IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 15, 2020, accepted March 16, 2020, date of publication March 26, 2020, date of current version April 15, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983438

Centralized Routing Protocol for Detecting Wormhole Attacks in Wireless Sensor Networks

OHIDA RUFAI AHUTU AND HOSAM EL-OCLA, (Senior Member, IEEE)
Department of Computer Science, Lakehead University, Thunder Bay, ON P7B 5E1, Canada
Corresponding author: Hosam El-Ocla (hosam@lakeheadu.ca)

ABSTRACT Nodes in wireless sensor networks (WSN) are resource and energy-constrained because they are generally batteries powered and therefore have limited computational capability. Due to the less secure environment in WSN, some malicious nodes at one point can tunnel packets to another location to damage the network in terms of packets dropping and eavesdropping and this is a so-called wormhole attack. Many of the current protocols solve the wormhole attack problem in isolation from the node energy consumption. However, some other proposed solutions consider reducing the energy consumption to detect such attacks but still it is needed to probe better performance. In this paper, we present a lightweight multi-hop routing protocol for 802.15.4 WSN that aims to minimize the energy consumption and also to detect the wormhole attacks. Simulation results prove that our MAC Centralized Routing Protocol (MCRP) outperforms other existing similar protocols.

INDEX TERMS Wireless, sensor, networks, MAC, routing, wormhole, attack, centralized, energy, consumption, 802.15.4.

I. INTRODUCTION

A wireless sensor network consists of a large number of low-power multi-functioning sensor nodes with limited sensing and computational capabilities deployed to monitor different types of physical or environmental phenomenon. These sensor nodes operate in an unattended mode as they are typically deployed in hostile environments with no means of renewing their energy source supplied by batteries [1]. WSN has wide application possibilities, such as temperature, pressure, humidity, and habitat monitoring, disaster management, military reconnaissance, forest fire-tracking, building automation, security surveillance and many more [2]–[5].

The infrastructure-less nature of WSN makes it flexible in terms of ease of deployment and multiple functionalities. However, this also makes it vulnerable to security threats and attacks. A Wormhole Attack occurs when an attacker creates a tunnel between distant locations in the network through an in-band or out-of-band channel to capture or reply to ongoing frames. The wormhole tunnel gives two distant nodes the illusion that they are close to each other [6]. A wormhole attack is regarded as one of the most severe and sophisticated security threats to WSN due to its man-in-the-middle characteristics where an attacker does not necessarily have to destroy the integrity-based communications or the network structure, thereby making it difficult to prevent and detect [7].

In this article, we propose a centralized-based routing protocol called MAC Centralized Routing Protocol (MCRP) for 802.15.4 wireless sensor network (WSN). MCRP utilizes a high-energy BS to calculate and deliver routing paths, monitor the network topology and perform other energy-intensive tasks. MCRP is a reactive routing protocol. Therefore, routes are determined only when needed. The main ideas in MCRP are the implementation of centralized network intelligence in one component via the BS to reduce energy consumption while maximizing the MAC routing efficiency and utilization of the consensus between sensor nodes and BS. Through this consensus, MCRP can detect efficiently wormhole attacks. In this regard, our proposed algorithm uses an end-to-end time delay between sensor nodes and the BS to pinpoint links that are potentially under wormhole attacks and in turn be avoided in the shortest path. The performance evaluation shows that MCRP improves the network scalability in terms of energy consumption, end-to-end delay, throughput and frame delivery ratio over its comparatives.

The associate editor coordinating the review of this manuscript and approving it for publication was Pierluigi Gallo.

The remaining sections of the paper are structured as follows: Section II presents a literature review. Section III outlines the proposed protocol. Section IV describes the methodology. Section V explains the simulation setup and results. Section VI draws on the conclusions.

II. LITERATURE REVIEW

Many algorithms, techniques and protocols have been proposed to improve the overall performance of WSN, some of which require specialized hardware or incur high communication overhead. Data-centric routing is a commonly utilized approach. Here, sensor nodes broadcast an advertisement describing the available data and wait for a request from an interested neighbor before sending the actual data [8]. The entire Sensor Protocols for Information via Negotiation (SPIN) [9] protocol family and Directed Diffusion (DD) [10] are based on data-centric routing. In SPIN, the sensor nodes that have data to send firstly broadcast an advertisement containing information about the data and then transmit the actual data only to interested nodes. To solve overlap and reduce the energy consumption incurred during the broadcast of advertisements, the SPIN protocol family (SPIN, SPIN-PP, SPIN-BC, SPIN-EC, SPIN-RL) [11] uses meta-data as a descriptor in the data dissemination based on the data received. Furthermore, to adjust the resource consumed adaptively, SPIN uses the negotiation between nodes to avoid the redundancy of data and thus reducing unnecessary data transmission. Directed Diffusion, however, uses a slightly different type of data-centric routing. In DD routing, data propagation, gradients, interests, reinforcements and data naming are the significant components for data dissemination. The sink broadcasts interest to the sensor nodes, which subsequently return their gradient to the sink. This is used to establish the path from source to sink and also to determine the relay of data to avoid routing loops. The data naming mechanism maps the task with attributes such as range and interest and this helps the neighbor nodes with deciding how to forward data. Reinforcement is used to determine the links for acquiring high-quality events. Overall, the data-centric routing approach can improve the robustness and scalability of wireless sensor networks but it suffers from a large amount of overhead energy spent on activities such as advertising and gradient setup. Moreover, the delay incurred during these activities may not suit some real-time applications that require nodes to respond in real-time [12]–[14]. To solve this problem, a clustering-based protocol was proposed in [15]. In the clustered routing approach, sensor nodes are grouped into clusters where dedicated cluster heads (CH) collect, aggregate and forward data from all sensor nodes within its cluster to the Base Station (BS). This helps to reduce the amount of data that needs to be transmitted. In general, the clustering-based protocol improves bandwidth reusability, enhances resource allocation and improves power control [16]. However, conventional clustering protocols do not improve network lifetime because it assumes the CH to be high-energy nodes and fixed which is not necessarily true in all WSNs. To solve this deficiency, an adaptive clustering protocol called Low-Energy Adaptive Clustering Hierarchy (LEACH) was proposed in [17]. The main objective of LEACH is to reduce energy consumption by pseudo-randomly rotating the role of CH among all nodes in the network. The operation of LEACH consists of multiple rounds where each round is divided into two phases: the set-up phase and the steady-state or transmission phase. During the set-up phase, nodes organize themselves into clusters and each node participates in a CH election process by generating a random priority value. Nodes with generated random number less than a predetermined threshold value become CH. A node cannot participate in consecutive CH elections. In this way, every node gets a chance to become the CH and energy consumption among the nodes is uniformly distributed. During the transmission phase, the elected CH gathers data from sensor nodes within their respective clusters and performs data aggregation before sending the sensed data to the BS.

LEACH reduces intra-cluster collision and energy consumption by using a Time Division Multiple Access (TDMA) schedule whereby sensor nodes within a cluster only send data to the CH during their allocated time slot. When a particular sensor node is sending data to the CH during its allocated time slot, other member nodes of the same cluster will remain in a sleep state. Transmission of data from CH to the BS is also performed with the use of the selected TDMA schedule. Thus, LEACH reduces energy consumption and increases the network lifetime over fixed clustering and other traditional routing protocols.

