Indian Journal of Science and Technology, Vol 8(23), DOI: 10.17485/ijst/2015/v8i23/72533, September 2015
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

A Hybrid Zone based Leader for Monitoring Sinkhole Attack in Wireless Sensor Network

D. Udaya Suriya Raj Kumar[1*] and Rajamani Vayanaperumal[2]

[1]Department of Computer Science and Engineering, Sathyabama University, Chennai - 600119, Tamil Nadu, India; u_suriya@yahoo.com
[2]Department of Electronic and Communication Engineering, Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai 600062, Tamil Nadu, India; rajavmani@gmail.com

Abstract

Objectives: The main aim of this paper is security by applying Intelligent Intrusion detection System to detect one of the critical attack know as sinkhole attack in Wireless Sensor network. **Methods/Analysis:** The major problem occurs while transmitting the data is security. The malicious node attracts the packets from the other normal sensor nodes and drops the sensitive packets which may leads to selective forwarding attack and black hole attack. **Findings:** In the existing system, Leader based intrusion detection system is used to monitor the surrounding node. Here the leader can monitor the nodes only region wise and does not have any clustering technique. By using the clustering technique we can monitor the surrounding nodes in efficient manner and better solution. In the proposed system, an Intelligent Intrusion Detection System (IIDS) mechanism to detect the intruder in the network, which uses a Hybrid Approach to detect and prevent sinkhole attack, with two approaches such as Zone-Based Leader Election Method and Leader Based Monitoring. In Zone-Based Leader Election method, a set of nodes is located in different regions and a Cluster Based Zone Leader (CBZL) is allocated to every region in the network. In the Leader Based Monitoring Approach, when a node gets detected as a compromised node, it communicates the status of that node to the other leader within the WSN. **Application/Improvement:** This technique can identify the intruder node and improve the efficiency of the network. As a simulation results, we are implementing in Network Simulator. In environment monitoring and military applications the proposed approach can be deployed.

Keywords: Cluster Zone-based Leader, Leader based Monitoring Approach, Sinkhole Node, Wireless Sensor Network

1. Introduction

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 secures data aggregation[1]. The IDS forms a second level of defense to the network and alerts it 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 on the tasks of characteristics like detection rate, false alarm rate, computational capability, energy consumption rate, etc[2,3]. One of the important low level security mechanisms is the 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[4].

*Author for correspondence

This paper focuses on the high level defense mechanism, namely, IIDS, used for detection of 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 the case of insider attacks, where a node is free to manipulate the packets and gain control over them. Most routing protocols in the sensor network do not initiate any mechanism for detecting security attacks. Encryption methodologies and authentication system and prove to be ineffective 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 the sinkhole attack in a WSN which uses two mechanisms. Sinkholes are induced in a WSN either by insiders or by an external attacker. The proposed IIDS algorithm detects the sinkhole attack with a 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:

- A lightweight IIDS is proposed with minimal computational complexity.
- The proposed lightweight IIDS is capable of capturing multiple attacks.
- Cluster Based Zone Allocation method (CBZA) for energy conservation and packet dropping in WSN where a Zone Leader (CBZL) is allocated to every region in the network.
- Proposed Leader Based Monitoring Approach compares and calculates the behavior of every node makes a logical execution of the detection module and monitors each node behavior within the cluster for any sinkhole attack to occur.

This paper is structured as follows Section 2 describes the Literature Survey on sinkhole attacks. A description of Research background, Research motivation and proposed approach are presented in Section 3. Section 4 shows the Experimental Results and discussion of proposed algorithm. In Section 5, conclusion and future work are given.

2. Materials and Method

An efficient IDS algorithm with low overhead was proposed to checks the data consistency and captures the intruder by verifying the network flow information. The algorithm is also robust in the presence of multiple malicious nodes. Different ways for launching the sinkhole attack are discussed[5]. The BS is identified as the trusted member in the network. Based on the sequence number, the sinkhole attack is 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.

