Hindawi Publishing Corporation
Journal of Sensors
Volume 2015, Article ID 203814, 12 pages
http://dx.doi.org/10.1155/2015/203814

Research Article

Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks

Ranjeeth Kumar Sundararajan and Umamakeswari Arumugam

School of Computing, SASTRA University, Tirumalaisamudram, Thanjavur, Tamil Nadu 613401, India

Correspondence should be addressed to Ranjeeth Kumar Sundararajan; ranjeethkumar@sastra.edu

Received 15 October 2014; Revised 5 January 2015; Accepted 12 February 2015

Academic Editor: Fei Yu

In wireless sensor network (WSN), the sensors are deployed and placed uniformly to transmit the sensed data to a centralized station periodically. So, the major threat of the WSN network layer is sinkhole attack and it is still being a challenging issue on the sensor networks, where the malicious node attracts the packets from the other normal sensor nodes and drops the packets. Thus, this paper proposes an Intrusion Detection System (IDS) mechanism to detect the intruder in the network which uses Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for its routing operation. In the proposed algorithm, the detection metrics, such as number of packets transmitted and received, are used to compute the intrusion ratio (IR) by the IDS agent. The computed numeric or nonnumeric value represents the normal or malicious activity. As and when the sinkhole attack is captured, the IDS agent alerts the network to stop the data transmission. Thus, it can be a resilient to the vulnerable attack of sinkhole. Above all, the simulation result is shown for the proposed algorithm which is proven to be efficient compared with the existing work, namely, MS-LEACH, in terms of minimum computational complexity and low energy consumption. Moreover, the algorithm was numerically analyzed using TETCOS NETSIM.

1. Introduction

Wireless sensor devices are used in a broad range of applications such as defense, farming, medicine, and industries. WSNs deploy an array of microsensors that senses the activities of a physical phenomenon and sends the information to the base station (BS). They face a lot of security issues that arise due to their low operating energy and minimal computational capabilities. Table 1 shows some of the security attacks in the different layers of the WSN protocol stack. This research work focuses on the network layer threat and it effects, namely, sinkhole attack which is set off by a malicious node that attracts the traffic from its neighboring nodes and either selectively forwards it or alters it, resulting in a successful intrusion and high data loss rate of the real time data [1]. An extensive study on sensor routing protocols and their attacks like selective forwarding, spoofing/replaying, sinkhole, wormhole, Sybil attack, and HELLO flood attack with the counter actions is available in [2]. Various security threats in WSN are identified and classified into two broad categories, namely, active and passive attacks. In active attack, the compromised node alters or makes changes in the data during transmission. Some of the active attacks are denial of service (DoS), modification, impersonation, fabrication, and so on. In passive attack, the malicious node does not make any changes in the data, but it overhears the data transmission. Some of the passive attacks are eavesdropping, traffic analysis, and camouflage adversaries.

The security mechanisms to counter these attacks are classified into two types, namely, low level and high level. The low level mechanism includes key establishment, privacy, and authentication. The high level mechanism includes secure group management, Intrusion Detection System (IDS), and secure data aggregation [3]. The IDS forms a second level of defense to the network and alerts the network in the presence of threats. There are four different types of IDS, namely, Signature IDS, Anomaly IDS, Hybrid IDS, and Cross Layer IDS. These IDS can be compared based on the characteristics like detection rate, false alarm rate, computational capability, energy consumption rate, and so on [4, 5]. One of

Table 1: Layer-wise threats.

Layer	Threats
Physical	Jamming, tampering
Data link	Collision, exhaustion, unfairness
Network	Sinkhole, black hole, selective forwarding
Transport	Flooding, false messages, desynchronization
Application	Reliability attack, clock skewing, data aggregation distortion

the important low level security mechanisms is cryptographic method, which includes key size, block size, and message about the round as corresponding information. Many security protocols like TinySec, MinSec, SPINS, and LSec are proposed to provide security to the sensor network and these protocols use encryption and authentication mechanisms [6].

This paper focuses on the high level defense mechanism, namely, IDS, to detect the malicious nodes. The malicious node launches the attack by advertising that it is the nearest node to the BS and attracts the packets and alters those passing through it. It still remains an open weakness in case of insider attacks, where a node is free to manipulate the packets and gain control over it. Most routing protocols in the sensor network do not initiate any mechanisms for detecting security attacks. Encryption methodologies and authentication system prove to be inefficient in the case of laptop and insider attacks. So, it has become imperative to devise a mechanism against these attacks practically. The main objective of this research work is to study the effects of sinkhole attack in a WSN which uses the LEACH protocol for its routing operation and devise a security mechanism to overcome the adverse effects. Sinkholes are induced in a WSN either by insiders or by an external attacker. The proposed IDS algorithm detects the sinkhole attack with high detection rate. The performance of the intrusion detection algorithm is verified numerically and simulations enforce the accuracy and the effectiveness of the algorithm. Four main contributions in this work are as follows.

(1) A lightweight IDS is proposed with minimal computational complexity.

(2) A novel intrusion detection metric, namely, intrusion ratio (IR), is introduced.

(3) A detailed security analysis is performed in three different scenarios.

(4) The proposed lightweight IDS is capable of capturing multiple attacks.

This paper is structured as follows: Section 2 gives the similar IDS works on sinkhole attacks and LEACH protocol. The description of LEACH protocol, sinkhole attack, and research motivation is presented in Section 3. Section 4 includes methods of launching the sinkhole attack in LEACH and the proposed IDS algorithm. Section 5 shows the simulation of sinkhole attack and analysis of proposed algorithm. In Section 6, conclusion and future work are given.

2. Related Work

An efficient IDS algorithm with low overhead was proposed by Ngai et al. [1]. This robust algorithm checks the data consistency and captures the intruder by verifying the network flow information. The algorithm is also robust against the presence of multiple malicious nodes. In [7], different ways to launch the sinkhole attack are discussed. The BS is identified as the trusted member in the network. Based on the sequence number, the sinkhole attack was launched and subsequently the packet transmission was performed through the Ad Hoc On-Demand Distance Vector (AODV) protocol to identify the malicious activity of the intruder. The authors in [8] propose a two-step intrusion detection process to detect the colluding nodes acting against the BS. They analyze the network routing patterns for data consistency. Based on the node ID's the BS identifies the compromised node and alerts the normal sensor nodes. The impact of wormhole attack on LEACH protocol has been analyzed [9]. A separate tunnel is created by the attacker through which the data is transferred to the wormhole nodes. The wormhole attack can also be used to launch the sinkhole attack by making one of the wormhole nodes a sinkhole. An IDS to detect the sinkhole attack in the WSN which uses Mintroute protocol for its routing operation was proposed [10]. Using a strategy of advertisement, the sinkhole attack was launched that exploits the link quality of the compromised node to send the data to the sinkhole node. Thus, an IDS mechanism is developed as a localized agent to detect such malicious activity of the sinkhole node in the distributed networks.