A centralized version of LEACH, called LEACH-C was proposed in [16]. LEACH-C utilizes the BS for CH selection and cluster formation. The BS receives information about location and energy level from sensor nodes during the setup phase. Based on this information, the BS elects CH and configures the network into clusters. Therefore, there is no overhead for sensor nodes during the formation of clusters since the setup phase is completely executed at the BS. This is unlike LEACH where nodes self-configure themselves into clusters. To create efficient clusters, LEACH-C presumes that there is a uniform distribution of energy among all sensor nodes. The BS decides that those nodes having an energy level less than that average energy level are prohibited from participating in the CH selection process for the current round. The BS then broadcasts the node ID of the selected CH to the network. Selected CH sends an advertisement message to all nodes and those nodes that are not cluster heads determine the cluster they belong to based on the strength of the message signal received from the CH. Although other functions of LEACH-C are similar to LEACH, results presented in [17] indicate improvement over LEACH. Wormhole attacks are among the severest and sophisticated security threats to WSN routing protocols where an attacker strategically places its malicious node in a strong position. This node establishes a tunnel with better metrics to distort the network topology and relay frames selectively using the false

established routes. Wormhole attacks are very challenging to defend against and are hard to detect because they use private and out of the bound channel between two nodes. Methods in [18], [19] were proposed to avoid the wormhole attack where these algorithms rely on the utilization of the information on the nodes' locations. In [18], it was introduced a mechanism assumes that a possibility of having a real route with a small number of nodes will never occur when a wormhole attack exists and this is not always a realistic assumption. In [19], it was introduced the concept of packet leashes that can be considered either temporally or geographically, however, this approach delimits the maximum distance that a packet can take in the transmission. In [20], [21], it was presented solutions to detect the wormhole attack based on node localization as well. The main concern about these methods is the consumption of an excessive amount of energy needed for node localization. Even the method in [20] is incapable of defending the network against the wormhole attack completely. In [22], another mechanism to detect the wormhole was introduced using the analysis of the compression header data particularly when there is a combination of various types of attacks. This method lacks efficiency as it consumes more energy and memory compared to other algorithms and therefore, the lifetime of nodes will be limited. Authors in [23] introduced a mechanism to work in a multi-rate network. This proposed protocol also consumes an excessive amount of energy as each node has to observe the status of its neighbors over the packet forwarding time. Also this mechanism makes each node be engaged in a heavy calculation of the processing, queuing and channel access times and this, in turn, would reduce greatly the lifetime of the node. In [24], a solution was proposed utilizing a graph model to calculate the connectivity between neighbor nodes. The major drawback of this technique is when the graphical configuration does not support a connectivity model. The mechanism in [25] is based on the signature and recommendation trust protocol. This mechanism shows efficient performance; however, it needs to go through several evaluation processes to detect the wormhole attack and this in turn slows down the response of the algorithm. Authors in [26] presented a technique based on a graph approach where if the assumptions of the proposed solution parameters are not valid in a real deployment, that would result in wormhole detection failure. Also, some other recent solutions presented in [27]–[29] use nodes connectivity considering ideal parameter presumptions that won't be applicable in real networks. Authors in [30]–[32] presented useful solutions that use neighboring approach, however, their wormhole detection methods are not comprehensive and hard to implement. Another solution presented in [33] depends on the neighboring approach and requires extravagant overhead that likely results in several traffic problems such as congestion. Also, another mechanism suggested a solution in [34] to utilize a combination of energy, routes traffic rate, number of nodes and nodes trust to select the optimum path avoiding wormhole attackers; however, this algorithm would add overhead to the network. It was introduced a solution in [35] based on several impractical assumptions such as negligible queueing delay where it cannot be neglected in case of an overloaded network. Also this method assumes having no packet loss where it is unlikely to happen particularly in a noisy environment. In [36], the proposed algorithm is an approximated approach that has a limited range of implementation. Another approach in [7] uses distributed systems and their proposed wormhole detection capability lacks energy consideration. Other solutions consider the time delay computations such as in [37], [38] whereas they are not commonly verified.

In [39], authors have shown the popularity of some routing protocols in wireless networks amongst the academic community. Presented statistics prove that hundreds of authors use specific authenticated and verified protocols to compare network performance. Accordingly, implementations using these protocols are trusted and have no faults. These protocols include as follows: Adhoc On-Demand Distance Vector (AODV) [40], Optimized Link State Routing (OLSR) [41] and Destination-Sequenced Distance-Vector Routing (DSDV) [42]. In [43], it was proposed a secured AODV (SAODV) to detect a wormhole attack. This protocol reduces the energy consumption slightly compared to the original AODV at the expense of the time delay and throughput.

The primary drawbacks of the aforementioned mechanisms include the excessive amount of consumed energy to find a route, assumption of nonrealistic parameters, limited range of the protocol applicability and lack of complete wormhole attack detection. As a result of the shortcoming of these protocols, we propose a routing algorithm that would detect the wormhole attack without performance degradation in the sense of energy consumption and data throughput. To preserve the consumed energy particularly needed in WSN, sensor nodes won't be heavily involved in finding the route as this would be the responsibility of the BS using our algorithm. Therefore, the proposed mechanism is designed to avoid the long latency in finding the shortest path. In the meantime, our technique selects a secured routing path in which it detects the wormhole nodes tunnel. Consequently, this protocol maximizes the throughput compared to the other protocols while it does not require any special hardware.

III. PROPOSED PROTOCOL

A. PROBLEM STATEMENT

The service life of each node in WSN is relevant to the life cycle of topology and the overall network lifetime, i.e., resource limit, battery power, physical damage and other factors. Thus, reducing energy consumption and detecting wormhole attacks are the primary goals of our research. Nodes in WSN generally run on a limited battery and its depletion has been identified as one of the principal causes of lifetime limitation of these networks. Physically replacing batteries regularly is impractical especially in large networks or impossible in hostile environments [7].

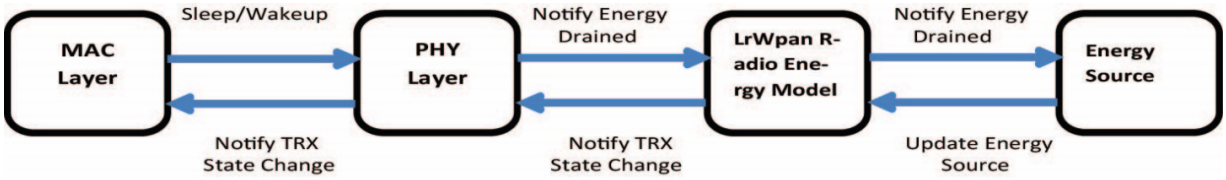

FIGURE 1. Notification of device state change in NS-3.

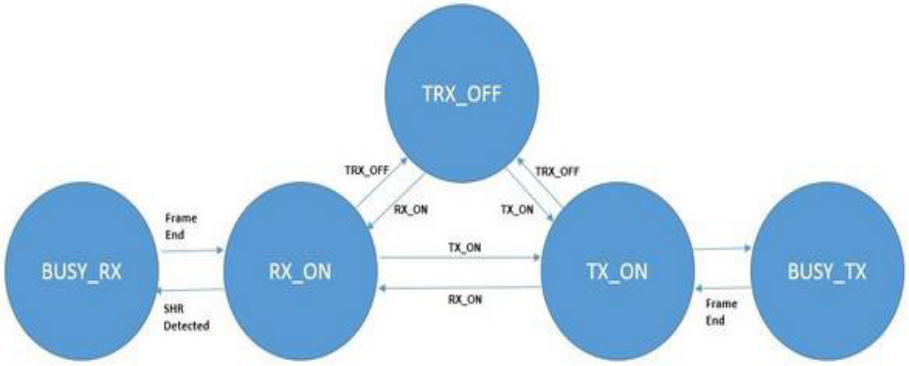

FIGURE 2. Relationship amongst device states in NS-3.

Therefore, a routing protocol that considers all energy consumption sources and also considers various scenarios that occur during the communication process is required.

B. PROPOSED SOLUTION

In this section, we describe how MCRP works. We will specify some assumptions in our sensor network. Then, we propose the concept of Time Ratio Threshold to detect wormhole links in the network. The foundation of MCRP is based on a single BS, which is a high-energy node with an unlimited amount of energy supply. Thus, MCRP employs the BS to facilitate network management to improve the performance of establishing a routing path from the source nodes to the sink. In this paper, we assume a model, with the following properties:

- Routing: The BS is tasked with calculating and delivering the routing path to sensor nodes. Hence, the sensor nodes do not need to search for routes as they make use of the data path in the flow table provided by the BS. The route calculation is based on the minimum number of hops.
- Energy Consumption: The sensor nodes are equipped with power control capabilities to adjust their power depending on the state. The state of senor nodes will switch between a Transmitter disabled (TRX_OFF), Transmitter enabled (TRX_ON), Transmitter busy (BUSY_TX), Receiver enabled (RX_ON) and Receiver busy (BUSY_RX) to conserve energy. Figure 1 and Figure 2 show the process of state changes in NS-3.
- Security: Our protocol is designed to detect wormhole attacks using the end-to-end time delay calculation.
- Data: The data structure in our design is majorly considered for the hand-shake-process, which includes assistant messages, a cache table and a flow table.
- Assistant messages, i.e., HELLO, Routing Information Message (RIM) and CONFIRM are exchanged to establish the routing path from source nodes to the BS and to deliver the flow table from the BS to the sensor nodes.
- All sensor nodes have similar communication range and are immobile.

