International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 14, No.1 (Oct-23)

http://dx.doi.org/10.12785/ijcds/1401108

Mitigation of Sinkhole Attack in Dynamic Directional Routing for Mobile Wireless Sensor Networks

Ali Maki Alaali[1] **and Reham Almesaeed**[2]

[1] *College of Information Technology, University of Bahrain, Sakheer, Bahrain*
[2] *College of Information Technology, University of Bahrain, Sakheer, Bahrain*

Received 25 Jun. 2023, Revised 8 Oct. 2023, Accepted 10 Oct. 2023, Published 15 Oct. 2023

Abstract: Wireless sensor networks (WSNs) play a major role in the 6G and beyond systems, thus it has been one of the major research fields in the past few decades. The deployment of WSNs in future communication networks has been investigated in literature and has shown great potential for many applications such as healthcare, industrial control and monitoring, agriculture, etc. However, there are many challenges that arise from deploying such networks to ensure efficient and reliable operation, such as energy efficiency, security, reliability, scalability, and adaptability. This article explores one of the security threats in WSNs, which is the sinkhole attack, and investigates the research projects in this area. This study highlights the limitations of the state-of-the-art research in this field, then designs and simulates a secured routing protocol to detect and mitigate Sinkhole attacks in mobile wireless sensor networks (MWSNs) and ensure their security and availability. The proposed Directional Routing Reflector Protocol is proven to achieve steady and reliable performance in threat detection, while maintaining the energy efficiency and the lifetime of the sensor nodes.

Keywords: WSN, MWSNs, DDR, CSARP, Sinkhole Attack

1. INTRODUCTION

MWSNs have introduced a growing well-known sort of wireless sensor network (WSN), and it plays some critical roles in today's real-world applications. To illustrate today's tradeoffs of MWSNs and WSN, it is useful to briefly inspect their history. The first WSN called Sound Surveillance System (SOSUS) purpose to track submarines was developed in the fifties of the last century by the United States Military during their war with the Soviets [1]. SOSUS is still used for scientific research such as vocalizations of whales and recording average ocean temperature changes over an ocean basin [2].

WSN consists of multiple small and low-cost sensor nodes formed in groups. Various types of sensors are used in such networks such as vibration sensors, thermal sensors, visual sensors, movement sensors, infrared sensors, and radar sensors aim to track, monitor, or supervise surrounding environmental conditions. These nodes can communicate with each other by using wireless connectivity and transmit the collected data to the main location which is called the base station, or sink node. The sensor nodes are implanted with, computation units, storage, tiny sensors, and communication functionalities to achieve this purpose. [3].

With the continuous revolutions in networking and computing technologies, a huge turn occurred in the WSN. MWSNs were introduced, where the sensors became mobiles and that add massive advances in this technology because it became more useful than the static sensors. Mobile nodes can move randomly, periodically, or in a fixed root. Furthermore, based on the applications the nodes will be either dependent or independent of each other [4]. Currently, MWSNs are used in many fields including the healthcare field, the industrial field, and the military field. Despite all of that, MWSNs introduced new challenges to its functionality such as network coverage area and security.

As mentioned earlier, MWSNs are used in many fields and some of them contain critical data, which makes MWSNs a target for enemies and competitors in many kinds of security attacks. Attacks that target network traffic and availability, such as Sinkhole attacks, are among the most serious and critical attacks.

Illegitimate or compromised nodes can cause significant damage to the network by poisoning the routing table with fake routing updates. This can result in dropped packets, delayed packets, or even manipulated data being forwarded to the sink node or the base station. These actions could

E-mail address: ali.alaali1991@gmail.com, ralmesaeed@uob.edu.bh

lead to disruptions in network communication, data loss, and potentially even security breaches [5].

While it is true that the limited resources in MWSN nodes can make it challenging to implement security measures, it is important to consider the potential consequences of ignoring this threat. Without proper security measures, MWSN nodes can be vulnerable to attacks that can compromise data availability and integrity. Although some routing protocols may not prioritize security due to the additional resources required. However, implementing secure routing processes can help to detect and prevent attacks earlier. This can help to ensure that data remains available and secure, even in the face of potential threats. Therefore, finding a balance between resource limitations with security needs is substantial in order to maintain robust and reliable MWSNs.

The primary objective of this research is to design and develop a secure, practical, and lightweight routing algorithm that aims to detect and mitigate Sinkhole attacks in MWSNs while maintaining the performance of the networks and simultaneously minimizing power consumption which can be achieved after a wide search and study on MWSNs, its routing protocol, applications, Sinkhole attacks, existing solutions to detect and mitigate Sinkhole attacks. Research objectives and contributions are listed below: noitemsep

- Conduct an extensive literature review of MWSNs and Dynamic Directional Routing protocol (DDR). Investigate the weaknesses of the current routing algorithm of DDR protocol that led to successful Sinkhole attacks.
- Apply the required changes to achieve the required security mechanism to protect MWSNs from Sinkhole attacks. The proposed solution is built upon the DDR protocol which uses the Threshold sensitive Low Energy Adaptive Clustering Hierarchy protocol (T-LEACH), it is an extended version of the Low Energy Adaptive Clustering Hierarchy (LEACH) protocol.
- Simulate the enhanced algorithm of DDR protocol and analyze the simulation results.

This research will provide a comprehensive literature review of MWSNs, DDR protocol, security aspects, challenges, Sinkhole attacks, detection techniques, and related work. The proposed solution should enhance the security of DDR protocol to detect Sinkhole attacks in MWSNs. Simulation results should ensure the effectiveness and efficiency of the proposed solution.

The rest sections are ordered as follows Section Two: Background, which provides an extensive overview of WSN and MWSNs, threats, and security challenges. Section Three: Related work, clarifies the Sinkhole attacks, and summarizes some of the proposed solutions to detect and mitigate Sinkhole attacks. Section Four: the Proposed Security Scheme, which contains the problem statement, the network and Sinkhole attack model, and the design of the proposed scheme for DDR protocol. Section Five: Simulation Results and Performance Analysis, which discusses and analyzes the simulation setup and results of the proposed scheme. Section Six: The Conclusion and Recommendations, which concludes the thesis and provides recommendations and future work.

2. Background

MWSNs are developed types of WSN that contain an additional feature which is mobility within the used sensor nodes. MWSNs were developed to support a wide range of applications in many fields like military, healthcare, industrial, and environmental monitoring. With this evolution in MWSNs a lot of new routing protocols developed to support the MWSNs, but new challenges appear to the MWSNs related to reliability and security.

A. Routing in MWSNs

Routing protocol plays a critical role in MWSNs, it is responsible for delivering the collected data from the source sensor node to another sensor node till it reaches the sink node or the base station by establishing an effective route path between any source node toward any destination. Various routing protocols proposed by many researchers based on different criteria and designs. However, no routing protocol can be perfect for all MWSNs applications. Some routing protocols might fit with specific applications, but they might fail with others. Due to the nature of MWSNs mobility, data redundancy, energy efficiency, and the dynamic nature of network topology need to be considered and managed carefully. The used routing protocols in MWSNs can be classified as shown in figure 1 [6].

In the network structure-based category there are three types. First, the flat-based routing which is appropriate for a sizeable network containing numerous sensor nodes and global identifiers is unfeasible due to the inability to allocate individual identification to every node [7]. In this approach, all nodes carry out the same functionality some examples are Directed Diffusion, Minimum Cost Forwarding Algorithm, Flooding approach, and Active Query forwarding[8] [9] [10] [11].