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[6]. A separate tunnel is created by the attacker through which data is transferred to the wormhole nodes. The wormhole attack can also be used for launching the sinkhole attack by making one of the wormhole nodes a sinkhole. IDS to detect the sinkhole attack in the WSN which uses Mint route protocol for its routing operation was proposed[7]. 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 was 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[8]. 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 viz., normal operation and under attack. The proposed IDS integrate node behavior strategies and evidence theory[9]. The multidimensional behavior characteristics are collected for calculation of its deviation from 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.

The second approach is of the mitigation type is used for identification of the intruders from the affected region. The author's in[10] propose IDS for detection of the sinkhole attack. The sinkhole attack is launched on the Mint route protocol by advertising a better link quality and changing the link quality value of the current parent node to the worst value. They propose rule-based IDS for detection of the sinkhole node. The authors also analyze the selective forwarding and black hole attacks on the Mint route protocol. They have developed IDS to detect the attacks. The authors propose IDS to capture the sinkhole node which set itself as a fake BS[11]. 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 to see if any changes have been made to the control fields, and then the IDS alert the presence of a malicious node.

An IDS agent on each sensor node has two intrusion detection modules, namely, local agent and global agent[12]. 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. The authors propose decentralized IDS which have watchdog modules residing in the monitor nodes[13]. These nodes analyze the behavior of other nodes including Cluster Head (CH). On their detection of an attack, the monitor node forwards an alarm to the BS and adds the compromised node to the blacklist.

The blacklisted nodes are also broadcast to all other nodes to avoid further communication. The author's in[14] propose IDS to identify the malicious activities according to the various phases of LEACH protocol. The CH selection for each round is done according to the energy level. When the same sensor node is selected as CH for the second time consecutively, it may be a compromised node. Malicious node sends strong signal and 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 Time Division Multiple Access (TDMA) schedule within a certain period of time, the CH may be a malicious node.

The authors list three works related to IDS on the LEACH protocol. A watchdog based IDS are proposed for capturing the attack on each phase by applying the rules and secondly a specification based IDS are 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[15]. The sensor nodes send the data along with the node membership certificate to the CH. By then, the CH aggregates and transfers the sensed data to the BS. The author's in[16] propose IDS by analyzing the detection rules in different architectures. They have verified their work by identifying the sinkhole nodes on the Mint route protocol with less resource consumption. In[17], cryptographic based IDS are proposed for detection of 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 the sinkhole node.

The author's in[18] propose centralized monitoring approach for detection of 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. A Threshold based Hierarchical IDS (THIDS) is proposed in[19] for detection of the selective forwarding, black hole, and sinkhole attacks. Each sensor node has a local list called Isolate list for storing 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 is sent to the neighboring nodes indicating the presence of sinkhole node.

3. Research Background

In this section, a description of sinkhole attack and the motivation of the research work are presented.

3.1 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. The compromised node grabs attention from the other nodes by establishing itself to have a high value with respect to the routing metric. Various methods are present for launching the sinkhole attack, either by directly giving false information about the routing metric to the sender nodes or by using a wormhole attack. The wormhole threat creates a separate link from the normal network link and starts 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 1 shows sinkhole attack (launched by compromised node).

The compromised node sends 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[20]. The sinkhole node can also be used as a platform for launching other threats like forwarding the packets

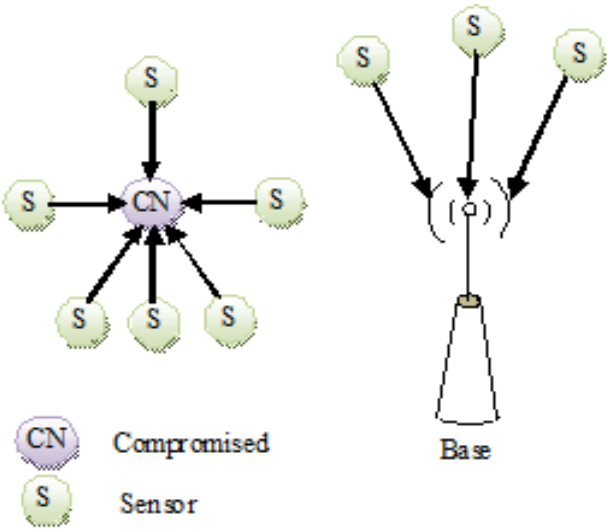

Figure 1. Sinkhole attack.

selectively or deleting some fields in the packet. This kind of attack is called selective forwarding. This research work focuses on the analysis of the adverse effects of the sinkhole attack on LEACH protocol and develops an efficient defense mechanism for the mitigation 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 is launched in the Mint route 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.