C. TIME RATIO THRESHOLD

To detect wormhole attacks, we use a simple nonetheless effective technique by employing the consensus between sensor nodes and the BS. We propose a Time Ratio Threshold to compare the expected time for a frame to travel from the source to the destination (T_c) against the actual measured time taken for a frame to travel from the source to the destination (T_m). If a frame travels through a wormhole link, the instant ratio of T_c and T_m would be less than the average ratio of T_c and T_m. That is:

$$T_{ci} = \frac{Hops * Dist}{SoT} + \frac{SFL + RFL}{DR} + TQE * Hops \quad (1)$$

$$T_{ca} = \frac{\sum_{i=1}^{n} T_{ci}}{n} \quad (2)$$

$$T_{ma} = \frac{\sum_{i=1}^{n} T_{mi}}{n} \quad (3)$$

where

$Hops$ = Number of intermediate nodes through which data must pass between source and destination

$Dist$ = Distance between two nodes

SoT = Speed of transmission
SFL = Sending frame length
RFL = Receiving frame length
DR = Data rate
QET = Queuing and Execution time at each node

MCRP is used to detect wormhole attacks and in doing this, we apply the ratio below (eq 4). If the instant ratio is less than the average ratio then there is a wormhole link in the network and this link will not be considered in the path selection.

$$\frac{T_{ci}}{T_{mi}} < \frac{T_{ca}}{T_{ma}} \tag{4}$$

where

T_{ci} = Calculated time for a frame to travel from source to destination per request

T_{ma} = Sum of measured time taken for a frame to travel from the source to the destination over the number of requests (n)

T_{mi} = Measured time for a frame to travel from source to destination per request

T_{ca} = Sum of calculated time for a frame to travel from source to destination over the number of requests

IV. METHODOLOGY

MCRP is a centralized wireless sensor routing protocol with the BS being an essential component with high computational, energy and communications resources. Therefore, reducing energy consumption and detecting wormhole links in sensor nodes is the core of our research. As a prelude, Figure 4 depicts the components and their relationship developed based on NS-3. As seen in Figure 4, the LrWPAN interface is placed between the layer 2 and layer 3 protocols to send and receive frames. The major components in layer 2 are listed below. This includes the setup phase where the source node is requesting a route to the BS ending up by a CONFIRM packet containing the routing information. This phase is on-demand and therefore saves the energy consumption of the nodes batteries. As indicated below, we rely on the time tracking system to be used in the wormhole attack algorithm.

1. Data Transmission Request: Sender checks its routing table to find the address of the next hop. If no result is returned, it calls the function Broadcast HELLO.
2. Broadcast HELLO: Sender constructs a HELLO message, where it inputs the position vector, MAC address, power level and a KEY. The KEY uses the current time and the MAC address to identify the message and to avoid redundancy. This process starts with sensor nodes broadcasting HELLO packets to their neighbors via multicasting to MAC addresses of the source node's neighbors.
3. Receive HELLO: Hello message received by any node would be parsed, and then it caches the MAC address and saves the route to neighbors. Intermediate nodes search the path to the BS from their routing tables. If the path exists, they call the component of unicast RIM; otherwise call Broadcast HELLO.
4. Unicast RIM (Routing Information Message): Nodes having a path to the BS send a unicast RIM to the original sender where RIM uses the IEEE 802.15.4 MAC frame format. However, malicious nodes will send a counterfeit RIM representing a tunnel, in which the number of hops is smaller than other possible routes. Nevertheless, the BS will detect the malicious node as explained in point 6.
5. BS RESPONSE: The BS will send a unicast CONFIRM message to the original sender. Whenever the BS receives a HELLO message during the initialization phase or at any time, it should return the CONFIRM message with the RIM.
6. RIM CALCULATION: RIM is sent back to the source node, requesting a route to the BS, by intermediate nodes or BS. When RIM is calculated by the BS, two constraints are considered in-order:
   - Constraint one: Security of the path which is calculated based on eq (4) to examine if the path has a wormhole attack or not.
   - Constraint two: Minimum number of safe hops where the BS selects the safe path with the least number of hops.
7. Receive RIM: The original sender receives RIM from intermediate nodes with routing information.
8. Data Transfer: Once the sender receives RIM from its neighbor node, it selects the path with a minimum number of secured hops avoiding the malicious nodes tunnel.
9. Energy Model: The model is developed according to the MCRP design and based on the tracing system in NS-3. MCRP protocol reduces the energy dissipation in data transmission. This would be through minimizing the energy consumption needed in the routing setup phase that is triggered on demand.
10. Frame Format: Figure 3 shows the frame format in MCRP. The format mainly consists of six categories: Sequence, Hops, Type, Original address, Timestamp and Data.
    - Sequence number: This is used to identify frames to avoid redundancy. Due to retransmissions, multiple frames with the same sequence number could arrive at a destination. In this case, the receiver will take only the first frame and ignore the succeeding ones.
    - Hops count: This contains information about the number of intermediate nodes through which a frame must pass between a source and its destination. During the setting up of routes, this field is used for comparison of the shortest path to the BS, since nodes can get multiple messages from various directions.
    - Type: This indicates the relevant function of a frame. There are mainly 4 types designed in this paper, i.e., HELLO, RIM, CONFIRM and DATA.

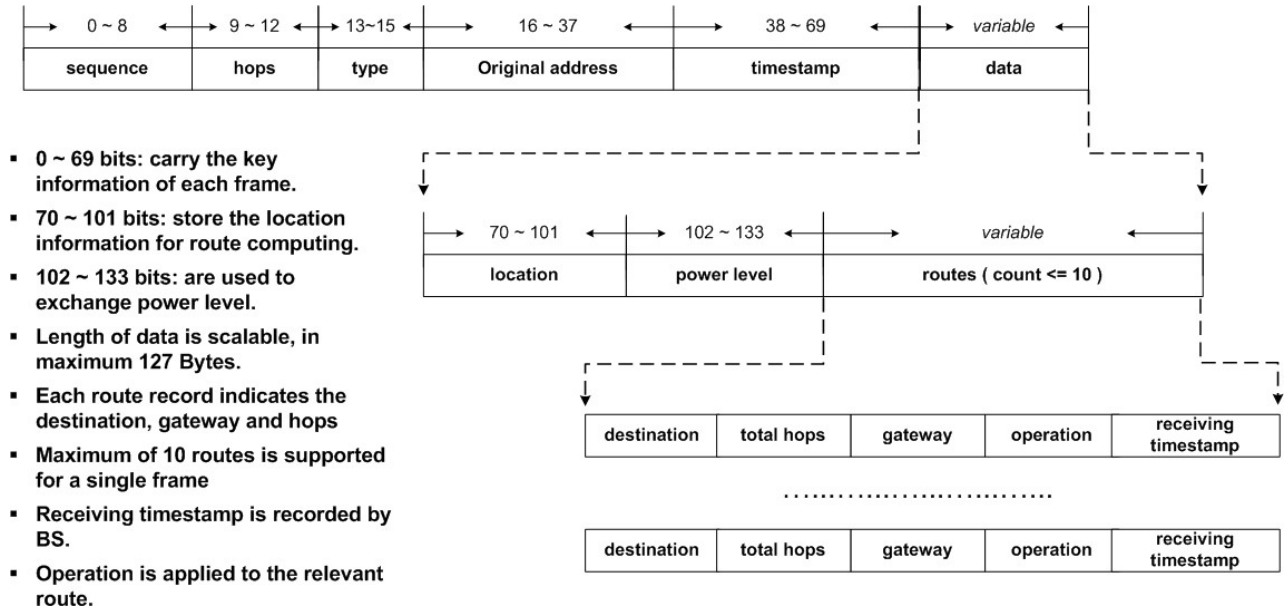

FIGURE 3. Frame format.