The second approach is hierarchical-based, which is known as well by the cluster-based routing protocol. This approach intends to optimize the power consumption of the network by dividing the nodes into groups called clusters, and within each cluster there is one node act as the cluster head and it is responsible for data collection from cluster members, then forward the collected data to the base station either directly or via other cluster head. This approach proved its concept of optimizing power consumption and extending network lifespan. The(LEACH) and Threshold-sensitive Energy Efficient Protocols (TEEN) are some examples of hierarchical-based routing protocols. [9] [12]. The last one is location-based routing, where routing path establishment depends on the location information of the nodes which could be determined by using a Global

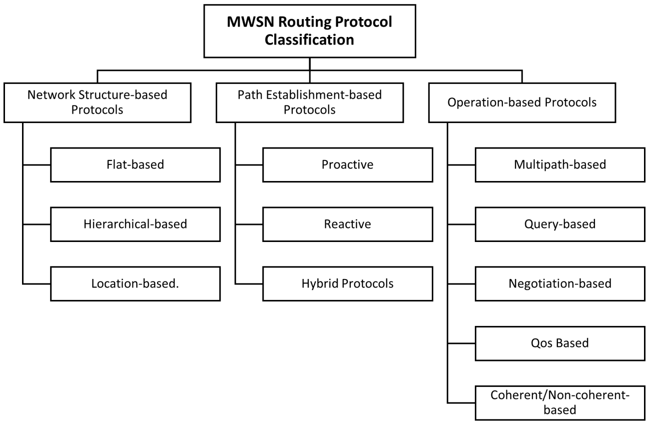
MWSN Routing Protocol Classification
Network Structure-based Protocols
Path Establishment-based Protocols
Operation-based Protocols
Flat-based
Hierarchical-based
Location-based.
Proactive
Reactive
Hybrid Protocols
Multipath-based
Query-based
Negotiation-based
Qos Based
Coherent/Non-coherent-based

Figure 1. MWSNs Routing Protocol Classification

Positioning System (GPS) or any other technology [13]. Minimum Energy Communication Network (MECN), and Geographical and Energy Aware Routing (GEAR) are some examples of location-based routing [14], [15].

The second category is the path establishment-based routing protocols. The routing path in this approach can be established in three ways which are proactive, reactive, or hybrid. The proactive protocol creates a routing table with all available paths even if the path is not in use Optimized link state routing (OLSR) is an example of proactive routing protocol. The reactive protocol routing process is performed once it is needed, Dynamic Source Routing (DSR), and Ad-hoc on-demand distance vector (AODV) are examples of the reactive protocol. The hybrid routing protocols combine both reactive routing protocol and proactive routing protocol[11], [16].

The last category is operation-based routing protocols. The first approach is the multipath routing protocol, in this approach the routing protocol utilizes several paths to send the data toward the base station such as Multipath and Multi SPEED (MMSPEED) and Sensor protocols for information via negotiation (SPIN) routing protocols. The second approach is the query-based routing protocol, which allows the base station to request the information from the node, some examples of this routing approach are (SPIN), Directed diffusion (DD), and COUGAR [17]. The utilization of negotiation-based routing protocols facilitates the maintenance of the lowest possible level of redundant data transmission by engaging in negotiations with neighboring nodes to identify and select the optimal pathway for transmitting data. (SPIN) and Sequential assignment routing (SAR) are examples of this approach [18]. QoS-based routing protocols are used to ensure Quality of Service, this protocol seeks to find a route path that meets certain levels of metrics such as throughput, delay, and power. Multi path and Multi SPEED (MMSPEED) and Sequential assignment routing (SAR) routing protocols use this approach. In coherent-based routing, the node is responsible to perform the minimum processing on the data such as time stamping and data compression then sending it to the next node or the aggregator. The aggregator is responsible for aggregating the received data and sending it to the base station. This approach is used to ensure energy-efficacy of the routing protocol, multiple winner algorithm is an example of a coherent-based routing protocol. On the other hand, non-coherent data routing where the node is processing the raw data only before sending it to the aggregator or other node for further processing Single Winner Algorithm (SWE) is an example of a non-coherent-based routing protocol [14], [16].

B. *Dynamic Directional Routing protocol (DDR)*

The DDR is a novel protocol proposed by Almesaeed and Jedidi for MWSNs almesaeed2021dynamic. This routing protocol operates based on a directional-based routing approach to determine the best routing path toward the base station dynamically while network topology is keep changing due to node mobility. Within the network, each sensor node is able to forward the data to its neighbor sensor node that is reachable within the routing zone. The routing zone in DDR is a limited zone defined by a specific angle that heads to the base station.

With the aim of transmitting data from any sensor node toward the base station, there exist two requisite processes. The initial process is referred to as the discovery process, where the node endeavors to identify the subsequent node to which the data must be sent. This is accomplished by employing two parameters: the search angle in degrees, which remains constant for all participating network nodes, and the distance between the sender node and the edge of the network region. Upon the completion of the discovery process, the subsequent phase of forwarding commences, whereby the data is transmitted to the designated node.

The outcomes of the simulation demonstrate that the introduced routing protocol exhibits a considerable advancement in the lifespan of the network. Specifically, the network lifespan improvements are measured to be 13% greater than that of T-LEACH and an impressive 50% greater than area-based routing protocols. Additionally, The DDR shows better route selection compared to area-based routing protocols and T-LEACH by providing shorter route lengths, which lead to enhanced packet delivery ratio, and that has been achieved by around 10%.

C. *Security Requirements in MWSNs*

There are many similarities between MWSNs and computer networks. However, it is still required unique security features due to the nature of MWSNs. The most security requirements are:

1) Confidentiality: data in MWSNs should be protected and messages transmitted in the network can be read only by the authorized receptionists. To achieve that, the key distribution techniques should be robust, and

information related to the node such as ID or keys should be secure to avoid any attack related to traffic analysis.

2) Integrity: MWSNs could be used in many critical fields such as healthcare, and the military. Data integrity is a must in these fields to protect the data from any manipulations because it might threaten businesses, people, and countries. As mentioned in section 2.1.1.3 The majority of sensor nodes operate on power sources with limited availability, typically precluding recharging or replacement of batteries. As a consequence, it is essential to utilize lightweight algorithms in order to safeguard data integrity and limit power consumption.

3) Availability: MWSNs are highly dependent on the durability and accessibility of their networks for smooth functioning. The occurrence of network failure can give rise to significant consequences, including detrimental effects on businesses, financial losses, or the risk of endangering individuals. The availability of a system can be affected by various factors, such as security attacks, software or system failures, as well as the absence of structured approaches towards system management. Hence, the functionality of MWSNs ought to be maintained even amidst attacks and system failure. This can be achieved through the implementation of redundancy, prevention and mitigation of attacks, and the establishment of a reliable software and hardware configuration.

4) Authentication: A critical aspect of MWSNs communication is the authentication process. Since MWSNs communications are broadcast, identifying the source or destination nodes is always challenging. The Message Authentication Code (MAC) mechanism could be used to identify the node before transmitting the data. However, this mechanism might cause to increase in power consumption and lead to a decrease in the lifespan of MWSNs. Some researchers have developed certain lightweight authentication techniques, and one of them is the Biphase authentication scheme (BAS) presented by Riaz, Chung, Rizvi, and Yaqub. BAS provides small-scale authentication and durability in front of DoS attacks that could be generated by malicious nodes [19]. Packet leashes, proposed by Hu, Perrig, and Johnson, is a novel and generic mechanism aimed at detecting and mitigating wormhole attacks that necessitate the gaining of unauthorized network access. [20].