The two security threats, namely, black hole and sinkhole attacks, are analyzed on the LEACH protocol [11]. The attacks are simulated in MATLAB with various metrics like residual energy, data transmission, and node longevity. The analyses were made in two different scenarios; normal operation and under attack. In [12], the proposed IDS integrate node behavior strategies and evidence theory. The multidimensional behavior characteristics are collected to calculate its deviation with the expected value and the belief factor is calculated for each sensor node. If the value of a senor node is less than 0.25, it is blacklisted and marked as a malicious node. In [13], the proposed work has two approaches to detect sinkhole node in the network. The first approach identifies the region of the network which may contain the intruders. This work is performed in two ways by using geostatistical frailty survival model and distributed monitoring. The second approach is of mitigation type and this method is used to identify the intruders from the affected region. The authors in [14] propose IDS to detect the sinkhole attack. The sinkhole attack is launched on the Mintroute protocol by advertising a better link quality and changing the link quality value of current parent node to the worst value. They propose rule-based IDS to detect the sinkhole node. The authors also analyze the selective forwarding and black hole attacks on the Mintroute protocol. They also developed IDS to detect the attacks. In [15], the authors propose IDS to capture the sinkhole node which set itself as a fake BS. The node sends a control packet directly to the BS; then it sends data packet hop-by-hop. When the packet arrives, the IDS compares some of

its control fields with the original control packet and if any changes have been made to the control fields, then the IDS alert the presence of malicious node.

An IDS agent on each sensor node has two intrusion detection modules, namely, local agent and global agent [16]. The local agent stores the information of the sensor node, while the global agent monitors the communication of its neighbor nodes. The global agent uses watchdog and predefined 2-hop neighbor knowledge to detect the anomalies within its transmission range. In [17], the authors propose decentralized IDS which have watchdog modules residing in the monitor nodes. These nodes analyze the behavior of other nodes including cluster head (CH). If they detect an attack, the monitor node forwards the alarm to the BS and adds the compromised node to the blacklist. The blacklisted nodes are also broadcasted to all other nodes to avoid further communication. The authors in [18] propose IDS to identify the malicious activities according to the various phases of LEACH protocol. The CH selection is done according to the energy level for each round. When the same sensor node is selected as CH for the second time consecutively, then it may be a compromised node. Malicious node sends strong signal indicating it as the CH. This type of compromised node is identified by calculating the signal strength based on the distance. When a sensor node sends the join request to the CH and if it does not receive the TDMA (Time Division Multiple Access) schedule within certain period of time, then the CH may be a malicious node.

IDS can be categorized based on their detection method as Misuse and Anomaly. Based on the architecture, it can be classified as Host IDS (HIDS), Network IDS (NIDS), and Distributed IDS (DIDS). Based on the response, the IDS can be classified as active and passive, and in view of the decision making it can be classified as cooperative and autonomous. The authors list three works related to IDS on the LEACH protocol. Firstly, watchdog based IDS is proposed to capture the attack on each phase by applying the rules and secondly specification based IDS is proposed. The third method, namely, CUSUM IDS, is proposed based on the path construction, which uses normal path and malicious path information for detecting the intrusions [19]. In [20], the authors propose TESLA (Timed Efficient Stream Loss-Tolerant Authentication) based security mechanism to protect the LEACH protocol. The BS acts as a Key Distribution Center (KDC) and transfer the TESLA key to the sensor nodes periodically. The sensor nodes send the data along with the node membership certificate to the CH. By then, the CH aggregates and transfer the sensed data to the BS. The authors in [21] propose IDS by analyzing the detection rules in different architectures. They verified their work by identifying the sinkhole nodes on the Mintroute protocol with less resource consumption. In [22], cryptographic based IDS are proposed to detect the sinkhole nodes. The BS verifies the digest value obtained from trustable forward path and from the trustable node to the destination. If the values are different, then the BS alerts the sensor nodes about the presence of sinkhole node. The authors in [23] propose centralized monitoring approach to detect the sinkhole node in the WSN. The monitoring node (or leader node) is randomly selected from the group of sensor nodes. The leader node compares the node ID and location of the route nodes; if the node ID exists in the information table then it allows the transmission or alerts the other nodes about the intrusion. In [24], the authors propose a dynamic random password based IDS to detect the malicious activities in the WSN. The BS assigns node ID for each node and a password is generated dynamically for successful transmission of the data. A threshold based hierarchical IDS (THIDS) is proposed in [25] to detect the selective forwarding, black hole, and sinkhole attacks. Each sensor node has a local list called Isolate list to store the adversary's identities. When the sensor node does not receive any message from the CH for a period of time, then it is added to the Isolate list and sends a local alert message to the neighboring nodes about the presence of sinkhole node.

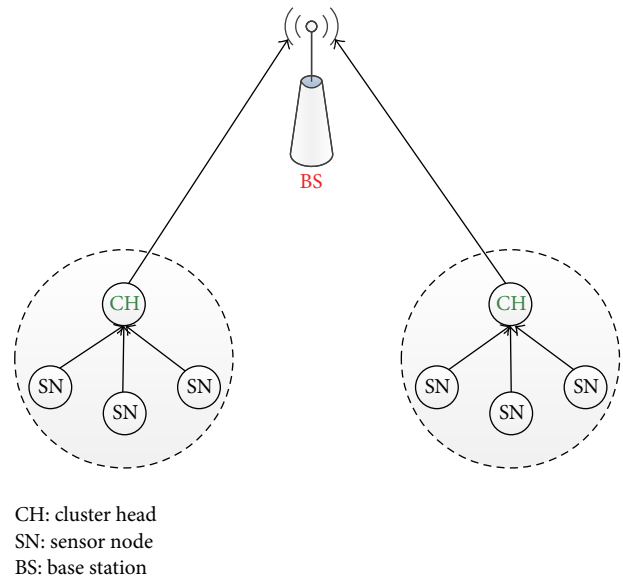

Figure 1: LEACH principle.

3. Research Background

3.1. Low Energy Adaptive Clustering Hierarchy (LEACH) Protocol. Hierarchical clustering is a method of arranging the nodes into a hierarchy of groups based on a weight function. Several hierarchical protocols exist in the literature and security is one of the prime concerns in these types of protocols [26]. LEACH is an energy efficient protocol that works based on hierarchical clustering. This protocol was proposed in 2002 by Heinzelman et al. [27]. They devised a new way of hierarchical clustering in WSNs that uses randomized rotation of CHs on the basis of sensor node (SN) properties such as energy and bandwidth. Unlike the usual clustering protocols where the CH continues to be the same node throughout the routing process, LEACH involves rotation of CHs in a dynamic and random manner so that energy is uniformly distributed to all the sensor nodes. Figure 1 shows the working principle of LEACH protocol.

The protocol works in two phases, namely, the setup phase and the steady state phase. In the first phase,

all the members of the sensor network participate in the election process by choosing a random number between 0 and 1 and if this number is less than the threshold value, $T(n)$, then that particular sensor node is elected as a CH [28].

$T(n)$ is calculated by the following equation:

$$T(n) = \frac{p}{1 - p\left(r \bmod (1/p)\right)} \quad \text{if } n \in G \text{ else } T(n) = 0, \quad (1)$$

where "p" is the probability or desired percentage to become a CH, "r" is the current round, and "G" is the node set that has not being selected as a CH in the past $1/p$ rounds [28]. When the election is over, the entire set of elected CHs announces itself to be the CH by broadcasting an ADV (advertisement) packet. The remaining nodes find the CH which is nearer to them based on the minimum communication energy required. When the cluster is decided, the nodes send a JOIN-REQ (join request) packet to the corresponding CHs. At the end of setup phase, clusters are created and each CH allots time slot for its cluster nodes using TDMA. The fixing of time slots based on TDMA ensures that each node communicates with the CH during the allotted time slot to minimize collision. The steady state phase involves each node sending its data during its allotted time slot to the corresponding CH. The CH performs data aggregation and transmits it either to the BS or to its nearest CH when the BS is outside its transmission range. Thus CHs are the only nodes that interact directly with the BS. Only during their time slot, a cluster node has its radio in the active state; otherwise it gets into the sleep mode and thus sensor nodes reserve energy.