Except DATA, all the other types of frames are used for building the routing tables.

- Source address: This contains the address of the initial sender in order to inform the receiving node of its own destination in the reverse direction. For example, the BS can extract this field and return RIM or CONFIRM directly back to the original sender. Hence, this can reduce the overhead for communication.
- Timestamp: This is designed to record the sending time of a frame. Moreover, together with sequence number and original address, the timestamp is used to identify a unique frame. Furthermore, because the sequence number cannot infinitely increase, i.e., multiple senders can generate the same sequence number. The timestamp allows the sequence number to be reused internally.
- Data: This is the longest field for carrying the contents of a frame. Besides delivering the sensed data, the data field can be used in exchanging routing messages. The preceding fields mostly focus on controlling the transmission but the data field can store main content of routing messages like location, power level and routing information.
- Location: This indicates the position of sensor nodes.
- Power level: This indicates the transmitting power consumed by the original sender. The BS takes the power level and location out of the data field to make energy efficient decisions. Based on the location, the BS adjusts its power and sends the reply messages back to the original sender.
- Route: This carries the routing path from the sensor nodes to the BS. Each routing path contains information about the destination, total hops, gateway, operation and receiving timestamp.
  - Destination address: is the address of BS.
  - Total hops: This represents the total number of hops from the sensor node to the BS.
  - Gateway: This is the next hop to the sender.
  - Operation: This is used to inform the sensor nodes of adding, updating or deleting routes in its routing table.
  - Receiving timestamp: This is recorded at the BS once the related frame is received. This timestamp is majorly used for the detection of wormhole attacks, as it can be used in the calculation of end-to-end time delay between a sensor node and the BS.

11. Algorithms: The algorithms are categorized into two main functions; setting up routing paths and detection of wormhole attacks at the BS. Algorithm 1 is used by every node in the network to create routing paths. Nodes without a path to the BS broadcast Hello frames and nodes with a path reply by forwarding a routing information message (RIM) to the requesting node. However, if the BS receives the Hello frame, it returns a CONFIRM and a RIM directly to the requesting node. Algorithm 2 is used by the BS to detect wormhole links via the aforementioned time ratio threshold to detect wormhole attacks. Parameters' assumptions needed for simulation experiments are listed in algorithm 2. This algorithm calculates and compares the instant ratio with the average ratio. If the instant ratio is greater than the average ratio, then the link is safe; otherwise, there is a wormhole attack.

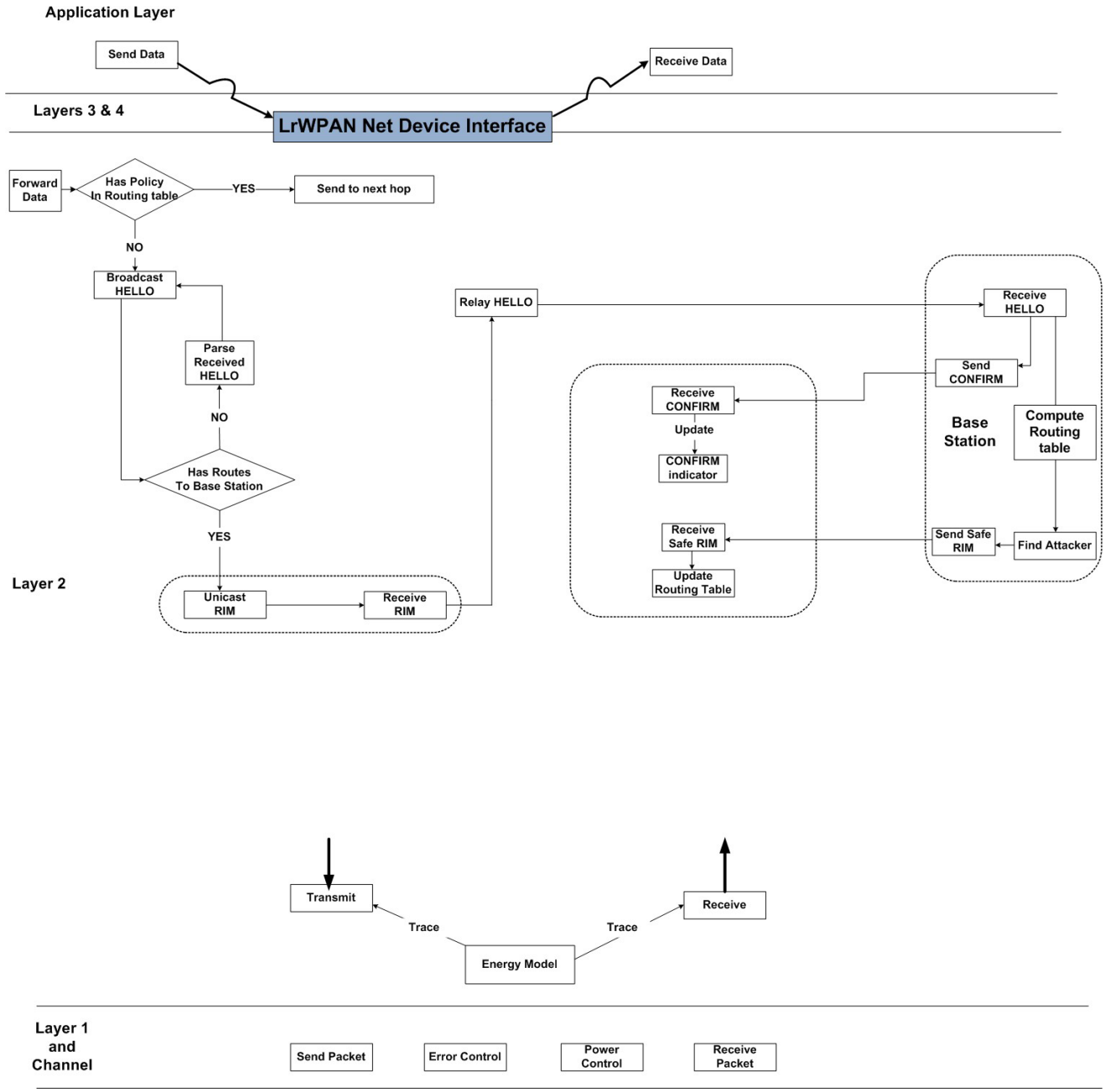

FIGURE 4. Relationship developed based on NS3.

V. SIMULATION SETUP

To evaluate the performance of MCRP, we simulated MCRP performance using NS-3 (version 3.26) on Ubuntu 16.04 LTS operating system. We compared its performance with other routing protocols like LEACH and LEACH-C. Performance is measured by quantitative metrics of average energy consumption, end-to-end delay, frame delivery ratio, and throughput. During the simulations, we considered different network configurations with randomly distributed sensor nodes in a 100 x 100 M^2 area with two nodes acting as the malicious nodes to create a wormhole link. In a real-world scenario, increasing the number of wormhole pairwise links would have a noticeable change in the network and thus the links can be easily identified [44]. Table 1 shows the simulation parameters. Experiments are all set to parameter assumptions in table 1 unless otherwise noted. The results indicate the efficiency of our protocol, even as the number of nodes increases.