5) Data freshness: The transferred data within the MWSNs need to be recent data, not old data. Malicious nodes can start replay attacks and send old data to consume node and network resources, once the key is exposed to the adversaries especially when MWSNs use shared keys for message communication. To ensure data freshness, two methods could be used by adding a nonce or time-specific counter in the packets. First is data dynamicity which depends on the frame sequence, and it can be checked by the destination node. The second method is by checking and verifying each packet individually, called delay tolerance and independent processing [21].

6) Secure localization: The location of the sensor node once it starts sending any information such as data or alarm is very important, in many situations such as disaster monitoring systems, the response team needs to know the location to respond. Also, in the oil and gas field, if the H2S is detected all employees at that location need to be informed to avoid human losses. A potential adversary can attack this information by manipulating signal strength or using replaying messages to provide a false location to the system. To overcome this issue, Lazos and Poovendran have proposed a scheme named secure range-independent localization (SeRLoC) [22].

7) Self-organization: The most important feature of MWSNs is that they can work without human interaction. Nodes in the MWSNs deployed without knowledge of the network size, and other connected nodes. Thus, nodes should be self-organizing and self-healing to be capable to communicate with the other sensor nodes and with the sink node or base station. Some MWSNs applications besides their dynamic nature make configuring secret or shared keys difficult [23]. Some researchers proposed key pre-distribution schemes with symmetric encryption such as random key pre-distribution schemes for sensor networks by Chan, Perrig, and Song [24]. Furthermore, for distributed sensor networks the key-management approach was also proposed by Laurent and Virgil [23]. Another pre-distribution scheme for WSNs proposed by Hwang and Kim named Revisiting random key pre-distribution [25]. Likewise, Liu, Ning, and Li proposed Establishing pair-wise keys in distributed sensor Networks [26].

8) Self-stabilization: This feature means that the node is able to recover and return to its normal state after the attack without user intervention, even if the threat persists in the network [27].

9) Survivability: During the incident or the attack this ability of the system ensures that all tasks are accomplished in a timely manner even in the occurrence of the intrusion. Furthermore, it makes sure that the network is able to restore and continue operating to accomplish the tasks even if some sensors are disconnected or destroyed [27].

10) Time synchronization is a critical task within any network because it could cause an outage or distribute the service. For an instant, time synchronization enables the node's movement speed and location to be determined [28]. Furthermore, any used security mechanism in MWSNs should also be time-synchronized. Some malicious attacks target time synchronization by using altered messages. Such attacks need to be prevented to ensure the functionality of the network. Chen, Cheng, and Cao

proposed detection techniques called the Maximum Consensus-Based Approach to detect the altered message [29]. Also, other researchers Ganeriwal, Capkun, Han, and Srivastava proposed a group of protocols to detect and protect the node and its neighbors from such attacks by securing the group synchronization besides pair nodes located within their power rages [30].

11) Isolation: Once an incident occurs in the network and the malicious node is discovered, the other sensor nodes should be capable of insulating themselves and their traffic from the malicious node to prevent the risk. Yang, Dai, illustrate in their research that lightweight cryptographic schemes could be used to achieve the isolation process [27].

D. *Security Challenges in MWSNs*

In MWSNs the mobility feature participates in introducing security challenges that introduce more vulnerabilities to the MWSNs. Due to the mobility feature, the sensor nodes required Medium Access Control (MAC) protocols in order to communicate, and they will be responsible for managing the throughput, transmitting data, and security of communication which increase the security challenges. Additionally, MWSNs contain a huge number of nodes that moves in random directions which means there is no limit to the network size, and to secure the network appropriate design and implementation is required [31].

As mentioned previously MWSNs are used in different sectors and one of the security requirements is self-healing. Thus, the nature of the MWSNs environment makes it difficult to fulfill this requirement because some nodes are deployed in a neglected spot in which self-healing and self-configuration cannot be achieved due to the condition of the environment. That could affect the node's correlations and lead to another network vulnerability [23]. While MWSNs use wireless medium there are other vulnerabilities that increase the chance of eavesdropper attack. Also, the adversary might be able to reach a node deployed in an unattended environment and gain physical access to the node to obtain critical information including security keys or manipulate the node to do malicious activities [32]. The last and most significant challenge is the resource limitations of the nodes. Due to their sizes, the available resources are limited, and security operations require efficient energy, memory, and sufficient processing unit [33].

E. *MWSNs Threats and Attacks*

As stated by the authors in [34], security threats could be categorized according to the origin of the threat actor, either external or internal. The purpose of the external threats is to disrupt the services of the MWSNs by focusing on its availability. However, the aim of the internal threats is to attain authorization and aim for the preservation of confidentiality and integrity. The internal threat actor potentially utilizes nodes that have been compromised to instigate malicious assaults. Furthermore, security attacks may be categorized, based on the objectives of the threat actor, into two distinctive forms, including passive and active attacks.

Passive attacks involve a threat actor who engages in passive monitoring of network traffic with the objective of gaining unauthorized access to confidential or privileged information. In the context of network security, passive attacks refer to cyber threats that are conducted without disrupting network services or triggering any alarms that may expose the activities of the threat actor. This covert approach obviates detection and ensures that the threat actors can continue their exploitative activities undetected. Passive attacks constitute a set of malicious actions which encompass a variety of illicit activities such as the decryption of encrypted information, eavesdropping, communication interception, and traffic analysis.

On the hand, active attacks are aimed at implementing specific actions targeted toward a given network, resulting in the service's disruption, manipulation of data, deployment of malicious activities, or the acquisition of control over accessible resources. In the sphere of cyber security, a significant portion of attacks with the intention of intrusion usually initiate with a passive approach, involving an examination of vulnerabilities present within the network. Following this reconnaissance phase, the threat actors proceed to develop an active attack methodology.

MWSNs is susceptible to security attacks that particularly target Open Systems Interconnection (OSI) layers. For instance, the physical layer of MWSNs may encounter attacks such as jamming and tampering. The Collision, Exhaustion, and Unfairness attacks are specifically directed toward the link layer. The network layer is vulnerable to a variety of malicious attacks such as Neglect and greed, Homing, Misdirection, Sinkhole, and Blackhole. Finally, it should be noted that the transport layer can be targeted by Flooding or Desynchronization attacks [35].

3. Related Work

This section clarifies the Sinkhole attack and summarizes some solutions which were proposed to detect and mitigate Sinkhole attacks.

A. *Sinkhole attack*

The Sinkhole attack targets the network layer, and it can be initiated in two ways, either by injecting a malicious or compromised node in the network or by hacking an existing one. Then the compromised node starts advertising forged routing information to all its neighbor nodes and pretends that it owns the shortest path toward the base station or sink node. The number of impacted nodes is determined by the location of the malicious sensor node if it is located nearby to the base station, it might pull all the traffic or most of the traffic. If the compromised node is deployed in the network successfully, the adversary will be able to do three things to the received data, either drop the data, delay the data, or modify the data then send it to the base station. From the possible actions on the data, the Sinkhole node is classified as below [36]: noitemsep

- Sinkhole message dropping node (SDP): The compromised sensor nodes drop the data.
- Sinkhole message delay node (SDL): The compromised sensor nodes delay the data.
- Sinkhole message modification node (SMD): The compromised sensor nodes alter the data and then resend it toward the destination.

B. Proposed Solutions

In light of the heightened need for applications in high-risk and sensitive areas, many researchers are focusing on WSNs. In spite of resource constraints, mechanisms must be provided to ensure security. Researchers have identified several approaches that can be used to detect and identify Sinkhole attacks in WSNs. Those approaches are classified into rules-based, key management, anomaly-based, statistical methods, and hybrid-based. In this section, some of the proposed solutions that use each of these approaches are summarized briefly below.