In addition to this, dynamic allocation of CHs ensures that every node has uniform energy and this makes LEACH as an energy efficient protocol. In LEACH, the sensors form local groups and a local CH is chosen randomly to serve as the local BS [27]. In this way, the CH position is rotated to assign CH to the cluster with the highest energy at any time. The energy load is balanced evenly so that none of the sensor nodes has drained off its energy fully. LEACH protocol is explained along with its advantages and disadvantages and the protocol performance is verified through simulation by considering the percentage of non-alive nodes [28].

3.2. Sinkhole Attack. Sinkhole attack is an active type of attack which focuses on the routing pattern of a protocol. The compromised node (CN) acts as a sinkhole and attracts all the traffic towards itself [10]. The compromised node grabs attention from the other nodes by establishing itself to have a high value with respect to the routing metric [11]. As a result, the intruder gets control over the packets and proceeds to launch further attacks like black hole, selective forwarding, altering packets, and so on. Various types of attacks based on the location are also present in the literature and existing schemes like multipath routing, hashing, cryptography, key distribution, localization, and IDS are used to counter these types of routing attacks [29]. Various methods are present to launch the sinkhole attack, either by directly giving false information about the routing metric to the sender nodes or by using wormhole attack. The wormhole threat creates a separate link from the normal network link and starts

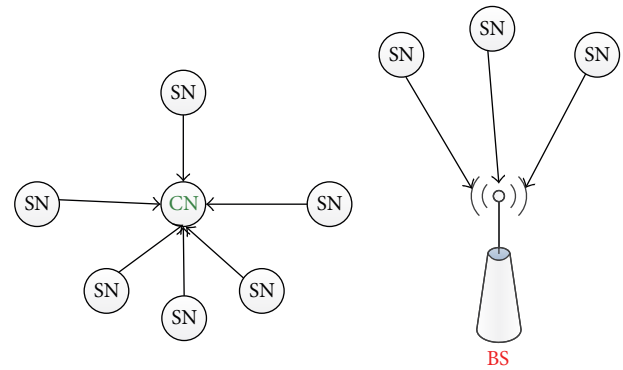

Figure 2: Sinkhole attack.

forwarding the data between them. Either of the nodes in the wormhole link can be made as a sinkhole node and further attacks can be launched. Figure 2 shows sinkhole attack (launched by compromised node).

The compromised node sends the fake routing information to the normal sensor nodes to transmit their sensed data. The compromised node can drop the packets completely and this process of threat is called black hole attack [30]. The sinkhole node can also be used as a platform for launching other threats like forwarding the packets selectively or deleting some fields in the packet. This kind of attack is called selective forwarding. This research work focuses on the analysis of adverse effects of the sinkhole attack on LEACH protocol and develops an efficient defense mechanism to reduce the adverse effects of the sinkhole attack to the network. The sinkhole attack can be launched on various routing protocols by falsifying the routing metric. The sinkhole attack in [10] is launched in the Mintroute protocol by giving false information about the link quality which is used as a routing metric by the protocol. The compromised node gives the high link quality to make other nodes forward their data to it.

The sinkhole attack is detected by identifying the intrusion region using geostatistical hazard model and distributed monitoring approach. This method is computationally expensive [13]. In case of LEACH protocol, the sinkhole attack can be launched using the CHs. The compromised node projects itself with high energy value and makes it to be selected as the CH. This compromised CH acts as a sinkhole node and performs the attack by dropping or altering the sensed data which is received from its cluster members. The sinkhole attack can be launched in other routing protocols and an efficient defense mechanism is needed to counter this attack.

3.3. Research Motivation. Table 1 classifies the attacks based on the layers of the WSN protocol stack, where the network layer has many potential vulnerabilities like sinkhole attack, black hole attack, selective forwarding, Sybil, HELLO flood, wormhole, and so on. The purpose of routing attack is to

create a serious threat to the sensor network. The sinkhole is one of the most susceptible threats to the sensor network as referred to in [9, 11, 21, 23, 25–27]. It can be extended further with the attacks like selective forwarding, black hole, and HELLO flood to devastate the network transmission [31–33]. Thus, this paper places its major concern on the sinkhole nodes, since it is more vulnerable than the other security threats. In addition, it is interesting to study the effects of the attack to develop the defense mechanism.

As LEACH is a hierarchical protocol, CH plays the major role for data transmission, where the CH is compromised as a sinkhole node to disrupt the condition of the network [34]. The protocol, like LEACH, has had several extensions like LEACH-C [35], LEACH-F [36], LEACH-B [37], LEACH-E [38], LEACH-M [39], MH-LEACH [40], I-LEACH [41], V-LEACH [42], and so on. These extended versions focus on minimizing the energy consumption and reducing the transmission overhead [43]. In addition, the extended versions of the LEACH protocol have not had its concern on the feature like intrusion detection. The existing security mechanisms of the LEACH protocol are generally classified into cryptographic based methods and non-cryptographic methods. The cryptographic methods are S-LEACH [44], Armor-LEACH [45], R-LEACH [46], MS-LEACH [47], and Sec-LEACH [48]. The non-cryptographic methods are signal strength based approach [49] and TM-LEACH [50]. In S-LEACH, the detection of sinkhole and selective forwarding attacks were dealt. Since it is a cryptographic method, it increases the computational overhead of the networks. Recently, the S-LEACH has been extended as MS-LEACH, though MS-LEACH still lacks in throughput efficiency and energy consumption. The non-cryptographic method is based on signal strength and trust-value security. But, it does not deal with the routing attacks in WSN. Above all, the effects of the sinkhole attack on the LEACH protocol is still not present on lightweight non-cryptographic method. Thus, this research focuses on the development of non-cryptographic IDS in turn to reduce the adverse effects with minimum resource utilization.

4. System Design

Security is the prime concern in a wireless network and the sinkhole attacks are so vicious that they overcome all the other attacks. The effort of providing security was channelized in studying the possibility of sinkhole attack in a sensor network having LEACH as the routing protocol, the attack effects, and developing an IDS to minimize the adverse effects. Important Notations Used Section shows the notations used and their description.

4.1. Problem Description. In LEACH protocol, the energy value is the deciding factor that selects the CH and it has a threshold dependency. The initial study is to understand the clustering pattern of the network. Thereafter, the intruder launches the attack, like sinkhole attack in the LEACH routing based network, with the help of a cluster of nodes. The parameters, namely, number of clusters (nc) and cluster members (SN_i), are observed to predict the values. During the attack operation, the values are considered to compromise the CHs in different locations. Since the routing attacks emerge as a problematic issue for the WSN, the intruders launch the attack in two different ways.

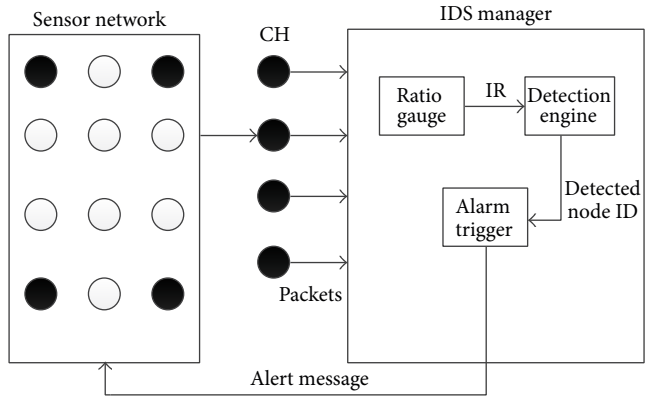

Figure 3: IDS architecture.