A. SIMULATION PARAMETERS

B. VALIDATION

We prove that our proposed threshold ratio can detect wormhole attacks by calculating the error rate between the instant ratio of T_c and T_m with and without a wormhole attack

Algorithm 1 Setup of Routing Paths

Input: Routing Table = NULL Frame
Tag = NULL
Procedure 1: Look Up Routing Table
  if (Routing Table is NULL)
  then
    Create a HELLO frame
    Broadcast the HELLO frame
  else
    Forward Received Frame to the Next Hop
  end if
return
Procedure 2: Receiving HELLO
  if (the node is BS)
  then
    Calculate Routing Paths
    Return RIM frame having the Shortest
    Path to relevant Nodes Return CONFIRM frame
    to relevant Nodes
  else
    Forward RIM to Sender
  end if
return
Procedure 3: Relevant nodes receive CONFIRM
  Update Indicator
Procedure 4: Relevant node receive RIM
  Sort the Routing paths

Algorithm 2 Detection of Wormhole Attack at BS

Input:
Calculated Time per request (T_{ci}) = NULL
Sending Frame Length (SFL) = NULL
Receiving Frame Length (RPL) = NULL
Distance between Two Nodes (Dist) =100m
Data Rate (DR) = 250kb/s
Speed of Transmission (SoT) = 3×10^8 km/s Number of Hops (Hops) = 0
Queuing Time + Execution time (QET) = 0.002
Procedure 1: Calculating Instant Ratio
  Set SPL = 60Bytes Set RPL = 60Bytes Calculate Expected time by formula: T_{ci} = eq (1)
  Instant Ratio = T_{ci}/T_{mi}
return *InstantRatio*
Procedure 2: Calculating Average Ratio
  T_{ca} = eq (2)
  T_{ma} = eq (3)
  Average Ratio = T_{ca}/T_{ma}
return *AverageRatio*
Procedure 3: Detecting Wormhole
  Call Algorithm 1's Procedure 1 to find route
  if (Routing Table is Not NULL)
  then
    Loop: Iteratively retrieve a Route
    from Routing Table
    Call Procedure 1 to get Instant Ratio,
    Call Procedure 2 to get Average Ratio
    if (Instant Ratio Average Ratio)
    then
      Use the retrieved Route
      !No wormhole attack detected
    else
      Select the next least Route
      !Wormhole attack detected
    end if
    End Loop
  else
    Drop Frame
  end if

during the 100-node simulation. Fig. 5a shows an error rate of 3% and this is because the instant measured end-to-end time delay for a frame, to travel from source to destination, when there is no wormhole attack is relatively close to the calculated or expected time delay. This low error rate shows that our calculated T_{ci} eq (1) is in a very good agreement with the measured T_{mi}. This in turn would enhance the malicious node detection capability. Fig. 5b shows that the increase in variation between T_{ci} and T_{mi} reflects the inconsistency of frames when traveling via the wormhole route. When a frame travels through a wormhole tunnel, the T_{mi} is unstable compared to when there is no wormhole attack.

C. EXPERIMENTAL RESULTS

Figures 6a and 6b show the average energy consumption for 100 nodes over the simulation duration. These plots depict that MCRP has a much more desirable energy consumption curve than those of LEACH and LEACH-C even when there is a wormhole link in the network. This is because CH in both LEACH and LEACH-C follow a single-hop communication to transmit data directly to the BS [3], [45].

It is observed from Fig. 6a that when the wormhole nodes participate in the CH selection in both LEACH and LEACH-C, they cause uneven energy consumption over time as these wormhole nodes try to be the CH for every round due to their high energy level. Besides, when the sensing area is beyond a certain distance, those CHs far away from the BS would spend more energy compared to CHs which are closer to the BS. This then leads to uneven energy dissipation, which ultimately reduces the network lifetime [46], [47].

TABLE 1. Simulation Parameters

Parameter Type	Parameter Value
Number of Nodes	100
Duration	300s
Transmission Power	0.0315w
Receiving Power	0.0015w
Interval of Sending Data (Exp. Dist.)	Mean=1
Data Transmission Starting Time (s)	0
Threshold	3.5J
MAC	802.15.4

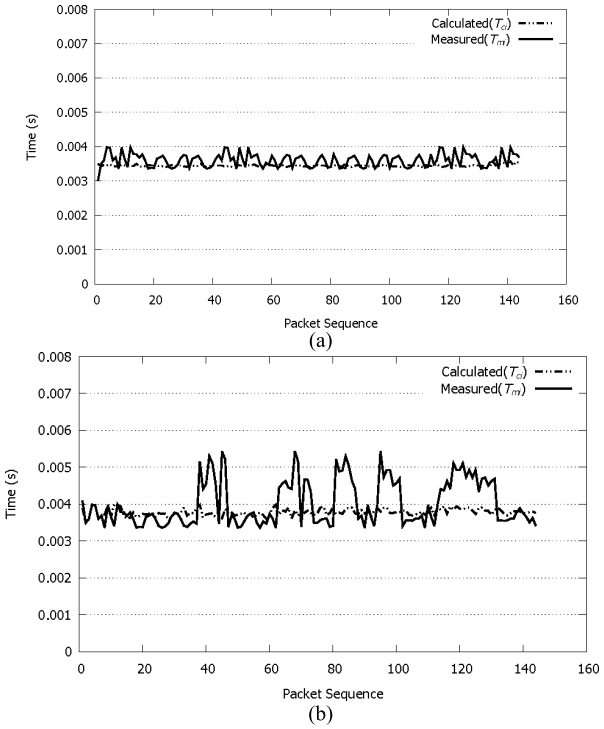

FIGURE 5. (a) Comparison between T_{ci} and T_{mi} without wormhole attack. (b) Comparison between T_{ci} and T_{mi} with wormhole attack.

MCRP alleviates this by having sensor nodes to send data (user or routing) only on demand to the BS through their neighbors. Furthermore, Fig. 7 illustrates the improvement gained through MCRP for the end-to-end delay.

These graphs show the time taken for frame transmission across the network from source to destination in two different network scenarios including having nodes with and without wormhole attackers. We can see that end-to-end delay across the network is relatively similar for the 25-Nodes simulation. However, as the number of nodes increases, the performance of LEACH and LEACH-C is negatively impacted. End-to-end delay with MCRP remains almost even across the two network scenarios particularly with a small number of nodes.

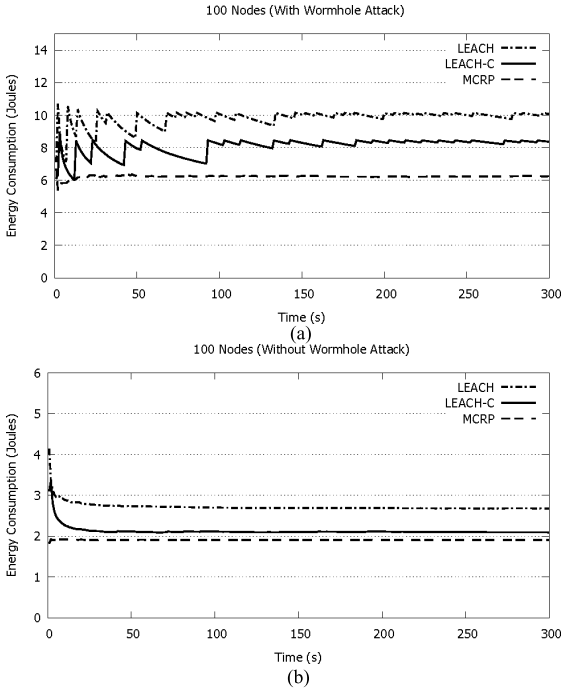

FIGURE 6. (a) Comparison between LEACH, LEACH-C and MCRP in a 100-Node simulation for average energy consumption with wormhole attack. (b) Comparison between LEACH, LEACH-C and MCRP in a 100-node simulation for average energy consumption without wormhole attack.