A. Rule-based

The rules were planned and developed in accordance with the behavior or method utilized to dispatch Sinkhole attacks. Later on, the designed rules are embedded within an intrusion detection system that runs the sensor node. These rules will be conducted on the packets transmitted through the network nodes. Whenever a node abuses any of the deployed rules, it is isolated from the network and considered as a suspicious node.

Krontiris, Dimitriou, Giannetsos, and Mpasoukos proposed a rules-based approach to detect Sinkhole attacks. Two rules were developed and implanted into the Intrusion Detection System (IDS). In the event of an intrusion by any node violating one of the two rules, the IDS triggers the alarm. However, their technique does not provide the node ID of the compromised node. The first rule is, “For each overhead route update packet, the sender’s ID must be different from your node ID”. The second rule is “For each overhead route update packet the ID of the sender must be one of the node IDs in your neighbors” [37].

In [38], the researchers again used the same approach with two rules. The first rule is “For each overhead route update packet the ID of the sender must be one of the node IDs in your neighbors ”The second rule is “For each pair of parent and child nodes their link quality they advertise for the link between them, the difference cannot exceed 50”.

B. Anomaly-based detection

In anomaly-based detection, the ordinary client behavior is characterized, then the intrusion detection is examining the network for any activity that is abnormal. According to this method, intrusions are considered abnormal because they appear unusual compared to normal behavior.

Tumrongwittayapak and Varakulsiripunth proposed a system that used Received Signal Strength Indicator (RSSI) values with the help of Extra Monitor (EM) nodes to detect Sinkhole attacks. In addition to having high communication ranges, the other function of the EM is to calculate the RSSI of each node and send the reading to the base station along with the source node ID beside the next hop ID. This process happens immediately when a node is deployed in the network. The Base stations use the received values to calculate Visual Geographical Map (VGM) to identify the position of the nodes. Later, when the EMs rescan the network to recalculate the RSSI and resend the updated values to the base station, which will compare the records to identify if there is any change in packet flow from previous data. If a change is detected, this indicates that there is a Sinkhole attack. The compromised node is identified and isolated from the network by the base station using VGM values. This approach was proposed based on a static network and did not mention how many EM nodes are required for a specific number of sensor nodes [39].

C. Statistical method

Statistical GRSh (Girshick-Rubin-Shyriaev)-based algorithm proposed by Chen, Song, and Hsieh for detecting suspicious nodes in a wireless sensor network. The variation in CPU usage of each node is calculated by the base station after monitoring the CPU usage for a specific time. Then it determines whether the node is legitimate or suspicious based on the comparison process between the CPU usage with the threshold [40].

A dynamic trust management system to detect and mitigate various attacks and the Sinkhole attack is one of them was proposed by four researchers. This system is based on the trust value which is based on the interactions between the nodes including the number of successful interactions, besides unsuccessful interactions, and the weight of net successful and unsuccessful interactions. This value is calculated by the sensor node and its neighbors. Later on, the calculated value is transmitted to the base station. The base station will receive various trust values for each node. Based on the received trust values, if any node trust value exceeds 0.5, it is considered as a suspicious node [41].

D. Hybrid-based intrusion detection

As part of this approach, both anomaly-based and signature-based are used. By using both methods the false positive rate generated by the anomaly-based approach is reduced. Furthermore, it has the ability to detect suspicious nodes by checking their signatures against detection databases. A group of researchers proposed a hybrid intrusion detection system to detect various types of attacks besides Sinkhole attacks by using a detection agent. The system was connected to the sensor node to gather the data.

The detection agent receives this data to decide whether the node is suspicious or not [42].

E. Key management

By using encryption and decryption keys, the integrity, and the authenticity of the packets traveling in the network will be achieved. A cryptographic approach was proposed to prevent Sinkhole attacks. The sensor nodes use the base station public key to validate the received message and ensure that is generated from the base station. Likewise, they use their own private and public keys that are uploaded to them offline, before deploying the network to authenticate themself and sign the messages. This method secures the network because the suspicious nodes are not able to hide their IDs and all messages are validated [43].

4. Proposed Security Scheme

The primary objective of this research is to design and develop a secure and practical technique to detect Sinkhole attacks based on DDR routing protocol for MWSNs while maintaining the performance of the network. The literature has an extensive review of different research and studies related to MWSNs, security requirements, and challenges, besides Sinkhole attacks, and many solutions have been proposed by numerous researchers with the purpose of detecting and mitigating Sinkhole attacks. Most of the proposed solutions succeed to detect Sinkhole attacks but with some limitations related to power consumption and memory size. Therefore, this thesis proposes a new Sinkhole attack detection technique that requires low resources and no additional hardware required. In the proposed mechanism, the base station is assumed to be static, and sensor nodes are mobile. Three scenarios of Sinkhole attacks were considered:

1) The adversary tries to insert a compromised node after the deployment of trustworthy nodes
2) The adversary tries to insert the compromised node during the deployment of the network
3) The adversary tries to insert the compromised node during the broadcast cycle with clone ID

A. Sinkhole Attack Model

The Sinkhole attack as presented in chapter two can be carried out after injecting a malicious node in the targeted network or manipulating a sensor node resident in the network. The malicious node will have the same specifications as the legitimate node. While the network is functioning normally, the malicious sensor node will advertise fake routing information to claim that it has the best path in order to draw data traffic from nearby nodes.

B. The Proposed Security Scheme

This section proposes the Directional Routing Reflector protocol (DRR), a new security scheme against Sinkhole attacks. As illustrated previously, The DDR provides a directional-based routing mechanism that dynamically adjusts the routes based on the changes that occur in the network topology due to the node mobility to reach the base station. The sensor nodes participate in the routing process by identifying the next hop node within their transmission range, figure 2 clarifies the process.

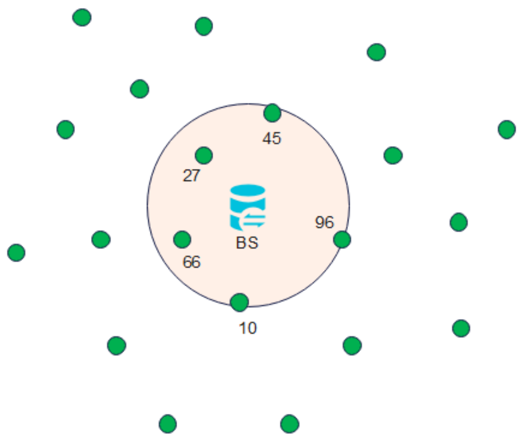

Figure 2. Neighbors' selection

The proposed security scheme (DRR) is inspired by the (DDR) discussed in section 2 subsection B. In the DRR protocol, the routes between the nodes and the base station are established initially at the nodes that are closer to the base station. To clarify the proposed security scheme, we assume a mobile wireless network that consists of the number of sensor nodes N which move randomly with the same speed (V m/s). In this scenario, one base station is deployed and located statically at point (xb,yb). Since we work with mobile nodes, we assume that they can verify their location by using Global Policy and Strategy (GPS) or any other pertinent technologies. Furthermore, nodes communicate through the low-rate wireless personal area network, IEEE 802.15.4 standard [44], and received signal power is used to check the quality of the communication signal. Furthermore, the abovementioned standard enables data transmission speeds starting from 20 kbps to 250 kbps [45]. These data rate values will be used as well to track the behavior of the sensor nodes.

Phase one: Trust Node Selection

During the preliminary phase, we assume that all nodes are legitimate, the base station will broadcast a message to select its trusted nearby sensor nodes based on the RSSI. The minimum RSSI necessary for reliable data transmission in the context of IEEE 802.15.4 is approximately -88 dBm [46]. Each neighbor will reply with its own ID. A database of the neighbor's information will be stored in the local cache to track each node and its behavior. Table I illustrates an example of the neighbor database created by the base station.

