dahane and N.-E. Berrached, Mobile, Wireless and Sensor Networks: A Clustering Algorithm for Energy Efficiency and Safety, Apple Academic Press, 2019.

[3] E. C. Whitman, "Sosus: The "secret weapon" of undersea surveillance," Undersea Warfare, vol. 7, no. 2, p. 256, 2005.

[4] V. Jindal, "History and architecture of Wireless sensor networks for ubiquitous computing," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), vol. 7, no. 2, pp. 214-217, February 2018.

[5] R. Silva, Z. Zinonos, J. S. Silva and V. Vassiliou, "Mobility in WSNs for critical applications," in 2011 IEEE Symposium on Computers and Communications (ISCC), 2011.

[6] D. Stevanovic and N. Vlajic, "Performance of IEEE 802.15. 4 in wireless sensor networks with a mobile sink implementing various mobility strategies," in 2008 33rd IEEE Conference on Local Computer Networks (LCN), 2008.

[7] V. Ramasamy, "Mobile Wireless Sensor Networks: An Overview," in Wireless Sensor Networks - Insights and Innovations, P. Sallis, Ed., IntechOpen, 2017.

[8] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," IEEE Communications magazine, vol. 40, no. 8, pp. 102-114, 2002.

[9] T. P. Lambrou and C. G. Panayiotou, "A survey on routing techniques supporting mobility in sensor networks," in 2009 Fifth International Conference on Mobile Ad-hoc and Sensor Networks, 2009.

[10] U. Burgos, U. Amozarrain, C. Gómez-Calzado and A. Lafuente, "Routing in mobile wireless sensor networks: A leader-based approach," Sensors, vol. 17, no. 7, p. 1587, 2017.

[11] M. Fonoage, M. Cardei and A. Ambrose, "A QoS based routing protocol for wireless sensor networks," in International Performance Computing and Communications Conference, 2010.

[12] J. N. Al-Karaki and A. E. Kamal, "Routing techniques in wireless sensor networks: a survey," IEEE wireless communications, vol. 11, no. 6, pp. 6-28, 2004.

[13] J. Sen, "Routing security issues in wireless sensor networks: attacks and defenses," in Sustainable Wireless Sensor Networks, InTech, 2010, pp. 279-309.

[14] M. Radi, B. Dezfouli, K. A. Bakar and M. Lee, "Multipath routing in wireless sensor networks: survey and research challenges," Sensors, vol. 12, no. 1, pp. 650-685, 2012.

[15] S. Varshney and R. Kuma, "Variants of LEACH routing protocol in WSN: A comparative analysis," in 2018 8th International conference on cloud computing, data science & engineering (confluence), 2018.

[16] D.-S. Kim and Y.-J. Chung, "Self-organization routing protocol supporting mobile nodes for wireless sensor network," in First International Multi-Symposiums on Computer and Computational Sciences (IMSCCS'06), 2006.

[17] G. Renugadevi and M. Sumithra, "An analysis on LEACH-mobile protocol for mobile wireless sensor networks," International Journal of Computer Applications, vol. 65, no. 21, pp. 38-42, 2013.

[18] 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 Communications and Mobile Computing, vol. 2017, 2017.