4.1.1. Launching of Sinkhole Attack. The launching of attacks is classified in two different ways. The former launching is to use a set of CH nodes to launch a coordinated sinkhole attack. The objective of this attack is to compromise "nc" nodes that are available across the network, such that each compromised node belongs to the cluster. In the coordinated sinkhole attack, the number of clusters is equal to the number of compromised nodes. So, the compromised nodes gain the control of normal sensor nodes to project its energy values as above the threshold to become a CH. In the steady state phase, the normal nodes transmit their data packets to the compromised CHs and thus every compromised CH or sinkhole node can drop or manipulate the packets to complete the security breaching. The latter launching is to introduce a compromised sinkhole attack to manipulate the data of its cluster members in the network. In order to launch the sinkhole attack, CH is compromised for each round of selection process instead of compromising "nc" cluster. In such scenario, one CH would be malicious to act as a sinkhole. Though it has limited performance loss for each data transmission, the malicious activity is extended further in the compromised sinkhole attack. Hence, it has been addressed as a challenging problem for the sensor networks. However, such attacks can be detected effectively by the mechanism of IDS.

4.2. IDS Architecture. Figure 3 gives an overview of working principle of the proposed IDS. Recent routing protocols face security issues in the presence of multiple sink or BS and node mobility [51]. The proposed IDS works fine in the presence of multiple sinks by placing the detection agent on each sink. The proposed work assumes that the compromised nodes, that is, the sinkhole nodes, blindly drop or selectively forward the packets which are received from the normal sensor nodes. The CH collects the data from the cluster member and it is later analyzed by the BS. The IDS agent that runs in the BS

```
Begin
S_n is the sensor network and PT_i be the total packets transmitted by the ith CH in S_n
PR_i is the total packets received by the ith CH in S_n
N_i is the Cluster head Node ID
P_i is the Intrusion ratio for the ith CH
Repeat
   Time_delay (100)
   For ∀ (C_i)
      Receive (PR_i, PT_i and N_i) packets from the CHs'
      Calculate P_i where P_i = PR_i/PT_i
      If P_i tends to ∞ then
         Corresponding N_i is the sinkhole node
         Isolate N_i
         Send warning message to the remaining cluster member nodes about N_i
      Else
         Corresponding N_i is the normal CH
      End if
   End for
   Until the nodes transmission process completes
   End
```

Algorithm 1: IDS Algorithm for Sinkhole Attack.

receives the packets by overhearing the transmission of the cluster members and CH nodes. The IDS agent contains ratio gauge module which calculates the intrusion ratio (IR) from the values obtained from the network. The packet received (PR_i), packet transmitted (PT_i), and CH node ID's (N_i) values are used to calculate the IR. The ratio gauge sends the IR value to the detection engine. The detection engine triggers the alarm which depends upon the IR value indicating the presence of compromised node.

The algorithm for the intrusion detection process is given in Algorithm 1.

4.2.1. Algorithm Description. The IDS agent module runs in the BS to identify the intrusion by analyzing the data packets that consists of PR_i, PT_i, and N_i periodically. The packet transmission value of CH (PT_i), the packet reception value of CH (PR_i), and the CH node identification of the CH (N_i) are used to validate the intrusion ratio (IR) as numeric or not by the IDS agent. If the ratio of PR_i to PT_i is numeric, it means that the packet is not completely dropped to ensure "the malicious activity is not existing." Otherwise (IR is infinity), the corresponding CH is a sinkhole node which had dropped the data packets completely that would lead to black hole attack. On the other hand, if there is a huge difference between PR_i and PT_i values, it infers that there may be a possibility of selective forwarding attack.

The purpose of the above strategy is to minimize the intrusion ratio so that the intruder node can be isolated in the next round of data transmission and blocked from the CH selection process by the BS. The proposed IDS mechanism alerts the respective cluster members regarding the presence of sinkhole node to stop the further data transmission. Moreover, this algorithm has much less computation to detect the sinkhole node from the available information (local) and it also increases the energy efficiency of the network by the quick identification of the compromised nodes. Since the proposed IDS mechanism has less communication overhead between the sensor networks and the BS, the ratio gauge calculation is simple to make the computation easier which reduces the computational complexity to the further extent. Even though the node density of the sensor network is increased, the proposed IDS mechanism works efficiently to alert the threat deduction. The proposed IDS has much less storage since its values are removed from the buffer after computing the IR value.

4.3. Intrusion Detection Model. A simple mathematical model is constructed to verify the effectiveness of the IDS algorithm. The sensor network (S_n) consists of many sensor nodes uniformly placed over the network. Let S_n consist of $SN_1, SN_2, \ldots$, and SN_n sensor nodes in the network. Let C_i be the cluster which contains the sensor nodes as its members. The N_i is the CH of a particular cluster C_i. The CHs are selected in the setup phase and the sensor nodes join the cluster depending upon the transmission range. The sensor nodes SN_i start sensing the physical phenomenon like temperature, humidity, movement tracking, and so on. The packets received (PR_i) and packets transmitted (PT_i) value of a particular CH (N_i) are calculated by the BS through overhearing the transmission of the cluster members and the CH.

Mathematically the intrusion ratio (IR) is represented by the following equation:

$$P_i = \frac{PR_i}{PT_i}. \tag{2}$$

The IR value (P_i) can take any of the following two values: $P_i = \infty$ or $P_i = n$. From the value of P_i, the IDS agent

decides whether a CH is malicious or normal. If the IR value is a numeric value (n), then it denotes that the packets are not fully dropped. If the IR value is an infinite value (∞), it denotes that $PT_i = 0$ which indicate the presence of some malicious activity. The following equation presents the values of the IR(P_i):

$$P_i = \begin{cases} n \longrightarrow N_i \text{ is a normal node, } \forall n \in \text{integer} \\ \infty \longrightarrow N_i \text{ is sinkhole node.} \end{cases} \quad (3)$$

Consider an example sensor network with four clusters. The sensor nodes SN_1, SN_2, SN_3, and SN_4 form a cluster C_1 and similarly clusters C_2, C_3, and C_4 are constructed. The cluster members transmit their sensed data to their corresponding CHs (N_i). The data is temporarily stored in the buffer of N_i. For the CH (N_1) in the cluster C_1, the IR is calculated as follows:

$$P_1 = \frac{PR_1}{PT_1}. \quad (4)$$

For the Other Clusters. The IR values can be calculated as $P_2 = PR_2/PT_2$, $P_3 = PR_3/PT_3$ and $P_4 = PR_4/PT_4$. To explain the model, the IR calculation is classified into two different cases with sample values to show the possibility, such as under attack/no attack.

Case 1 (under attack). Consider 4 cluster members SN_1, SN_2, SN_3, and SN_4 and a CH N_1, given some sample input values, the IR is calculated. Let the PR_1 value of the CH $N_1 = 80$ and the PT_1 value of CH $N_1 = 0$. The IR value of the CH N_1 is calculated from (4) as $P_1 = 80/0 = \infty$ which indicate that the CH N_1 is a sinkhole node, since it drops all the 80 packets ($PT_1 = 0$).