Neighbors	ID	Path
1	45	Direct
2	27	Direct
3	10	Direct
4	96	Direct
5	66	Direct

TABLE I. Neighbors Database.

Phase Two: Route Redistribution

The nodes that have been chosen by the base station will propagate their route information to their neighboring nodes. The primary goal of this stage is to establish a communication routes between the trusted node, equipped with a pathway to the base station, and its neighbor nodes that are located within their respective coverage zones as shown in figure 3. During the process of this phase, a virtual pie-shaped coverage area will be created by each sensor node as calculated by Equation (1).

$$A = \frac{R^2}{2}\left(\frac{\pi}{180}\alpha - sin\alpha\right) \qquad (1)$$

It is important to know that α is the searching angle in degrees which is fixed for all nodes in the network, R is the distance from the node to the boundary of its coverage area. The sensor node will send the route information to its neighbors that reside in the computing area where the area is centered around a straight line between the base station location $x \in A$ and the current source node. Therefore, in the route redistribution phase, the sensor node will send the route advertisement message which contains its location, route bath towards the base station, and preferred angle to redistribute the route to the next sensor nodes. By using a defined search angle to create the virtual pie-shaped coverage area, only the nodes within that area will respond to the source node which will reduce the overall node power consumption, as well as the memory usage. Therefore, each sensor node will build its own database to maintain the routing table.

The node that receive the route advertisement message will reply to the source with its ID which will be used to build a routing table in each node including its neighbor. This allows the base station to have full network topology information, and monitor the behavior of the sensor node and track the amount of data transmitted to identify if there is a security breach.

This process will be done in cycles to keep maintaining routing tables in each node. Whenever any node has data to transmit, it will use the routing table to send the packets. The route redistribution process is clarified in algorithm 1.

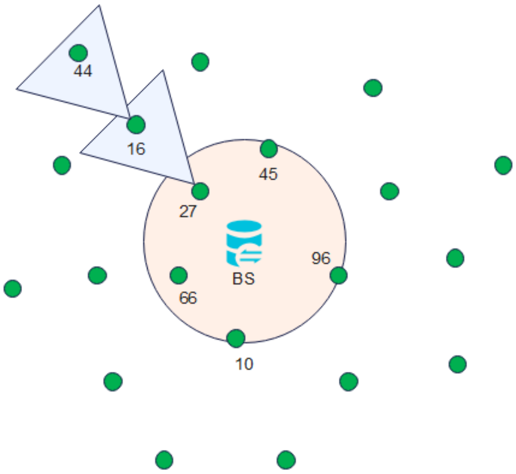

Figure 3. Route Redistribution

Algorithm 1: Pseudocode of area discovery phase in DRR protocol

```
Input: $nodeID,\ Node_{(x,y)},\ BS_{(x,y)}, node\ range\ transmission\ \alpha$
Output: find the connected nodes in the range $\alpha$ associated with
$Node_{(x,y)},\ Residual\ Energy\ (energy),\ Power\ Receive\ (Pr),\ Availability\ (AV)$.
For i ← 1 To $N$        //N is the total number of nodes in the WSN
$N\_Cur \leftarrow Node(i)$        //Node(i) is the current node ID
$TArea \leftarrow \left[\widehat{Node(i)}_{(x,y)}\ \frac{\alpha}{2},\ \frac{\alpha}{2}\ \widehat{NetEdge}_{(x,y)}\ \right]$        //the Transmission range is the area
from Node(i) to network edge
For $j \leftarrow 1$ To $Z$        //Z is the total number of nodes within the transmission range Tr
$N\_Can \leftarrow Node(j)$        //N(j) is the candidate node ID
If $N\_Cur \leftrightarrow N\_Can$ Then        //the connection established
    $PNodeID \leftarrow N(j)$        //the add node ID to potential next hope nodes
    $Pnode_{(x,y)} \leftarrow N(j)_{(x,y)}$        //the add node coordinates to potential next hope nodes
    energy ← $energy(j)$        //the add node residual energy to potential next hope nodes
    Pr ← $Pr(j)$        //the add node received power to potential next hope nodes
    $AV \leftarrow AV(j)$        //the add node availability status to potential next hope nodes
End If
End For
End For
```

Phase Three: Data Forwarding Phase

After completing phases one and two, the data source node will have its own routing table. Once the node has data to send, it will check it routing database for the potential next hope nodes. Based on the data shared by the potential next hope devices, such as the residual energy, the distance, the current node shall chose the best next hope as discussed below. Please not that the calculation of distance at the source node shall be performed by means of the Euclidean Distance Formula, as demonstrated in Equation (2). This calculation will create a temporary database to determine the best path, later on, the source node will prioritize the selected nodes N from the routing table depending on the shared which had been received information from the neighbors. Later on, the source node will erase the temporary routing table to maintain the memory resource of the node. We assume that the required time to complete phases 1 and 2 is smaller than the time required for the nodes to change their position due to mobility speed.

$$d(N_i, AP) = \sqrt{(Xp - X_i)^2 + (Yp - Y_i)^2} \qquad (2)$$

Algorithm 2: Pseudocode of node selection phase in DRR protocol.

```
Input: $nodeID$, $node_{(x,y)}$, $Residual\ Energy(energy)$, $Pr$, $Availability(AV)$
Output: find the connectivity between the nodes.
For $i \leftarrow 1$ To $Nodes$        // Nodes is the total number of nodes in the WSN
$N\_Cur \leftarrow N(i)$        //N(i) is the current node ID
For $j \leftarrow 1$ To M        //M is the total number of nodes within the transmission range
$\mathbf{energy_{avrg}} \frac{= \sum_1^z \mathbf{energy_i}}{\mathbf{z}}$        // the average of the residual energy for all Z nodes
Then Do While $i \neq j$
For $k \leftarrow 1$ To M
   $AV \leftarrow Max(AV(k))$
   If energy$(K) > energy_{avrg}$
   If $Pr(K) > \mathrm{Pr}_{threshold}$ Then        // node SNR exceed threshold
         $N\_Can(l) \leftarrow N(K)$
         l$\leftarrow l++$
      Else
         $AV(k) \leftarrow 0$
      End If
   Else
         $AV(k) \leftarrow 0$
   End If
   End For
For $l \leftarrow 1$ To M
   $dis \leftarrow Min(d\{N(l); Sink\})$
   If $dis = d\{N(l); Sink\}$ Then
         $N\_Can \leftarrow N(1)$        // N_Can is the list for next hope candidates after filtering
process
   End If
End While
End For
End For
```

After listing the available nodes, the source node will filter and prioritize them based on the residual energy PE_J and received power Pr_J level by using Equations (3 and 4)

$$PE_j > PE_{avrg} \tag{3}$$

$$Pr_j > Pr_{threshold} \tag{4}$$

According to [46], -88 dBm may enable reliable data transfer in IEEE 802.15.4 which was considered as $Pr_{threshold}$. After filtering the next hope nodes based on residual energy, the node with lowest distance to the source node will be selected as next hope in the data routing. Due to the nodes mobility and the change in the network topology, the senor nodes are expected to update their routing paths frequently and this can be configures in the proposed methodology by controlling the rate at which phase 1,2 and 3 are occurring.

C. Sinkhole Attack Detection

A. The first scenario we assume, after successful negotiation and route redistribution between the nodes, an illegitimate node will try to compromise the route of some nodes by sending its fake route information, figure 4 illustrates how node 52 tries to compromise node 44. The new node ID and its route information are not in the routing table as shown in table II , thus node 44 will reject the advertised route and won't send any packet to node 55, because route advertisement will be done on a cycle basis, thus all node will monitor the new routes advertisement at the beginning of each cycle.