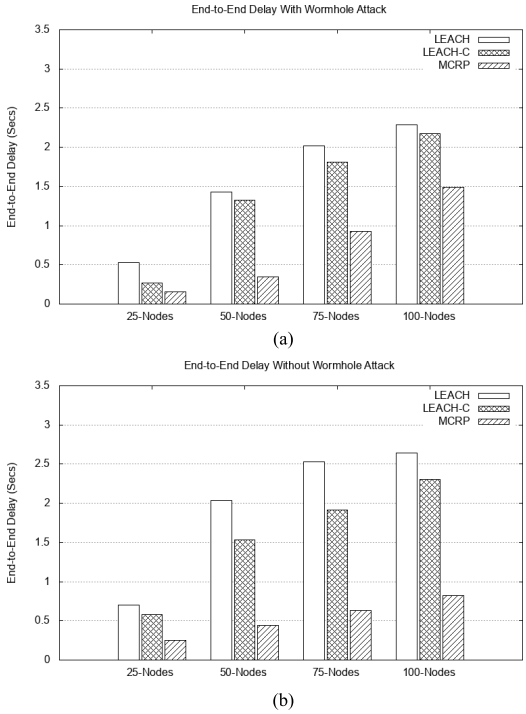

FIGURE 7. (a) Comparison between LEACH, LEACH-C and MCRP for end-to-end delay with wormhole attack. (b) Comparison between LEACH, LEACH-C and MCRP for end-to-end delay without wormhole attack.

This proves that MCRP can detect the wormhole attack and the selected path is safe and avoids data transfer over malicious nodes. With a larger number of nodes, we noticed that

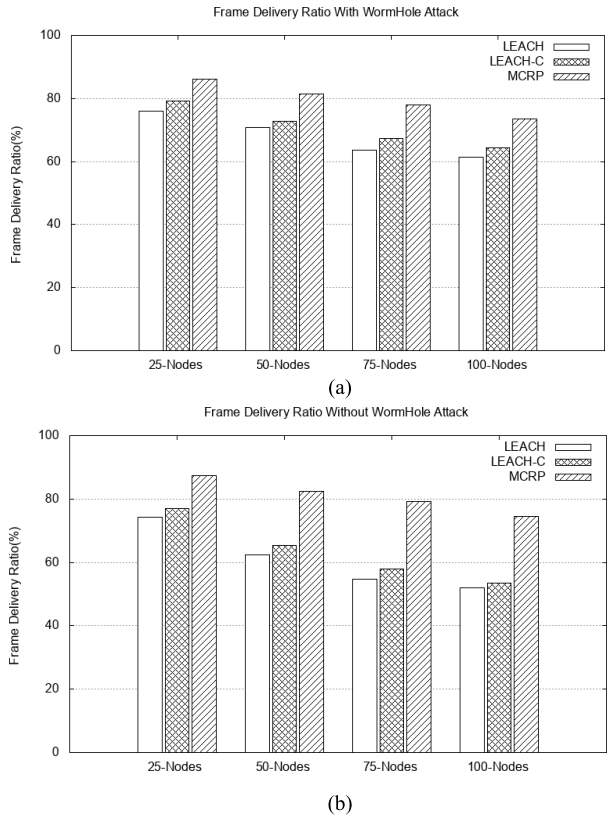

FIGURE 8. (a) Comparison between LEACH, LEACH-C, and MCRP for frame delivery ratio with wormhole attack. (b) Comparison between LEACH, LEACH-C and MCRP for frame delivery ratio without wormhole attack.

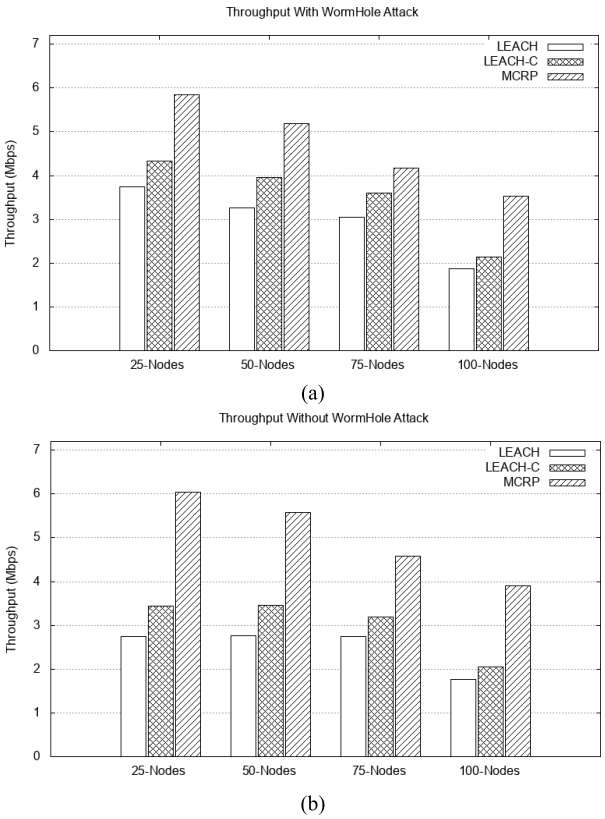

FIGURE 9. (a) Comparison between LEACH, LEACH-C and for throughput with wormhole attack. (b) Comparison between LEACH, LEACH-C and MCRP for throughput without wormhole attack.

MCRP incurred longer delay during the wormhole attack and this is because MCRP employs the time ratio threshold mechanism to detect the wormhole links and this, in turn, adds up more delay. Next, we analyze the ratio of frames successfully delivered to the BS over the total number of frames sent by the sensor nodes, with and without a wormhole attack. Figure 8 shows the frame delivery ratio for the three protocols. The plots clearly show the effectiveness of MCRP in delivering significantly more frames than other comparatives.

MCRP offers improvements in frame delivery ratio by delivering at least 72% of frames sent compared to 61% and 63% for LEACH and LEACH-C, respectively while detecting the wormhole link. The throughput graphs further exemplify the amelioration gained through MCRP in Figure 9. These plots show the rate of successful frames received by the BS per unit time. MCRP outperforms both LEACH and LEACH-C even when the number of nodes increases. We discover that both LEACH and LEACH-C perform better when there is a wormhole link in the network as these protocols cannot detect wormhole attacks and thereby allowing sensor nodes to send frames through this malicious low latency link. Nonetheless, MCRP outperforms both protocols by using the consensus between the BS and sensor nodes to detect the wormhole links.

FIGURE 10. Wormhole detection.

Figure 10 shows the comparison between the average measured end-to-end time delay (T_{ma}) when there is no wormhole attack and when there is a wormhole attack in 100-Node network simulation. As seen in Fig. 9, when there is a wormhole link in the network, T_{ma} is inconsistent because frames would then travel through the wormhole tunnel. The BS would detect this since it is equipped with the network topology and the actual number of hops between sensor nodes so when an adversary tries to create a low latency link with a better hop value, the BS sends a warning message to inform other nodes in the network.

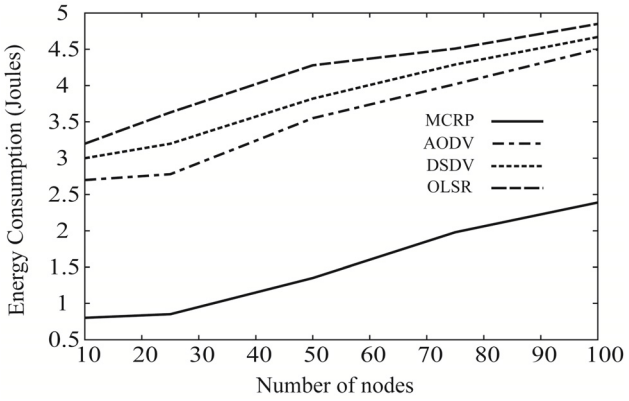

FIGURE 11. Comparison between AODV, DSDV, OLSR and our proposed protocol MCRP for total energy consumption.

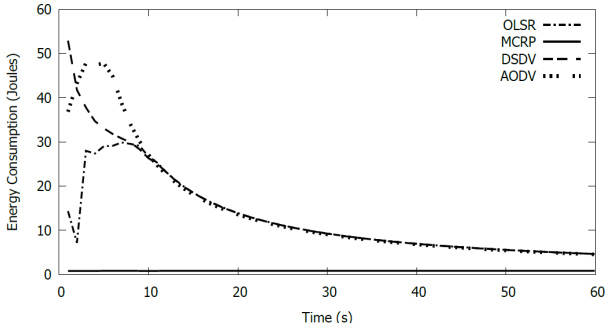

FIGURE 12. Comparison between AODV, DSDV, OLSR and our proposed protocol MCRP for average energy consumption.