Case 2 (no attack). Consider 4 cluster members SN_1, SN_2, SN_3, and SN_4 and a CH N_1. Given some sample input values, the IR is calculated. Let the PR_1 value of the CH $N_1 = 80$ and the PT_1 value of CH $N_1 = 76$. The IR value of the CH N_1 is calculated from (4) as $P_1 = 80/76 = 1.05$, which is a numeric value and indicates that the CH N_1 is a normal node since it forwards the packets. Similarly, the process of IR estimation is done to all the CHs in the network. Minor packet loss occurs due to network link conditions. The IR value is calculated from the local data collected by the ratio gauge present in the IDS agent and hence the proposed IDS reduce the energy consumption to acquire the global data access.

5. Simulation and Analysis

5.1. Simulation Process. The proposed work was simulated using TETCOS NETSIM. Table 2 shows the simulation setup. The following are the assumptions for simulation of the proposed IDS.

(1) BS has the highest energy resource.

(2) All the sensor nodes are static.

Table 2: Simulation setup.

Sensor nodes	36
Agent nodes	1
Base station	1
Transmission range	100 m
Transmission power	100 mW
Frame retries	0
Arrangement	Uniform

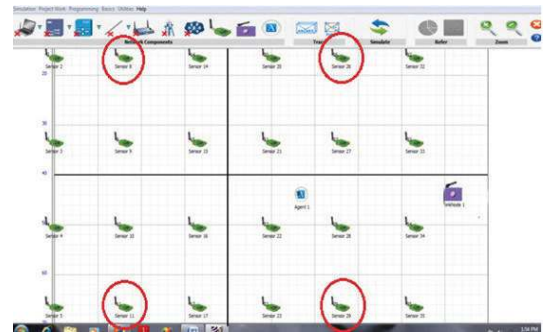

Figure 4: Initial scenario.

(3) All the sensor nodes transfer data in the allocated frame.

(4) Compromised nodes have higher energy level than normal sensor nodes.

The initial setup consists of 4 clusters of 9 sensors inclusive of the one being the CH of each cluster and the members are increased for the simulation process. The scenario highlighting the initial set of CHs, namely, sensors 8, 11, 26, and 29, is shown in Figure 4.

The simulation of LEACH in NETSIM resulted in the packet transfers depicted in Figures 5, 6, and 7. Figure 5 shows the normal packet transfer operation from the sensor node to CH 8. In Figure 6, the transmission happens between CHs 8 and 26 because the BS is not within the transmission range of CH 8. Figure 7 shows the packet transmission of CH 26 to the final destination BS.

When a coordinated sinkhole attack is launched in the above scenario, all the CHs drop the packets and no packets are received by the BS. However, sinkhole attack on a single CH showed that the BS received packets from all the CHs except the compromised CH. The following section shows the results of simulation depicting the number of packets transmitted and received. The simulation results are graphically represented in which the x-axis denotes the CH and y-axis the packets. Figure 8 shows the values recorded during the normal LEACH operation.

In Figure 9, the values recorded during cooperative sinkhole attack are shown, where the BS receives no data. Figure 10 shows the values recorded when a single CH, that is, sensor node 8, is attacked. Note that the number of packets transmitted by sensor node 8 is 0.

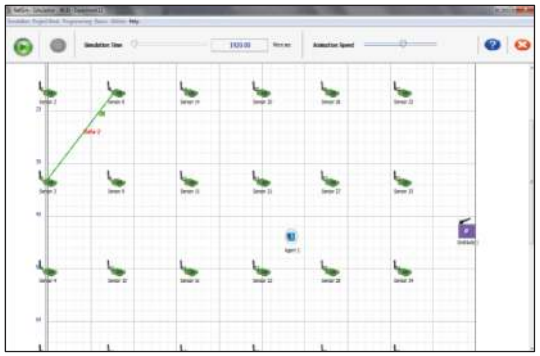

Figure 5: Node sending data to CH 8.

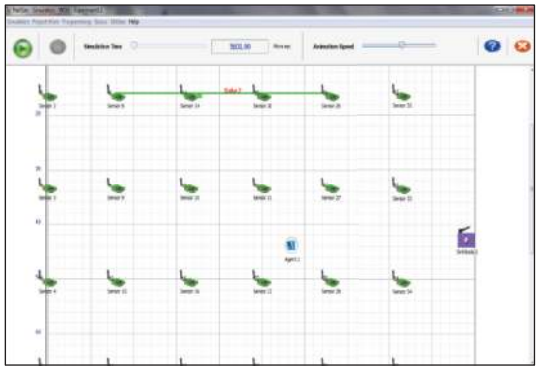

Figure 6: CH 8 sending data to BS.

5.2. Analysis. To analyze the proposed algorithm, the recorded values during the simulation are taken. Table 3 lists the values of the LEACH normal operation and also the values recorded after launching the coordinated sinkhole attack and attack on a single CH, respectively.

The nodes in Table 3, N_8, N_{11}, N_{26}, and N_{29}, denote the CH nodes and the node N_{37} indicates the BS which does not forward any data, so its PT_i value is 0. For the analysis of the results, three different scenarios are considered.

5.2.1. Results and Discussion. The results are analyzed in three different scenarios, that is, normal operation, coordinated sinkhole attack, and single node sinkhole attack.

LEACH Normal Operation. Consider CH 8: applying the algorithm for the values listed in Table 3, the IR is calculated using (2):

$$P_8 = \frac{67}{77}, \tag{5}$$

$P_8 = 0.87$, where the ratio value is a numeric value which shows sensor 8 is a normal node, since the packets are transmitted.

Consider CH 11: the IR value is calculated using (2):

$$P_{11} = \frac{65}{74}, \tag{6}$$

$P_{11} = 0.88$, which indicate a numeric value which proves node N_{11} is a normal node. This process is repeated for other two nodes N_{29} and N_{26}. The result is a numeric value which proves them as attack-free nodes.

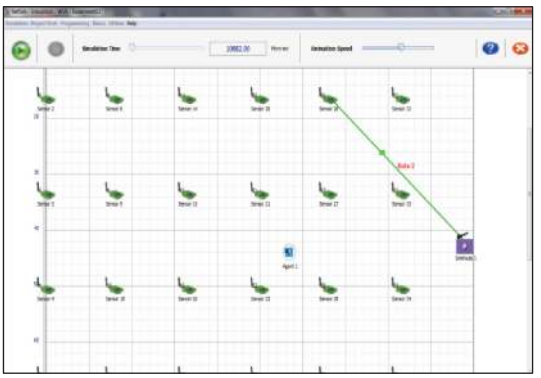

Figure 7: CH 26 sending data to BS.

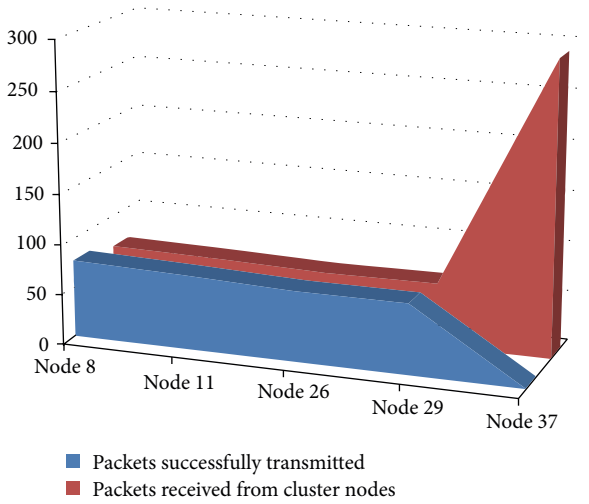

Figure 8: Normal LEACH operation.