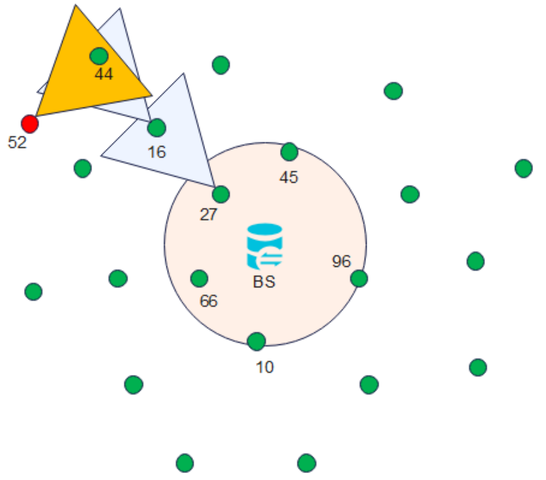

Figure 4. Scenario A

B. In the second scenario, the illegitimate node might enter the network in the early phases of network establishment, and it is added to the established routes as shown in figure 5. The attack might occur in this case, and the behavior of node 87 will be tracked by the base station. The amount of traffic generated from node 87 either will be 0 or low compared to the number of its clients for a specific time. In this situation, the base station will raise an alarm and send a message to the other sensor nodes in order to avoid and block the route through sensor node 87 and a notification will be sent to the network administrator. The route through node 87 will not be used till it is manually granted again by the network administrator.

C. In the third scenario, we assume illegitimate node 16 as shown in figure 6 will try to enter the routing table at any broadcast cycle with a clone ID. As clarified previously, the base station will have a full database of the network and connected node IDs. During any routing update cycle, the illegitimate node might successfully enter the network. In this scenario there will be duplicated record in the base station, the base station will send a broadcast message to all its neighbors to block the duplicated node and notify the network administrator about the attack.

Neighbors	ID	Path
1	27	27
2	44	client

TABLE II. Routing table of node 16

Neighbors	ID	Path
1	16	16-27

TABLE III. Routing table of node 44.

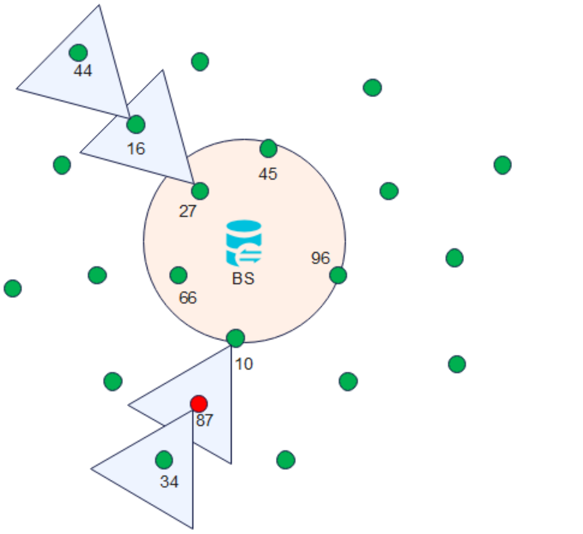

Figure 5. Scenario B

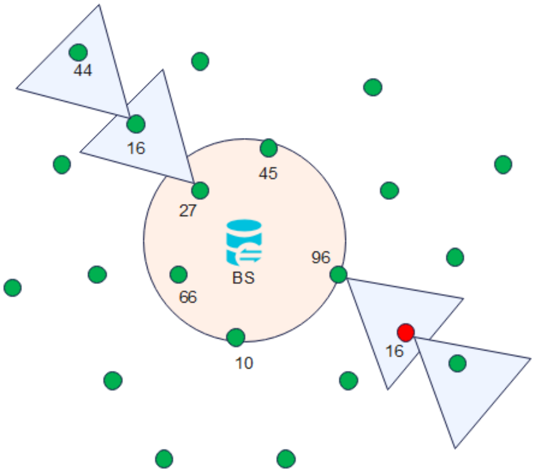

Figure 6. Scenario C

5. Simulation Results and Performance Analysis

A. Simulation Setup

In order to measure the performance of the proposed Sinkhole attack detection mechanism, a Monte-Carlo simulation is carried out using the Matlab tool. A total of 500 random network realizations are tested with random locations for the sensor devices. The reason behind having such a large number of network realizations is to achieve an accurate statistical result. Additionally, it is assumed that there are 100 devices in total, distributed throughout a two-dimensional geographic space of size 500m X 500m, with the assumption of single source-destination pair. The sensor nodes are moving within the aforementioned area with a mobility speed of 5 m/s, therefore, each network realization represents a shift in the sensor nodes' location based on the mobility speed assumed. It is worth mentioning also that the nodes are moving in random directions according to the Random-way point mobility model [47]. The energy consumption resulted from sending β bit data from node (i) to node (j) is calculated in equation (5):

$$(\epsilon_{fs} + \epsilon_{mp} D^2_{(i \leftrightarrow j)})\beta \tag{5}$$

$$E_r(j) = \epsilon_{fs}\beta \tag{6}$$

However, the energy consumption for receiving β bit data by node (j) is given by equation (6) [48]. Where ϵ_{fs} and ϵ_{mp} are the energy dissipated from the transmission and reception of one bit, and the free space amplification factor respectively. A summary of the simulation parameters is presented in table IV.

Parameter Definition	Symbol	Value
deployment area	-	500 m × 500 m
Number of nodes	M	100
Sink position	$Sink$	(0, 0)
Transmission power	Pt	2 dBm
Initial energy	E_i	0.05 Joules
Tx or Rx Transceiver energy	ϵ_{fs}	10 nJ/bit
Free space amplifier energy	ϵ_{mp}	0.0013 pJ/bit/m^2
Nodes velocity	V	5 m/s
Node radio sensitivity	-	-88 dBm
Number of malicious nodes	-	0,1,3

TABLE IV. Simulation Parameters.

B. Simulation Results

The evaluation of the detection method proposed herein is conducted with respect to three critical metrics, namely network lifetime, detection ratio, and energy consumption. Furthermore, a comparison between the results of the proposed security scheme and those of the Configurable Secured Adaptive Routing Protocol (CSARP) in [49] is done in order to establish a reliable benchmark. The CSARP protocol is designed for MWSNs, where the authors developed a (CSARP) that detects packet-dropping attacks. The (CSARP) protocol was inspired by the LEACH-mobile-enhanced and Mobility-based clustering (MBC) protocols.