[19] G. S. Kumar, M. V. Paul, G. Athithan and K. P. Jacob, "Routing protocol enhancement for handling node mobility in wireless sensor networks," in TENCON 2008-2008 IEEE Region 10 Conference, 2008.
[20] Z. Qi and Y. Min, "A routing protocol for mobile sensor network based on leach," in 10th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2014), 2014.
[21] S. Mottaghi and M. R. Zahabi, "Optimizing LEACH clustering algorithm with mobile sink and rendezvous nodes," AEU-International Journal of Electronics and Communications, vol. 69, no. 2, pp. 507-514, 2015.
[22] B. Nazir and H. Hasbullah, "Mobile sink based routing protocol (MSRP) for prolonging network lifetime in clustered wireless sensor network," in 2010 International Conference on Computer Applications and Industrial Electronics, 2010.
[23] C. E. Perkins, Ad hoc networking, vol. 1, Addison-wesley Reading, 2001.
[24] techopedia.com, "Definition - What does Ad Hoc On-Demand Distance Vector (AODV) mean?," 2019. [Online]. Available: https://www.techopedia.com/definition/2922/ad-hoc-on-demand-distance-vector-aodv. [Accessed November 2019].
[25] H. I. Sigiuk and A. A. Ihbeel, "Performance evaluation of dynamic source routing protocol (DSR) on WSN," International Journal of Computing and Digital Systems, vol. 1, no. 1, pp. 19-24, 2012.
[26] D. Karaboga and B. Basturk, "A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm," Journal of global optimization, vol. 39, no. 3, pp. 459-471, 2007.
[27] Y. Yue, J. Li, H. Fan and Q. Qin, "Optimization-based artificial bee colony algorithm for data collection in large-scale mobile wireless sensor networks," Journal of Sensors, vol. 2016, 2016.
[28] S. Cakici, I. Erturk, S. Atmaca and A. Karahan, "A novel cross-layer routing protocol for increasing packet transfer reliability in mobile sensor networks," Wireless personal communications, vol. 77, no. 3, pp. 2235-2254, 2014.
[29] S. A. Awwad, C. K. Ng, N. K. Noordin and M. F. A. Rasid, "Cluster based routing protocol for mobile nodes in wireless sensor network," in 2009 International Symposium on Collaborative Technologies and Systems, 2009.
[30] J. Shi, X. Wei and W. Zhu, "An efficient algorithm for energy management in wireless sensor networks via employing multiple mobile sinks," International Journal of Distributed Sensor Networks, vol. 12, no. 1, 2016.
[31] S. Deng, J. Li and L. Shen, "Mobility-based clustering protocol for wireless sensor networks with mobile nodes," IET wireless sensor systems, vol. 1, no. 1, pp. 39-47, 2011.
[32] S. Lindsey and C. S. Raghavendra, "PEGASIS: Power-efficient gathering in sensor information systems," in Proceedings, IEEE aerospace conference, 2002.
[33] M. R. Jafri, N. Javaid, A. Javaid and Z. A. Khan, "Maximizing the lifetime of multi-chain pegasis using sink mobility," arXiv preprint arXiv:1303.4347, 2013.
[34] R. Velmani and B. Kaarthick, "An efficient cluster-tree based data collection scheme for large mobile wireless sensor networks," IEEE sensors journal, vol. 15, no. 4, pp. 2377-2390, 2014.
[35] R. Velmani and B. Kaarthick, "An energy efficient data gathering in dense mobile wireless sensor networks," ISRN Sensor Networks, vol. 2014, 2014.
[36] R. Anitha and P. Kamalakkannan, "Enhanced cluster based routing protocol for mobile nodes in wireless sensor network," in 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering, 2013.
[37] T. Hayes and F. H. Ali, "Proactive Highly Ambulatory Sensor Routing (PHASeR) protocol for mobile wireless sensor networks," Pervasive and Mobile Computing, vol. 21, pp. 47-61, 2015.
[38] C. Tunca, S. Isik, M. Y. Donmez and C. Ersoy, "Ring routing: An energy-efficient routing protocol for wireless sensor networks with a mobile sink," IEEE Transactions on Mobile Computing, vol. 14, no. 9, pp. 1947-1960, 2014.
[39] A. E. Kostin, Y. Fanaeian and H. Al-Wattar, "Anycast tree-based routing in mobile wireless sensor networks with multiple sinks," Wireless Networks, vol. 22, no. 2, pp. 579-598, 2016.
[40] S. Sarangi and S. Kar, "Genetic algorithm based mobility aware clustering for energy efficient routing in wireless sensor networks," in 2011 17th IEEE International Conference on Networks, 2011.