Table 3: Comparison of normal and threat operation in LEACH protocol.

Cluster head (CH)	N_8		N_{11}		N_{26}		N_{29}		N_{37} (BS)	
	PT_i	PR_i	PT_i	PR_i	PT_i	PR_i	PT_i	PR_i	PT_i	PR_i
LEACH normal operation	77	67	74	65	70	62	70	63	0	291
Coordinated sinkhole attack	0	67	0	65	0	59	0	62	0	0
Sinkhole attack on CH 8	0	67	74	65	69	61	69	60	0	212

Coordinated Sinkhole Attack. Calculate the IR for CH 8 from Table 3 using (2):

$$P_8 = \frac{67}{0}, \qquad P_8 = \infty. \tag{7}$$

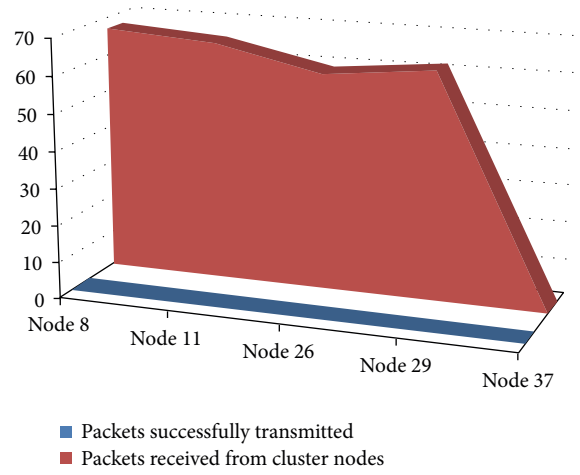

Figure 9: Coordinated sinkhole attack.

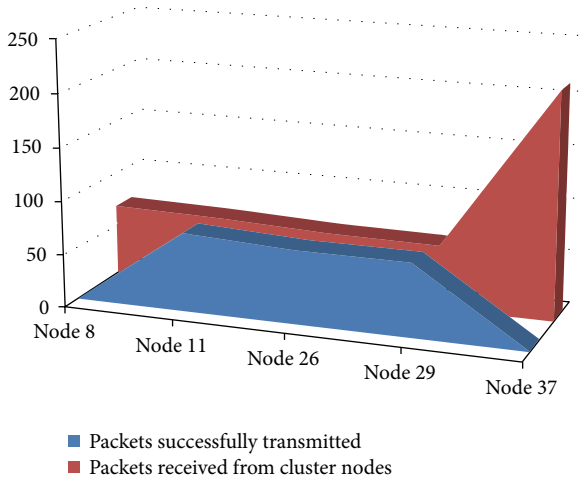

Figure 10: Sinkhole attack on CH 8.

The IR value is "∞" which shows packet dropping had occurred ($PT_i = 0$) and hence CH 8 is compromised.

Consider the CH 11: from (2),

$$P_{11} = \frac{65}{0}, \tag{8}$$

$P_{11} = \infty$, which shows the occurrence of malicious activity. This process is repeated for the other two nodes N_{29} and N_{26}. The result is an infinite value (∞) which proves them as sinkhole nodes. Hence coordinated sinkhole attack is identified.

Sinkhole Attack on CH 8. Calculating the IR for values in Table 3 for CH 8, from (2)

$$P_8 = \frac{67}{0}, \tag{9}$$

$P_8 = \infty$, which shows the presence of a sinkhole node.

Consider CH 11. The IR value is calculated using (2),

$$P_{11} = \frac{65}{74}, \tag{10}$$

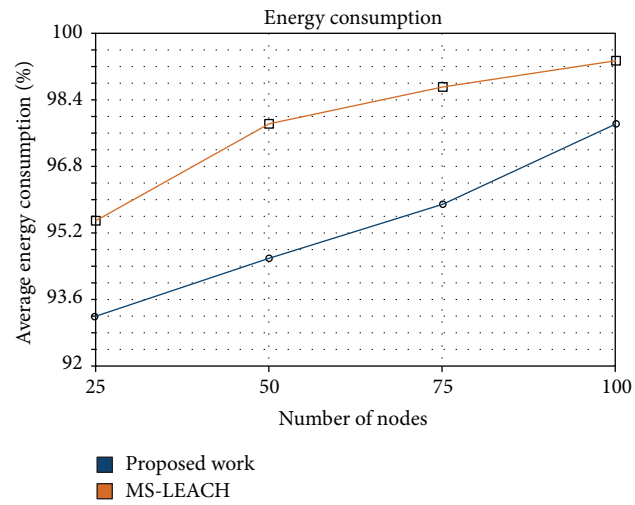

Figure 11: Average energy consumption rate comparison.

$P_{11} = 0.87$, which indicate an integer proving node N_{11} is a normal node. This process is repeated for other two nodes N_{29}, N_{26}. The result is an integer which proves them as attack-free nodes and these analyses prove that the attack is launched only on CH 8. The above analysis proves the correctness of the proposed algorithm.

5.3. Performance Evaluation. The recent method to detect the sinkhole attack in LEACH based network is MS-LEACH which is an extension of S-LEACH. The S-LEACH is the first security extension of LEACH and it follows the SPIN building blocks for its security features. MS-LEACH adapts pairwise key establishment method to provide data confidentiality and authentication for cluster member to CH. This protocol outperforms the S-LEACH in terms of power consumption, network throughput, and lifetime [47]. To compare our proposed scheme with the recent existing work, MS-LEACH is chosen. Since this protocol is the extension of S-LEACH and also provides detection of sinkhole attack, it would be a better work for our comparative study. For the performance comparison, three main metrics are used, namely, average energy consumption, average network lifetime, and average network throughput. The following section gives a brief comparison of the performance of the proposed scheme with the existing work.

5.3.1. Average Energy Consumption. The ratio of the energy consumed by all the sensor nodes to the amount of the total startup energy is the average energy consumed by the nodes. Figure 11 shows that the proposed scheme consumes around 2% less energy compared to MS-LEACH.

The proposed scheme allows the computation to be performed on the BS. Since the BS is the powerful energy resource, it performs all the computation effectively. In the proposed work, the cluster members and CH are not involved in the computation process, so the energy consumption by the sensor nodes is very minimal and proves to be energy efficient method.

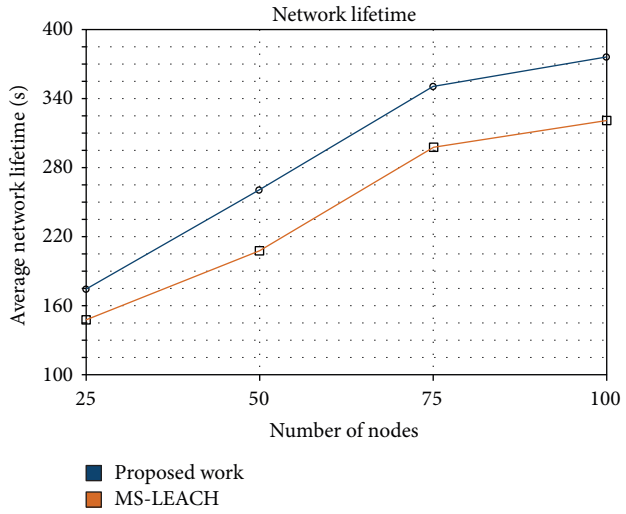

Figure 12: Average network lifetime comparison.