In the case of the proposed IIDS, the sinkhole attack can be launched using the CHs. The compromised node projects itself with a high energy value and gets selected as the CH. This compromised CH acts as a sinkhole node and performs the attack by dropping or altering the sensed data received from its cluster members. The sinkhole attack can be launched in other routing protocols. An efficient defense mechanism is needed to counter this attack.

3.2 Research Motivation

The network layer has much potential vulnerability like sinkhole attack, black hole attack, selective forwarding, Sybil, HELLO flood, wormhole and so on. The purpose of the 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. It can be extended further with the attacks like selective forwarding, black hole, and HELLO flood to devastate the network transmission. Hence, 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.

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, Armor-LEACH, R-LEACH, MS-LEACH, and Sec-LEACH. The non-cryptographic methods are signal strength based approach and TM-LEACH. But, they do 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. Hence, this research focuses on the development of IIDS in turn to reduce the adverse effects with minimum resource utilization.

3.3 Proposed Intelligent Intrusion Detection System Design

Security is the prime concern in a wireless network. 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 two effective approaches, the attack effects and developing an IIDS to minimize the adverse effects.

3.3.1 Cluster based Zone Allocation and Zone Leader Election Method

In Cluster based Zone Allocation method (CBZA), zones are formed and packet transmission occurs over the routing process. In MDR, packet loss increases due to link failure and packet delivery ratio decreases. End to end delay becomes very high. So, overall packet transmission time gets increased and overall network efficiency gets reduced. In CBZA, when the zones are formed, it split into four regions.

The packet transmission takes place into the regions and, the next region starts its transmission only, when the transmission in first region is completed. Each region has a Cluster Head (CH) which controls packet transmission and the reception through it. This method helps identification of a packet when lost. But in MDR, the detection of lost packet is somewhat a critical process.

CBZA has low packet loss when compared to MDR. So, the end to end delay and packet transmission time is reduced. Incidentally, the network throughput or efficiency can be increased. Normally, in network infrastructure, nodes are deployed and source and destinations are allocated. Then, a single node acts as a router or agent. In group management, a set of nodes are initialized at a particular region or in four regions. Each region has a Zone Leader (ZL) and zone members. Zone Leader election is conducted among the nodes in the zone and a particular node will elected as a Zone Leader depending on its energy level which is called threshold value. Except the Zone Leader other nodes will behave as neighbors or coordinators. When the routing process/packet transmission is commenced through the network, zone members are coordinated with each other and a Request/Response process is performed by coordinators. Finally, every packet transmission like entering and exceeding packets is operated by the Zone Leader as they are passed through it. The above process is then repeated. In this approach nodes, share their IDs and energy value using broadcast messages. After a random period, the node with maximum energy level is elected Leader. If two nodes have the same energy level, the node having the maximum number of neighbors is elected Leader. Zone Formation Cluster Allocation with Leader Election is illustrated in Figure 2.

3.3.2 A Leader based Intelligent Intrusion Detection System

There are many intrusion detection systems developed for WSN. In this study Leader Election Mechanism is used for the LBIIDS approach. In this mechanism, a leader is elected for solving the IDS in the WSN, which is a cost effective and resource effective approach. Figure 3 gives an overview of working principles of the proposed LBIIDS. Recent routing protocols face security issues in the presence of multiple sink or BS and node mobility. The proposed LBIIDS works satisfactorily 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 received from the normal sensor nodes. The CH collects the data from the cluster member and later analyzed by the BS. Algorithm for Intelligent Intrusion Detection System (IIDS) is shown in Table 1.