1) Network Lifetime

Figure 7 represents the lifespan of the network based on the number of completed simulation cycles before all nodes expired by losing their energy reserve. The simulation is carried out for three different scenarios, which are zero, one, and three malicious nodes. The results are compared with the CSARP protocol, where it is clearly shown that our proposed DRR protocol extends the lifetime of the networks since it implements directional-based routing to constringe the energy consumption via eliminating redundant routing

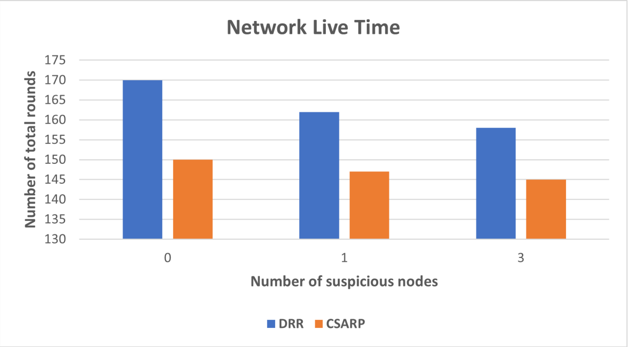

Figure 7. Network Lifetime

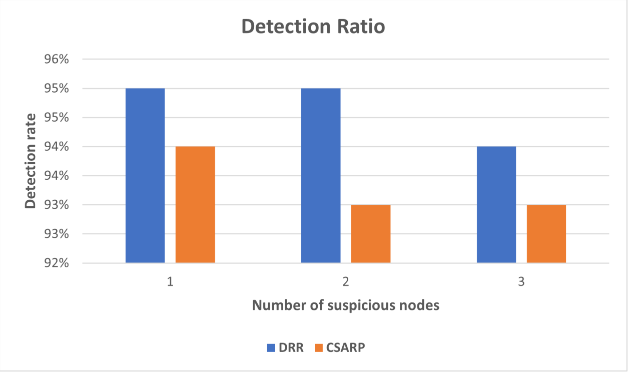

Figure 8. Detection Ratio

toward the base station and reducing the number of nodes that participate in the routing process by optimizing the routes. As shown in figure 7, the proposed DRR results in a longer lifetime for the sensor nodes as compared to the CSARP protocol, for example, when no malicious nodes assume, the total lifespan of the network is 170 cycles in DRR while it is 150 cycles in the CSARP protocol. When malicious nodes are injected into the network, a slight degradation in the lifetime is observed in the DRR protocol, some broadcast and alarm messages are sent by the base station to all nodes in the network to acknowledge suspicious nodes or routes in the network.

2) *Detection Ratio*

The present research encompasses an evaluation of a second metric, referred to as the detection ratio, whereby the ratio of detected malicious nodes out of the total number of 500 network realizations is determined. This metric aims to ascertain the percentage of identified malicious nodes relative to the total number of such nodes under consideration. the relation between the number of malicious nodes and the detection ratio is illustrated in figure 8. As illustrated in figure 8, even with the increase in the number of injected malicious nodes in the network, our proposed protocol is achieving consistent detection performance, therefore outperforming the CSARP protocol. For example, when two malicious nodes are injected into the network, 95% of the time, the nodes are detected by our protocol as compared to 93% in the CSARP protocol.

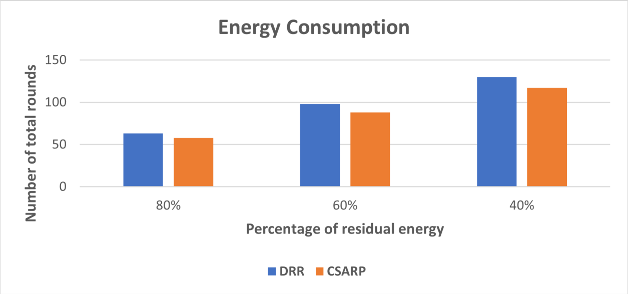

Figure 9. Energy Consumption

3) *Energy Consumption*

The present research evaluates transmission energy consumption as the third performance metric, which holds immense significance in both WSN and MWSNs, with a particular focus on networks that operate within the constraints of a limited supply of battery power. The metric is defined as the mean percentage of the remaining energy across all mobile sensor nodes in the network at every round interval as calculated in equations (5 and 6). figure 9 illustrates the total consumed energy by the proposed DRR as compared to the CSARP protocol. It is observed our proposed directional routing protocol is capable of reducing energy consumption. Please note that the results here are based on the assumption one malicious node is injected into the network.

C. *Simulation Limitation*

This study assumes a density of 100 nodes in an area of 500X500 m, where the increase in the node density can raise more challenges in relation to the route establishment between the base station and the sensor nodes. As the nodes get closer to each other's, the possibility of having multiple potential next hope will increase, which increase the possible routes that can be established. The study has also assumed a stationary base station, where a mobile base station might result in more frequent changes in the routes that can be established between the base station and the sensor nodes, which consequently makes the detection of sinkhole nodes more challenging.

6. Conclusion and Recommendations

A. *Conclusion*

Investigating MWSNs raises a variety of security issues. Mobility in MWSNs, in contrast to WSNs, increases the difficulty of securing the network against threats to its physical and data security. Attacks that disrupt network availability and data availability are one of these key issues. In addition, the lack of resources creates further difficulties. Investigating state-of-the-art information on MWSNs, security issues, security needs, threats and defenses, routing protocols, and related work is the primary objective of this research. Designing and developing a secure routing protocol to detect and mitigate Sinkhole Attacks in MWSNs is the other objective.

There is a lack of research on securing and mitigating techniques on MWSNs against Sinkhole attacks at the routing level. However, most of the available proposed solutions are designed for WSNs with specific configurations which are not applicable to some MWSNs application requirements. To secure MWSNs against Sinkhole attacks, a proposed routing protocol was designed and developed by using MATLAB software named Directional Routing Reflector Protocol (DRR). The proposed routing protocol is categorized as a dynamic routing protocol managed by the base station to detect and isolate the malicious sensor nodes while maintaining the availability of the network and reducing the energy consumption of the sensor nodes. Multiple simulations with various settings and situations were done for the proposed protocol to examine and analyze the protocol's efficiency at detecting and preventing processes. The performance evaluation of the proposed detection scheme is conducted based on the considerations of network lifetime, detection ratio, and energy consumption. The results are benchmarked by comparing them with the results of the CSARP performance Routing Protocol.

The proposed DRR has a longer network lifespan for the sensor nodes as compared to the CSARP protocol in the selected three conditions, no malicious node, one malicious node, and three malicious nodes by around 10%. Also, DRR showed a slight improvement in detection ratio compared to the CSARP protocol. Lastly, DRR showed that it is able to maintain and minimize energy consumption, compared to the consumed energy in the CSARP protocol, a simulation done with the assumption of one malicious node in the network. When comparing the proposed security scheme to the CSARP protocol, which has already been proven to be superior to existing security solutions in [49], the proposed protocol has shown superior performance.

B. Recommendations and Future Work

The proposed protocol has proven that it is capable to detect and mitigate Sinkhole attacks more effectively than the other solutions while maintaining the network lifetime and transmission energy consumption besides increasing the detection ratio, our recommendation is to consider DRR to be used as the routing protocol for all MWSNs.

For future work, further investigation will be done to add more security techniques to enhance the security against Sinkhole attacks and prevent other different types of attacks. The below points are intended to conduct some future work including:

1) Utilize secret keys to exchange routing information between MWSN nodes.
2) Encryption and hashing techniques could be considered by using lightweight algorithms to maintain good network performance.
3) The speed of the sensor nodes could be considered as multi-speed instead of one-speed.
4) The location of the base station will be considered as a mobile to ensure that the DRR is applicable for most of the MWSN applications.

References

[1] dosits, "Sound surveillance system (sosus)," *Discovery of Sound in the Sea*, Oct 2021. [Online]. Available: https://dosits.org/galleries/technology-gallery/locating-objects-by-listening-to-their-sounds/sound-surveillance-system-sosus/

[2] S. Laboratories, "The evolution of wireless sensor networks - silicon labs," *silabs*, 2013. [Online]. Available: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf

[3] O. Khalaf and B. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Journal of Computational and Theoretical Nanoscience*, vol. 7, pp. 1096–1101, 07 2019.

[4] R. Silva, J. Sá Silva, and F. Boavida, "Mobility in wireless sensor networks — survey and proposal," *Computer Communications*, vol. 52, 10 2014.

[5] G. Kibirige and C. Sanga, "A survey on detection of sinkhole attack in wireless sensor network," *International Journal of Computer Science and Information Security*, vol. 13, pp. 1–9, 05 2015.