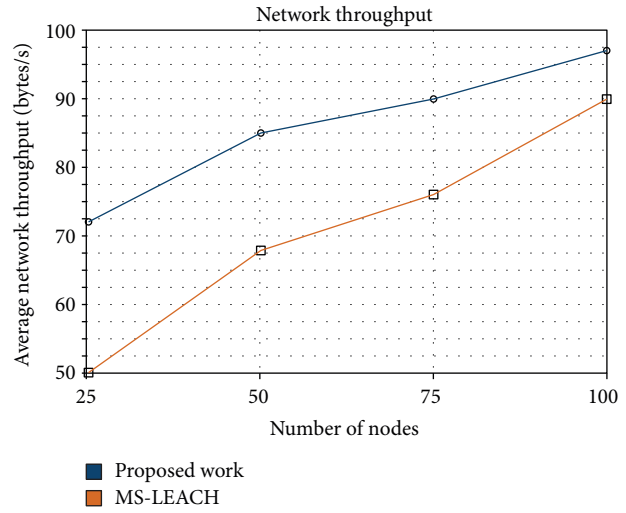

Figure 13: Average network throughput comparison.

5.3.2. Average Network Lifetime. The average network lifetime is the total time period between the start of the simulation process and the termination of the process due to energy depletion. Figure 12 shows the comparison of network lifetime between the proposed scheme and the MS-LEACH protocol.

The proposed scheme holds network lifetime of about 52% more than MS-LEACH which makes the network extend the lifetime and makes the sensor nodes alive for a long period.

5.3.3. Average Network Throughput. The network throughput is the ratio of the total data received to the certain period of time. The proposed scheme detects the sinkhole nodes at the earliest and minimizes the packet drop rate. So, the network throughput increases gradually compared to MS-LEACH.

Figure 13 shows that the proposed scheme increases the network throughput by 15% more than MS-LEACH since it uses lightweight IDS to detect the intrusion quickly. The throughput is the important metric to compare the effectiveness of the proposed work with the existing work, since the proposed IDS deals with the packet dropping attack.

In summary, the proposed work outperforms the existing MS-LEACH in terms of less energy consumption, extended network lifetime, and increased network throughput.

6. Conclusion and Future Work

WSNs are easily prone to security breach like sinkhole attack. Thus an IDS mechanism has been proposed that identifies such attacks on LEACH protocol and alerts the normal sensor node to reduce the data loss rate. The TETCOS NETSIM simulator has been used for the analysis, where the sinkhole attack and IDS were launched. The simulation result shows that the vulnerability like sinkhole attacks on LEACH drops all the transmitted packets across the CH. The proposed IDS captured the sinkhole nodes with the minimum computation and alerted the normal sensor nodes. Since the computation of proposed IDS is simple, it consumes less energy, whereas the network lifetime can be extended as compared to the existing work, namely, MS-LEACH. In addition, the numerical analysis proves that the proposed IDS can achieve minimum computational overhead and less energy consumption. In future, the proposed algorithm can be extended towards the detection of selective forwarding attack which alters fragment of the data and snooze attack, respectively.

Important Notations Used

nc: Number of clusters
p: Probability of sensor node to be elected as CH
P_i: Intrusion ratio (IR)
PR_i: Packets received by the ith CH
PT_i: Packets transmitted by the ith CH
N_i: CH node ID's
SN_i: Sensor node or cluster members
S_n: Sensor network
C_i: Cluster.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgment

The authors would like to acknowledge SASTRA University for the great support and assistance rendered to carry out this research work.

References

[1] E. C. H. Ngai, J. Liu, and M. R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor

networks," *Computer Communications*, vol. 30, no. 11-12, pp. 2353–2364, 2007.

[2] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2-3, pp. 293–315, 2003.

[3] G. Padmavathi and D. Shanmugapriya, "A survey of attacks, security mechanisms and challenges in wireless sensor networks," *International Journal of Computer Science and Information Security*, vol. 4, no. 1-2, 2009.

[4] N. A. Alrajeh, S. Khan, and B. Shams, "Intrusion detection systems in wireless sensor networks: a review," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 167575, 7 pages, 2013.

[5] J. A. Chaudhry, U. Tariq, M. A. Amin, and R. G. Rittenhouse, "Dealing with sinkhole attacks in wireless sensor networks," *Advanced Science and Technology Letters*, vol. 29, pp. 7–12, 2013.

[6] M. Dener, "Security analysis in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2014, Article ID 303501, 9 pages, 2014.

[7] T. Singh and H. Kaur Arora, "Detection and correction of sinkhole attack with novel method in WSN using NS2 tool," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 2, pp. 32–35, 2013.

[8] S. A. Salehi, M. A. Razzaque, P. Naraei, and A. Farrokhtala, "Detection of sinkhole attack in wireless sensor networks," in *Proceedings of the 3rd IEEE International Conference on Space Science and Communication (IconSpace '13)*, pp. 361–365, Melaka, Malaysia, July 2013.

[9] P. Maidamwar and N. Chavhan, "Impact of wormhole attack on performance of LEACH in wireless sensor networks," *International Journal of Computer Networking, Wireless and Mobile Communications*, vol. 3, no. 3, pp. 21–32, 2013.

[10] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor network," in *Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors '07)*, vol. 4837, pp. 150–161, Wrocław, Poland, 2007.

[11] S. Iqbal, S. P. Aravind Srinivas, G. Sudharsan, and S. S. Kashyap, "Comparison of different attacks on LEACH protocol in WSN," *International Journal of Electrical, Electronics and Data Communication*, vol. 8, no. 8, pp. 16–19, 2014.

[12] X. Deng, R. Wu, W. Wang, and R. Bu, "An intrusion detection system for cluster based wireless sensor networks," *Information Technology Journal*, vol. 12, no. 9, pp. 1764–1771, 2013.

[13] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644–653, 2014.

[14] V. K. Jatav, M. Tripathi, M. S. Gaur, and V. Laxmi, "Wireless sensor networks: attack models and detection," in *Proceedings of IACSIT Hong Kong Conferences*, vol. 30, pp. 144–150, 2012.

[15] M. Bahekmat, M. H. Yaghmaee, A. S. H. Yazdi, and S. Sadeghi, "A novel algorithm for detecting sinkhole attacks in WSNs," *International Journal of Computer Theory and Engineering*, vol. 4, no. 3, pp. 418–421, 2012.

[16] E.-N. Huh, T. H. Hai, and M. Jo, "A lightweight intrusion detection framework for wireless sensor networks," *Wireless Communications and Mobile Computing*, vol. 10, no. 4, pp. 559–572, 2010.

[17] M. R. Rohbanian, M. R. Kharazmi, A. Keshavarz- Haddad, and M. Keshtgary, "Watchdog-LEACH: a new method based on LEACH protocol to secure clustered wireless sensor networks," *Advances in Computer Science*, vol. 2, no. 3, pp. 105–117, 2013.

[18] S. Lee, Y. Lee, and S.-G. Yoo, "A specification based intrusion detection mechanism for the LEACH protocol," *Information Technology Journal*, vol. 11, no. 1, pp. 40–48, 2012.