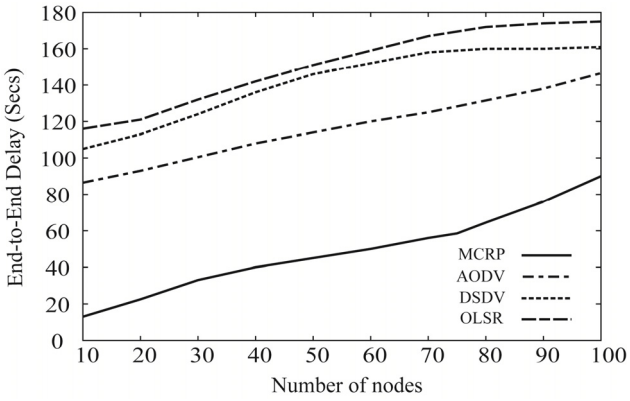

FIGURE 13. Comparison between AODV, DSDV, OLSR and our proposed protocol MCRP for end-to-end delay.

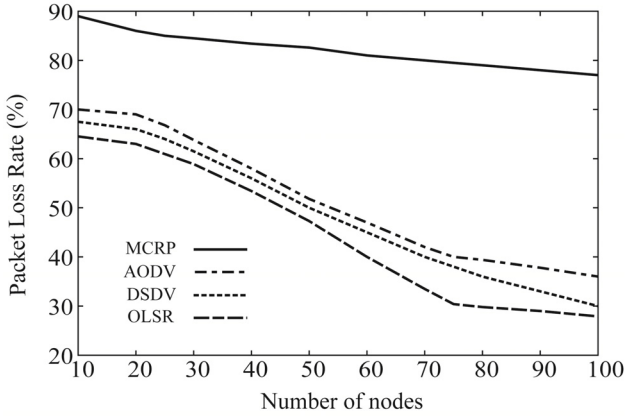

FIGURE 14. Comparison between AODV, DSDV, OLSR and our proposed protocol MCRP for packet lost ratio.

As pointed out in [30], the most popular routing protocols that provide accurate performance analysis are AODV, DSDV and OLSR so we present results comparing them with MCRP assuming wormhole attack and constant average time ratio. The ability of the SAODV is quite similar to the standard AODV to detect the wormhole attack as pointed out in [34]. Therefore, we use the original AODV to compare it with.

Concerning the total energy consumption, figure 11 shows that our proposed protocol consumes less energy compared to the other protocols. MCRP does not send out route packets periodically like traditional layer 3 routing protocols and it only sends route data on demand which in turn reduces the energy consumption. Figure 12 shows a comparison among protocols for the average energy consumption. We can see that these protocols consume more energy during the first 10 seconds of the simulation because during this period lots of energy is consumed by the nodes to find their neighbors and during also the network initialization process. However, the energy consumption drops after about 10 seconds as the network becomes stable but our proposed protocol MCRP is more stable as we only require fewer packets even during the network discovery phase.

Figure 13 shows the comparison to the MCRP protocol for the total time delay. Figure 14 shows the total number of lost packets over the total number of packets sent over the simulation period. From all these figures, we can see that MCRP outperforms all the protocols where OLSR has the worst performance.

VI. CONCLUSION

In this paper we propose a MAC centralized routing protocol (MCRP) that makes the use of the high-energy BS to perform most energy-intensive tasks. Thus, sensor nodes are only responsible for data forwarding while the BS handles all other functions. We also propose the concept of the time ratio threshold to detect wormhole attacks. Since the BS is equipped with the network topology and the actual distance between sensor nodes, it calculates the expected time for a frame to travel from a source to its destination and then compares it to the actual time taken for the frame to travel during the transmission journey. If the instant ratio of T_c to T_m is less than the average ratio of T_c to T_m, the BS ignores that route and updates the flow table. The main ideas in the MCRP routing protocol are the implementation of centralized network intelligence in one component of the BS to reduce the energy consumption while maintaining the consensus between sensor nodes and BS to efficiently detect wormhole attacks. The performance of the proposed MCRP is assessed

by simulations and compared to other protocols. MCRP exhibits an increase in the rate of successfully delivered frames per unit time of 56% and 39% over LEACH and LEACH-C, respectively, while detecting wormhole attack. MCRP also outperforms standard protocols including AODV, DSDV, and OLSR. The overall simulation results show that MCRP can further improve the performance of WSN, even as the number of nodes increases.

REFERENCES

[1] V. Tabus, D. Moltchanov, Y. Koucheryavy, I. Tabus, and J. Astola, "Energy efficient wireless sensor networks using linear-programming optimization of the communication schedule," *J. Commun. Netw.*, vol. 17, no. 2, pp. 184–197, Apr. 2015.

[2] M. Sefuba and T. Walingo, "Energy-efficient medium access control and routing protocol for multihop wireless sensor networks," *IET Wireless Sensor Syst.*, vol. 8, no. 3, pp. 99–108, Jun. 2018.

[3] S. K. Singh, P. Kumar, and J. P. Singh, "A survey on successors of LEACH protocol," *IEEE Access*, vol. 5, pp. 4298–4328, 2017.

[4] H. Kim and S.-W. Han, "An efficient sensor deployment scheme for large-scale wireless sensor networks," *IEEE Commun. Lett.*, vol. 19, no. 1, pp. 98–101, Jan. 2015.

[5] K. Eritmen and M. Keskinoz, "Improving the performance of wireless sensor networks through optimized complex field network coding," *IEEE Sensors J.*, vol. 15, no. 5, pp. 2934–2946, May 2015.

[6] D. Dong, M. Li, Y. Liu, X.-Y. Li, and X. Liao, "Topological detection on wormholes in wireless ad hoc and sensor networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1787–1796, Dec. 2011.

[7] J. Padmanabhan and V. Manickavasagam, "Scalable and distributed detection analysis on wormhole links in wireless sensor networks for networked systems," *IEEE Access*, vol. 6, pp. 1753–1763, 2018.

[8] M. Ditzel and K. Langendoen, "D3: Data-centric data dissemination in wireless sensor networks," in *Proc. Eur. Conf. Wireless Technol.*, Paris, France, 2005, pp. 185–188.

[9] P. R and M. Pushpalatha, "SDN enabled SPIN routing protocol for wireless sensor networks," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, Mar. 2016, pp. 639–643.

[10] C. Intanagonwiwat, R. Govindan, D. Estrin, J. Heidemann, and F. Silva, "Directed diffusion for wireless sensor networking," *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 2–16, Feb. 2003.

[11] P. Mishra and R. Tripathi, "Optimum energy path (OEP) protocol for wireless sensor network," in *Proc. Int. Conf. Circuits, Syst., Commun. Inf. Technol. Appl. (CSCITA)*, Mumbai, India, Apr. 2014, pp. 116–120.

[12] X. Yang, L. Wang, and Z. Zhang, "Wireless body area networks MAC protocol for energy efficiency and extending lifetime," *IEEE Sensors Lett.*, vol. 2, no. 1, Mar. 2018, Art. no. 7500404.

[13] M. Elsersy, T. M. Elfouly, and M. H. Ahmed, "Joint optimal placement, routing, and flow assignment in wireless sensor networks for structural health monitoring," *IEEE Sensors J.*, vol. 16, no. 12, pp. 5095–5106, Jun. 2016.

[14] S. Puvaneshwari and S. Vijayashaarathi, "Efficient monitoring system for cardiac patients using wireless sensor networks (WSN)," in *Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET)*, Chennai, India, 2016, pp. 1558–1561.

[15] H. Lin, L. Wang, and R. Kong, "Energy efficient clustering protocol for large-scale sensor networks," *IEEE Sensors J.*, vol. 15, no. 12, pp. 7150–7160, Dec. 2015.

[16] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Trans. Wireless Commun.*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[17] D. M. Birajdar and S. S. Solapure, "LEACH: An energy efficient routing protocol using Omnet++ for Wireless Sensor Network," in *Proc. Int. Conf. Inventive Commun. Comput. Technol. (ICICCT)*, Coimbatore, India, 2017, pp. 465–470.