The IIDS agent that runs in the BS receives the packets by overhearing the transmission of the cluster members and CH nodes. The IDS agent contains ratio a 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 for calculation of the IR. The ratio gauge sends the IR value to the detection engine. With that, it is clear that the regions and the common cluster, region wise cluster and the Info Table ($Table_{info}$) store the ID. The location of the nodes is shown in Figure 4. Whenever a node starts communication in the network, the clusters can verify the Table and permit various phases of leader based algorithm. The detection engine triggers the alarm

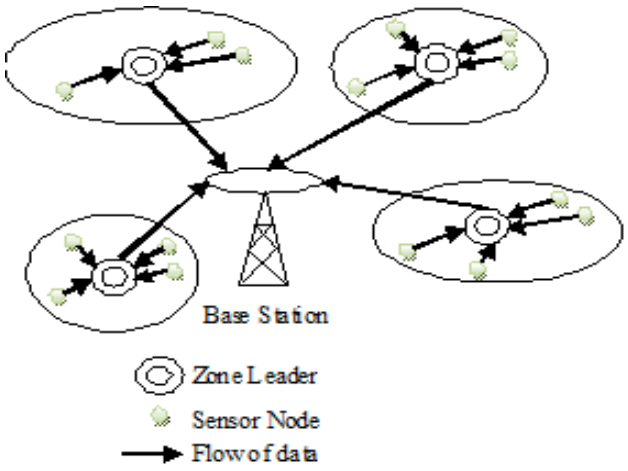

Figure 2. Zone formation cluster allocations with leader election.

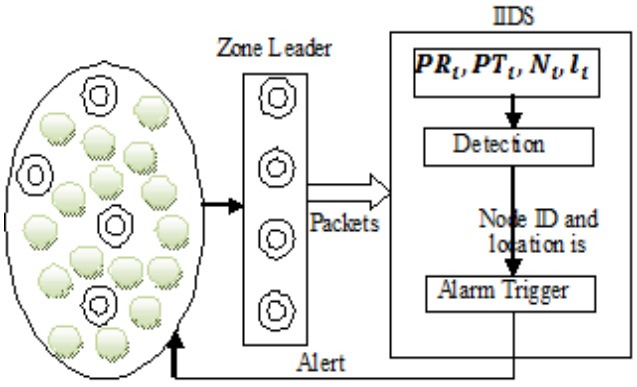

Figure 3. Leader based intelligent intrusion detection system architecture.

Table 1. Shows Node ID table

Node ID	N1	N2	N3	N4	..	..	Ni	..	Nm
Location	1,2	34,45	5,6	76,56	43	5,87	88,98	34,13	43,44

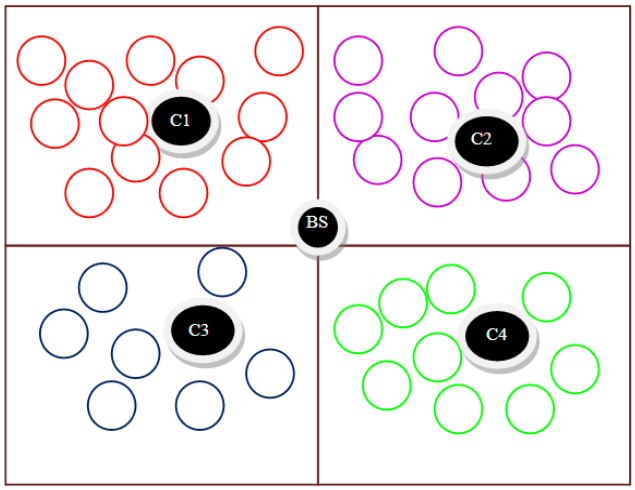

Figure 4. Zone leader election in wireless sensor network.

which depends upon the IR value indicating the presence of compromised node.