[19] S. Gupta and V. Grover, "Survey of intrusion detection techniques in LEACH," *International Journal of Computer Trends and Technology*, vol. 17, no. 4, pp. 166–171, 2014.

[20] S. Ramachandran and V. Shanmugam, "An approach to secure leach using tesla based certificate," *Life Science Journal*, vol. 10, no. 2, pp. 1018–1027, 2013.

[21] M. A. Rassam, A. Zainal, M. A. Maarof, and M. Al-Shaboti, "A sinkhole attack detection scheme in mintroute wireless sensor networks," in *Proceedings of the 1st IEEE International Symposium on Telecommunication Technologies (ISTT '12)*, pp. 71–75, 2012.

[22] S. Sharmila and G. Umamaheswari, "Detection of sinkhole attack in wireless sensor networks using message digest algorithms," in *Proceedings of the International Conference on Process Automation, Control and Computing (PACC '11)*, pp. 1–6, Coimbatore, India, July 2011.

[23] D. U. S. Rajkumar and R. Vayanaperumal, "A leader based monitoring approach for sinkhole attack in wireless sensor network," *Journal of Computer Science*, vol. 9, no. 9, pp. 1106–1116, 2013.

[24] A. Thomas Paul Roy and K. Balasubadra, "DRPGAC: detecting and preventing malicious activities in wireless sensor networks," *Journal of Theoretical and Applied Information Technology*, vol. 69, no. 1, pp. 143–150, 2014.

[25] S. Sahraoui and S. Bouam, "Secure routing optimization in hierarchical Cluster-Based wireless sensor networks," *International Journal of Communication Networks and Information Security*, vol. 5, no. 3, pp. 178–185, 2013.

[26] S. Sharma and S. K. Jena, "A survey on secure hierarchical routing protocols in wireless sensor networks," in *Proceedings of the International Conference on Communication, Computing and Security (ICCCS '11)*, pp. 146–151, February 2011.

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

[28] A. Kaur and S. Saini, "Simulation of low energy adaptive clustering hierarchy protocol for wireless sensor network," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 7, pp. 1316–1320, 2013.

[29] M. Elhoseny, H. K. El-Minir, A. M. Riad, and X. Yuan, "Recent advances of secure clustering protocols in wireless sensor networks," *International journal of Computer Networks and Communications Security*, vol. 2, no. 11, pp. 400–413, 2014.

[30] S. Athmani, D. E. Boubiche, and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," in *Proceedings of the World Congress on Computer and Information Technology*, pp. 1–5, June 2013.

[31] M. Tripathi, M. S. Gaur, and V. Laxmi, "Comparing the impact of black hole and gray hole attack on LEACH in WSN," in *Proceedings of 4th International Conference on Ambient Systems, Networks and Technologies (ANT '13)*, vol. 19, pp. 1101–1107, June 2013.

[32] A. Jangra and P. Swati, "Securing LEACH protocol from sybil attack using jakes channel scheme (JCS)," in *Proceeding of International Conference on Advances in ICT for Emerging Regions*, pp. 79–87, Colombo, Sri Lanka, September 2011.

[33] S. Magotra and K. Kumar, "Detection of HELLO flood attack on LEACH protocol," in *Proceedings of the 4th IEEE International Advance Computing Conference (IACC '14)*, pp. 193–198, February 2014.

[34] M. Sankar, M. Sridar, and M. Rajani, "Performance evaluation of LEACH protocol in wireless network," *International Journal of Scientific & Engineering Research*, vol. 3, no. 1, 2012.

[35] W. Xinhua and W. Sheng, "Performance comparison of LEACH and LEACH-C protocols by NS2," in *Proceedings of the 9th International Symposium on Distributed Computing and Applications to Business Engineering and Science (DCABES '10)*, pp. 254–258, Hong Kong, China, August 2010.

[36] W. Heinzelman, *Application-specific protocol architectures for wireless networks [Ph.D. dissertation]*, Massachusetts Institute of Technology, 2000.

[37] M. Tong and M. Tang, "LEACH-B: an improved LEACH protocol for wireless sensor network," in *Proceedings of 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM '10)*, pp. 1–4, Chengdu, China, September 2010.

[38] L. Qing, Q. Zhu, and M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks," *Computer Communications*, vol. 29, no. 12, pp. 2230–2237, 2006.

[39] D.-S. Kim and Y.-J. Chung, "Self-organization routing protocol supporting mobile nodes for wireless sensor network," in *Proceedings of the 1st International Multi-Symposiums on Computer and Computational Sciences (IMSCCS '06)*, vol. 2, pp. 622–626, Hanzhou, China, June 2006.

[40] R. V. Biradar, D. S. R. Sawant, D. R. R. Mudholkar, and D. V. C. Patil, "Multi-Hop routing in self-organizing wireless sensor networks," *International Journal of Computer Science Issues*, vol. 8, no. 1, pp. 154–164, 2011.

[41] N. Kumar and J. Kaur, "Improved LEACH protocol for wireless sensor networks," in *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '11)*, pp. 1–5, September 2011.

[42] N. Sindhwani and R. Vaid, "V LEACH: an energy efficient communication protocol for WSN," *Mechanica Confab*, vol. 2, no. 2, pp. 79–84, 2013.

[43] H. Dhawan and S. Waraich, "A comparative study on LEACH routing protocol and its variants in wireless sensor networks: a survey," *International Journal of Computer Applications*, vol. 95, no. 8, pp. 21–27, 2014.

[44] A. C. Ferreira, M. A. Vilaça, L. B. Oliveira, E. Habib, H. C. Wong, and A. A. Loureiro, "On the security of cluster-based communication protocols for wireless sensor networks," in *Proceedings of the 4th IEEE International Conference on Networking (ICN '05)*, vol. 3420 of *Lecture Notes in Computer Science*, pp. 449–458, 2005.

[45] M. A. Abuhelaleh, T. M. Mismar, and A. A. Abuzneid, "Armor-LEACH—energy efficient, secure wireless networks communication," in *Proceedings of the 17th International Conference on Computer Communications and Networks (ICCCN '08)*, pp. 1–7, St. Thomas, Virgin Islands, USA, August 2008.

[46] K. Zhang, C. Wang, and C. Wang, "A secure routing protocol for cluster-based wireless sensor networks using group key management," in *Proceedings of the 4th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '08)*, pp. 1–5, October 2008.

[47] M. El-Saadawy and E. Shaaban, "Enhancing S-LEACH security for wireless sensor networks," in *Proceedings of the IEEE International Conference on Electro/Information Technology (EIT '12)*, pp. 1–6, IEEE, Indianapolis, Ind, USA, May 2012.

[48] L. B. Oliveira, A. Ferreira, M. A. Vilaça et al., "SecLEACH-on the security of clustered sensor networks," *Signal Processing*, vol. 87, no. 12, pp. 2882–2895, 2007.

[49] V. Pal, S. Aishwarya, and S. Jain, "Signal strength based HELLO flood attack detection and prevention in wireless sensor networks," *International Journal of Computer Applications*, vol. 62, no. 15, pp. 1–6, 2013.

[50] W. Wang, F. Du, and Q. Xu, "An improvement of LEACH routing protocol based on trust for wireless sensor networks," in *Proceedings of the 5th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '09)*, pp. 1–4, September 2009.

[51] A. M. El-Semary and M. M. Abdel-Azim, "New trends in secure routing protocols for wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, Article ID 802526, 16 pages, 2013.