[41] J. Wang, Y.-Q. Cao, B. Li, S.-Y. Lee and J.-U. Kim, "A glowworm swarm optimization based clustering algorithm with mobile sink support for wireless sensor networks," Journal of Internet Technology , vol. 16, no. 5, pp. 825-832, 2015.
[42] D. W. Carman, P. S. Kruus and B. J. Matt, "Constraints and approaches for distributed sensor network security," 2000.
[43] I. Kamel and H. Juma, "A lightweight data integrity scheme for sensor networks," Sensors, vol. 11, no. 4, pp. 4118-4136, 2011.
[44] C.-M. Chen, Y.-H. Lin, Y.-H. Chen and H.-M. Sun, "Sashimi: secure aggregation via successively hierarchical inspecting of message integrity on wsn," Journal of Information Hiding and Multimedia Signal Processing, vol. 4, no. 1, pp. 57-72, 2013.
[45] I. Silva, L. A. Guedes, P. Portugal and F. Vasques, "Reliability and availability evaluation of wireless sensor networks for industrial applications," Sensors, vol. 12, no. 1, pp. 806-838, 2012.
[46] R. Riaz, T.-S. Chung, S. S. Rizvi and N. Yaqub, "BAS: The Biphase Authentication Scheme for Wireless Sensor Networks," Security and Communication Networks, vol. 2017, 2017.
[47] S. A. Ch, Z. Mehmood, D. Rashid Amin, M. Alghobiri and T. A. Malik, "Ensuring Reliability & Freshness in Wireless Sensor Networks," in 2010 International Conference on Intelligent Network and Computing (ICINC 2010) , 2010.
[48] L. Lazos and R. Poovendran, "SeRLoc: Robust localization for wireless sensor networks," ACM Transactions on Sensor Networks (TOSN), vol. 1, no. 1, pp. 73-100, 2005.
[49] A. Srinivasan and J. Wu, "A survey on secure localization in wireless sensor networks," Encyclopedia of Wireless and Mobile communications, pp. 1-26, 2007.
[50] J. Hwang and Y. Kim, "Revisiting random key pre-distribution schemes for wireless sensor networks," in Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, 2004.
[51] A.-S. K. Pathan, Security of self-organizing networks: MANET, WSN, WMN, VANET, CRC press, 2016.
[52] J. He, J. Chen, P. Cheng and X. Cao, "Secure Time Synchronization in WirelessSensor Networks: A MaximumConsensus-Based Approach," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 4, pp. 1055-1065, 2014.
[53] S. Ganeriwal, S. Čapkun, C.-C. Han and M. B. Srivastava, "Secure time synchronization service for sensor networks," in Proceedings of the 4th ACM workshop on Wireless security, 2005.
[54] G. Yang, L. Dai and Z. Wei, "Challenges, threats, security issues and new trends of underwater wireless sensor networks," Sensors, vol. 18, no. 11, p. 3907, 2018.
[55] M. Riaz, A. Buriro and A. Mahboob, "Classification of Attacks on Wireless Sensor Networks : A Survey," International Journal of Wireless and Microwave Technologies, vol. 8, pp. 15-39, 11 2018.
[56] S. Sudheendran, O. Bouachir, S. Moussa and A. O. Dahmane, "Review — Challenges of mobility aware MAC protocols in WSN," in 2018 Advances in Science and Engineering Technology International Conferences (ASET), 2018.
[57] H. Gong, X. Zhang, L. Yu, X. Wang and F. Yi, "A study on MAC protocols for wireless sensor networks," in 2009 Fourth International Conference on Frontier of Computer Science and Technology, 2009.
[58] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in Proceedings of the World Congress on Engineering, 2015.
[59] P. M. Jawandhiya, M. M. Ghonge, M. Ali and J. Deshpande, "A survey of mobile ad hoc network attacks," International Journal of Engineering Science and Technology, vol. 2, no. 9, pp. 4063-4071, 2010.
[60] D. R. Raymond and S. F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses," IEEE Pervasive Computing, pp. 74-81, 2008.
[61] A. D. Wood and J. A. Stankovic, "Denial of service in sensor networks," computer, vol. 35, no. 10, pp. 54-62, 2002.
[62] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah and K. N. Qureshi, "Security Issues and Attacks in Wireless Sensor Network," World Applied Sciences Journal, vol. 30, no. 10, pp. 1224-1227, 2014.
[63] T. H. Hadi, "MANET and WSN: WHAT MAKES THEM DIFFERENT?," IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), vol. 7, no. 6, pp. 23-28, Nov-Dec 2017.
[64] M. L. Messai, "Classification of attacks in wireless sensor networks," in International Congress on Telecommunication and Application 2014 arXiv preprint arXiv:1406.4516, 2014.