[18] T. Giannetsos and T. Dimitriou, "LDAC: A localized and decentralized algorithm for efficiently countering wormholes in mobile wireless networks," *J. Comput. Syst. Sci.*, vol. 80, no. 3, pp. 618–643, May 2014.

[19] G.-H. Lai, "Detection of wormhole attacks on IPv6 mobility-based wireless sensor network," *EURASIP J. Wireless Commun. Netw.*, vol. 2016, no. 1, p. 274, Dec. 2016.

[20] X.-W. Wanga, F. Hu, C.-X. Zhai, Y. Zhang, X.-X. Su, Y. Li, Z.-K. Wu, T.-T. Li, and Z.-H. Deng, "Research on improved DV-HOP algorithm against wormhole attacks in WSN," in *Proc. 3rd Annu. Int. Conf. Inf. Technol. Appl. (ITA)*. Les Ulis, France: EDP Science, vol. 7, 2016, Art. no. 03007.

[21] J. Li, D. Wang, and Y. Wang, "Security DV-hop localisation algorithm against wormhole attack in wireless sensor network," *IET Wireless Sensor Syst.*, vol. 8, no. 2, pp. 68–75, Apr. 2018.

[22] M. Naplah, M. Y. I. B. Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (CHA—IDS) for 6LoWPAN communication protocol," *IEEE Access*, vol. 6, pp. 16623–16638, 2018.

[23] S. Qazi, R. Raad, Y. Mu, and W. Susilo, "Multirate DelPHI to secure multirate ad hoc networks against wormhole attacks," *J. Inf. Secur. Appl.*, vol. 39, pp. 31–40, Apr. 2018.

[24] S. Bai, Y. Liu, Z. Li, and X. Bai, "Detecting wormhole attacks in 3D wireless ad hoc networks via 3D forbidden substructures," *Comput. Netw.*, vol. 150, pp. 190–200, Feb. 2019.

[25] S. Kaur and R. Mahajan, "Integrated signature and recommendation-based trust evaluation protocol for wireless sensor networks," *J. Eng.*, vol. 2017, no. 11, pp. 606–613, Nov. 2017.

[26] F. Giroudot and A. Mifdaoui, "Graph-based approach for buffer-aware timing analysis of heterogeneous wormhole NoCs under bursty traffic," *IEEE Access*, vol. 8, pp. 32442–32463, 2020.

[27] G. Wu, X. Chen, L. Yao, Y. Lee, and K. Yim, "An efficient wormhole attack detection method in wireless sensor networks," *Comput. Sci. Inf. Syst.*, vol. 11, no. 3, pp. 1127–1141, 2014.

[28] X. Luo, Y. Chen, M. Li, Q. Luo, K. Xue, S. Liu, and L. Chen, "CREDND: A novel secure neighbor discovery algorithm for wormhole attack," *IEEE Access*, vol. 7, pp. 18194–18205, 2019.

[29] J.-W. Ho and M. Wright, "Distributed detection of sensor worms using sequential analysis and remote software attestations," *IEEE Access*, vol. 5, pp. 680–695, 2017.

[30] T. Hayajneh, P. Krishnamurthy, D. Tipper, and A. Le, "Secure neighborhood creation in wireless ad hoc networks using hop count discrepancies," *Mobile Netw. Appl.*, vol. 17, no. 3, pp. 415–430, Jun. 2012.

[31] S. Ji, T. Chen, and S. Zhong, "Wormhole attack detection algorithms in wireless network coding systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 660–674, Mar. 2015.

[32] D. Sasirekha and N. Radha, "Secure and attack aware routing in mobile ad hoc networks against wormhole and sinkhole attacks," in *Proc. 2nd Int. Conf. Commun. Electron. Syst. (ICCES)*, Oct. 2017, pp. 505–510.

[33] G. Akilarasu and S. Shalinie, "Wormhole-free routing and DoS attack defense in wireless mesh networks," *Wireless Netw.*, vol. 23, no. 6, pp. 1709–1718, 2017.

[34] A. Zahedi and F. Parma, "An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks," *Peer-to-Peer Netw. Appl.*, vol. 12, no. 1, pp. 167–176, Jan. 2019.

[35] P. Kaur, D. Kaur, and R. Mahajan, "Wormhole attack detection technique in mobile ad hoc networks," *Wireless Pers. Commun.*, vol. 97, no. 2, pp. 2939–2950, Nov. 2017.

[36] S. B. Geetha and V. C. Patil, "Graph-based energy supportive routing protocol to resist wormhole attack in mobile adhoc network," *Wireless Pers. Commun.*, vol. 97, no. 1, pp. 859–880, Nov. 2017.

[37] X. Su and R. V. Boppana, "On mitigating in-band wormhole attacks in mobile ad hoc networks," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2007, pp. 1136–1141.

[38] F. Nait-Abdesselam, B. Bensaou, and J. Yoo, "Detecting and avoiding wormhole attacks in optimized link state routing protocol," in *Proc. IEEE Wireless Commun. Netw. Conf.*, Mar. 2007, pp. 3117–3122.

[39] E. Hoque, H. Lee, R. Potharaju, C. Killian, and C. Nita-Rotaru "Automated adversarial testing of unmodified wireless routing implementations," *IEEE/ACM Trans. Netw.*, vol. 24, no. 6, pp. 3369–3382, Dec. 2016.

[40] C. E. Perkins and E. M. Royer, "Ad-hoc on-demand distance vector routing," in *Proc. IEEE WMCSA*, Feb. 1999, pp. 90–100.

[41] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, and L. Viennot, "Optimized link state routing protocol for ad hoc networks," in *Proc. 21st IEEE Int. Multi Topic Conf. (INMIC)*, Dec. 2001, pp. 62–68.
[42] C. Perkins and P. Bhagwat, "Highly dynamic DSDV for mobile computers," *Comput. Commun. Rev.*, vol. 24, no. 4, pp. 234–244, 1994.
[43] W. A. Aliady and S. A. Al-Ahmadi, "Energy preserving secure measure against wormhole attack in wireless sensor networks," *IEEE Access*, vol. 7, pp. 84132–84141, 2019.
[44] S. Mukherjee, M. Chattopadhyay, S. Chattopadhyay, and P. Kar, "Wormhole detection based on ordinal MDS using RTT in wireless sensor network," *J. Comput. Netw. Commun.*, vol. 2016, Nov. 2016, Art. no. 3405264.
[45] K. Roshan and K. R. Sharma, "Improved LEACH protocol with cache nodes to increase lifetime of wireless sensor networks," in *Proc. 2nd Int. Conf. Trends Electron. Informat. (ICOEI)*, Tirunelveli, India, May 2018, pp. 903–908.
[46] A. Yousaf, F. Ahmad, S. Hamid, and F. Khan, "Performance comparison of various LEACH protocols in wireless sensor networks," in *Proc. IEEE 15th Int. Colloq. Signal Process. Appl. (CSPA)*, Penang, Malaysia, Mar. 2019, pp. 108–113.
[47] J. Zhang and R. Yan, "Centralized energy-efficient clustering routing protocol for mobile nodes in wireless sensor networks," *IEEE Commun. Lett.*, vol. 23, no. 7, pp. 1215–1218, Jul. 2019.

OHIDA RUFAI AHUTU received the B.Sc. degree in computer information systems from Babcock University, Nigeria, in 2015, the PGD degree in information security management from Fanshawe College, London, ON, Canada, in 2017, and the M.Sc. degree in computer science (network technologies) from Lakehead University, Thunder Bay, ON, Canada, in 2019. His research interests include information and network security, and wireless ad hoc and sensor networks.

HOSAM EL-OCLA (Senior Member, IEEE) received the M.Sc. degree from the Department of Electrical Engineering, Cairo University, in1996, and the Ph.D. degree from Kyushu University, in 2001. He joined the Graduate School of Information Science and Electrical Engineering, Kyushu University, Japan, in 1997, as a Research Student. He joined Lakehead University, in 2001, as an Assistant Professor, and has been an Associate Professor, since 2007. He has more than 90 publications in journals and international conferences. His current main interests are in wireless sensor networks.