[6] G. S. Sara and D. Sridharan, "Routing in mobile wireless sensor network: A survey," *Telecommunication Systems*, vol. 57, no. 1, pp. 51–79, 2014.

[7] N. Swarna, A. H. Srinivasa, H. C. Harishkumar, R. Ait, and B. Arathi, "Flat based network routing protocol in wireless sensor network," *INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY*, vol. 3, 2015.

[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks," in *Proceedings of the 6th annual international conference on Mobile computing and networking*, 2000, pp. 56–67.

[9] N. A. Pantazis, S. A. Nikolidakis, and D. D. Vergados, "Energy-efficient routing protocols in wireless sensor networks: A survey," *IEEE Communications surveys & tutorials*, vol. 15, no. 2, pp. 551–591, 2012.

[10] L. K. Ketshabetswe, A. M. Zungeru, M. Mangwala, J. M. Chuma, and B. Sigweni, "Communication protocols for wireless sensor networks: A survey and comparison," *Heliyon*, vol. 5, no. 5, p. e01591, 2019.

[11] S. M. T. U. Kumar, Prabhat, "A review of routing protocols in wireless sensor network," *International Journal of Engineering Research & Technology (IJERT)*, vol. 1, no. 4, pp. 1–14, 2012.

[12] O. Mezghani and M. Abdellaoui, "Improving network lifetime with mobile leach protocol for wireless sensors network," in *2014 15th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering (STA)*. IEEE, 2014, pp. 613–619.

[13] A. Kumar, H. Y. Shwe, K. J. Wong, and P. H. Chong, "Location-based routing protocols for wireless sensor networks: A survey," *Wireless Sensor Network*, vol. 9, no. 1, pp. 25–72, 2017.

[14] R. Chaudhary and D. S. Vatta, "A tutorial of routing protocols in wireless sensor networks," *International Journal of Computer Science and Mobile Computing*, vol. 3, no. 6, pp. 971–979, 2014.

[15] M. A. Matin, *Wireless sensor networks: Technology and protocols*. BoD–Books on Demand, 2012.

[16] N. Shabbir and S. R. Hassan, "Routing protocols for wireless sensor networks (wsns)," *Wireless Sensor Networks-Insights and Innovations*, pp. 36–40, 2017.

[17] P. J. Sallis, *Wireless Sensor Networks: Insights and Innovations*. BoD–Books on Demand, 2017.

[18] A. Dwivedi and O. Vyas, "Network layer protocols for wireless sensor networks: existing classifications and design challenges," *International Journal of Computer Applications*, vol. 8, no. 12, pp. 30–34, 2010.

[19] 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.

[20] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428)*, vol. 3. IEEE, 2003, pp. 1976–1986.

[21] S. A. Ch, Z. Mehmood, D. R. 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.

[22] 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.

[23] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proceedings of the 9th ACM Conference on Computer and Communications Security*, 2002, pp. 41–47.

[24] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *2003 Symposium on Security and Privacy, 2003.* IEEE, 2003, pp. 197–213.

[25] 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, pp. 43–52.

[26] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," *ACM Transactions on Information and System Security (TISSEC)*, vol. 8, no. 1, pp. 41–77, 2005.

[27] 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.

[28] S. Karthik and A. A. Kumar, "Challenges of wireless sensor networks and issues associated with time synchronization," in *Proceedings of the UGC sponsored national conference on advanced networking and applications*, 2015, pp. 19–23.

[29] 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, 2013.

[30] 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, pp. 97–106.

[31] S. Sudheendran, O. Bouachir, S. Moussa, and A. O. Dahmane, "Challenges of mobility aware mac protocols in wsn," in *2018 Advances in Science and Engineering Technology International Conferences (ASET)*. IEEE, 2018, pp. 1–6.

[32] M. Burhanuddin, A. A.-J. Mohammed, R. Ismail, M. E. Hameed, A. N. Kareem, and H. Basiron, "A review on security challenges and features in wireless sensor networks: Iot perspective," *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, vol. 10, no. 1-7, pp. 17–21, 2018.

[33] M. N. Riaz, A. Buriro, and A. Mahboob, "Classification of attacks on wireless sensor networks: A survey," *International Journal of Wireless and Microwave Technologies*, vol. 8, no. 6, pp. 15–39, 2018.

[34] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks manets," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 28–33.

[35] I. Butun, P. Österberg, and H. Song, "Security of the internet of things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[36] M. Wazid, A. K. Das, S. Kumari, and M. K. Khan, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 17, pp. 4596–4614, 2016.

[37] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Algorithmic Aspects of Wireless Sensor Networks.* Berlin, Heidelberg: Springer Berlin Heidelberg, 2008, pp. 150–161.

[38] I. Krontiris, T. Giannetsos, and T. Dimitriou, "Launch sinkhole attack in wireless sensor network; the intruder side," in *IEEE International Conference on Wireless and Mobile Computing*. IEEE, 2008, pp. 526–531.

[39] V. Tumrongwittaya, "Detection of sinkhole attack in wireless sensor networks," in *ICCAS-SICE*. IEEE, 2009, pp. 1966–1971.

[40] C. Chen, M. Song, and G. Hsieh, "Intrusion detection sinkhole attack in large scale wireless sensor network," in *Wireless Communication, Networking and Information Security (WCNIS), 2010 IEEE Interational Conference on*. IEEE, 2010, pp. 711–716.

[41] D. S. Roy, A. S. Singh, and S. Choudhury, "Countering sinkhole and blackhole attacks on sensor networks using dynamic trust management," in *Computers and Communications*. IEEE, 2008, pp. 537–542.

[42] L. Coppolino, S. Antonio, L. Romano, and G. Spagnuolo, "An intrusion detection system for critical information infrastructures using WSN technologies," in *Critical Infrastructure (CRIS), 2010 5th International Conference on*. IEEE, 2010, pp. 1–8.

[43] A. Papadimitriou, L. F. Fessant, and C. Sengul, "Cryptographic

protocols to fight sinkhole attacks on tree based routing in WSN," in *Secure Network Protocols*. IEEE, 2009, pp. 43–48.

[44] J. Adams, "An introduction to ieee std 802.15.4," in *2006 IEEE Aerospace Conference*, 2006, pp. 8 pp.–.

[45] A. G. Ramonet and T. Noguchi, "Ieee 802.15.4 historical evolution and trends," in *2019 21st International Conference on Advanced Communication Technology (ICACT)*, 2019, pp. 351–359.

[46] W.-S. Jang and W. M. Healy, "Wireless sensor network performance metrics for building applications," *Energy and Buildings*, vol. 42, no. 6, pp. 862–868, 2010.

[47] T. Camp, J. Boleng, and V. Davies, "A survey of mobility models for ad hoc network research," *Wireless communications and mobile computing*, vol. 2, no. 5, pp. 483–502, 2002.

[48] T. Amgoth and P. K. Jana, "Energy-aware routing algorithm for wireless sensor networks," *Computers Electrical Engineering*, vol. 41, pp. 357–367, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0045790614001888

[49] A. Alnaser, H. Al-Junaid, and R. Almesaeed, "Configurable secured adaptive routing protocol for mobile wireless sensor networks," *International Journal of Electronics and Telecommunications*, vol. vol. 68, no. No 3, pp. 577–586, 2022. [Online]. Available: http://journals.pan.pl/Content/124269/PDF-MASTER/17-3497-12090-1-PB.pdf

Ali Maki Alaali Received his BE degree in Information Communication Technology from Bahrain Polytechnic, Bahrain. He is currently working as IP core and SDWAN Operation team leader at Kalaam Telecom, Seef, Bahrain.

Dr. Reham Almesaeed Assistant Professor Computer Engineering Department IT College-University of Bahrain Bahrain