[65] R. Maheshwari, J. Gao and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information," in IEEE INFOCOM 2007-26th IEEE International Conference on Computer Communications, 2007.

[66] C. a. M.-P. C. Del-Valle-Soto, I. Aldaya, F. Lezama, J. A. Nolazco-Flores and R. Monroy, "New Detection Paradigms to Improve Wireless Sensor Network Performance under Jamming Attacks," Sensors, vol. 19, no. 11, p. 2489, 2019.

[67] M. Tellez, S. El-Tawab and H. M. Heydari, "Improving the security of wireless sensor networks in an IoT environmental monitoring system," in 2016 IEEE Systems and Information Engineering Design Symposium (SIEDS), 2016.

[68] O. Adarkar, R. Mane and D. Shah, "IMPACT OF WORMHOLE ATTACK IN WIRELESS SENSOR NETWORK," International Research Journal of Engineering and Technology (IRJET), vol. 5, no. 6, pp. 2237-2241, June 2018.

[69] K. Harsányi, A. Kiss and T. Szirányi, "Wormhole detection in wireless sensor networks using spanning trees," in 2018 IEEE International Conference on Future IoT Technologies (Future IoT), 2018.

[70] D. C. Mehetre, S. E. Roslin and S. J. Wagh, "Detection and prevention of black hole and selective forwarding attack in clustered WSN with Active Trust," Cluster Computing, vol. 22, no. 1, pp. 1313-1328, 2019.

[71] F. A. Khan, A. H. Farooqi and A. Derhab, "A comprehensive security analysis of LEACH++ clustering protocol for wireless sensor networks," The Journal of Supercomputing, vol. 75, no. 4, pp. 2221-2242, 2019.

[72] M. I. Abdullah, M. M. Rahman and M. C. Roy, "Detecting sinkhole attacks in wireless sensor network using hop count," International Journal of Communication Networks and Information Security (IJCNIS), vol. 7, no. 3, pp. 50-56, 2015.

[73] L. Lamport, R. Shostak and M. Pease, "The Byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382-401, 1982.

[74] Y. Yang, P. Xiong, Q. Wang and Q. Zhang, "Analysis of Byzantine Attacks for Target Tracking in Wireless Sensor Networks," Sensors, vol. 19, no. 15, p. 3436, 2019.

[75] P. Anusuya, R. Chithradevi and S. Dhivya, "Prevent Byzantine Attack on Manet Using Enhanced Co-Operative Bait Detection and Prevention Scheme," International Journal of Engineering Technologies in Engineering Research, vol. 4, no. 5, pp. 217-220, 2016.

[76] Y.-C. Hu, A. Perrig and D. B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network," in Proceedings of the 2nd ACM workshop on Wireless security, 2003.

[77] T. Bhattasali, R. Chaki and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network," arXiv preprint arXiv:1203.0231, 2012.

[78] U. S. R. K. Dhamodharan and R. Vayanaperumal, "Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method," The Scientific World Journal, vol. 2015, 2015.

[79] H. Chen, C. Meng, Z. Shan, Z. Fu and B. K. Bhargava, "A Novel Low-Rate Denial of Service Attack Detection Approach in ZigBee Wireless Sensor Network by Combining Hilbert-Huang Transformation and Trust Evaluation," IEEE Access, vol. 7, pp. 32853-32866, 2019.

[80] C. Marigowda, J. Thriveni, S. Gowrishankar and K. Venugopal, "An Efficient Secure Algorithms to Mitigate DoS, Replay and Jamming Attacks in Wireless Sensor Network," in Proceedings of the World Congress on Engineering and Computer Science, 2018.

[81] W. J. Chung and T. H. Cho, "A Multi-Path Routing Determination Method for Improving the Energy Efficiency in Selective Forwarding Attack Detection Based MWSNs," International Journal of Wireless & Mobile Networks (IJWMN), vol. 10, no. 4, pp. 9-19, August 2018.

[82] J. Cui, L. Shao, H. Zhong, Y. Xu and L. Liu, "Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks," Peer-to-Peer Networking and Applications, vol. 11, no. 5, pp. 1022-1037, September 2018.