3.3.3 *Algorithm for Intelligent Intrusion Detection System*

Procedure call cluster based zone allocation method()
Set of nodes are initialized at particular region
Zone leader election → Energu level E(N)
If (E(N1)=E(N2)
Then
Select the node which has Maximum numberof neighbors as a Leader (L)
Else
The node with maximum energy level in each zone will be elected as a Leader (L)
End
Procedure Call LBIIDS ()
Repeat
time delay (100)
For ∀ (Li)
Receive (PRi,PTi,Ni,Li)Packets from L
Calculate IRi= $\frac{PRi}{PTi}$
If ($IR_i \rightarrow \infty$ & $l_i \neq T_{info}$)then
Corresponding Ni is the Sink Node
Isolate Ni
Send Warning Message to the Remaining Cluster Member node about Ni
Else
Corresponding Ni is not Sink Node
End if
End for
Until Node's Transmission Process Complete
End

The IIDS agent module runs in the BS to identify the intrusion by analyzing the data packets that consists of PR_i, PT_i, N_i and l_i periodically. The packet transmission value of L (PR_i), the packet reception value of L (PT_i), and the node identification of the L (N_i) and location of the nodes in the zone (l_i) are used to validate the Intrusion Ratio (IR) as numeric or not by the IIDS 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 is a possibility of a selective forwarding attack. The purpose of the above strategy is to minimize the intrusion ratio to enable isolation of the intruder node in the next round of data transmission and blocked from the leader selection process by the BS. The proposed IIDS mechanism alerts the respective cluster members regarding the presence of sinkhole node to stop further data transmission. Moreover, this algorithm has much less computation for detection of the sinkhole node from the available information (local). It also increases the energy efficiency of the network by a quick identification of the compromised nodes. Since the proposed IIDS mechanism has less communication overhead between the sensor networks and the BS, the ratio gauge calculation is simple, making the computation easier which in turn reduces computational complexity to the further extent. Despite increase in node density of the sensor network, the proposed IIDS mechanism works efficiently to alert the threat deduction. The proposed IIDS has much less storage since its values are removed from the buffer after computing the IR value.

4. Experimental Results and Discussion

The proposed IIDS algorithm is implemented in NS2. LEACH, MS-LEACH is chosen for comparison of the proposal scheme with the currently available work. Three main metrics are used, for performance

comparison namely, average energy consumption, average network lifetime, average network throughput and Malicious Activity. The following section gives details of a brief comparison of the performance of the proposed scheme with the existing work. Table 2 shows the simulation setup. The following are the assumptions for simulation of the proposed IDS BS has the highest energy resource, all the sensor nodes are static, all the sensor nodes transfer data in the allocated frame, and Compromised nodes have higher energy level than normal sensor nodes.

4.1 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 5 shows that the proposed scheme consumes around 2% and 2.4% less energy compared to MS-LEACH and LEACH.

The proposed scheme allows the performance of computation on the BS. Since the BS is a powerful energy resource, it performs all the computation effectively. In the proposed work, the Leader is not involved in the computation process, and hence the energy consumption by the sensor nodes is very minimal and proves to be an energy efficient method.

Table 2. Simulation parameters

Parameters	Range
Number of Nodes	100
Base Station	1
Transmission Range	100m
Transmission Power	100m W

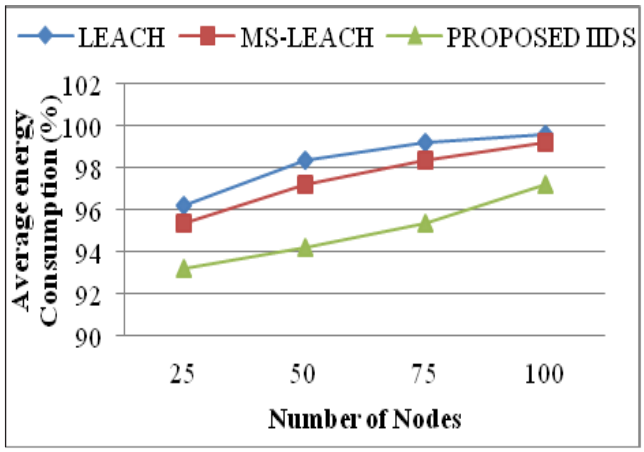

Figure 5. Average energy consumption rate comparison.

4.2 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 caused by energy depletion. Figure 6 shows the comparison of network lifetime between the proposed scheme, MS-LEACH protocol and LEACH.

The proposed scheme holds a network lifetime of about 19% and 49% more than MS-LEACH and LEACH which enables extension of the lifetime by the network and makes the sensor nodes alive for a long period.

4.3 Average Network Throughput

The network throughput is the ratio of the total data received to a known 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 and LEACH.

Figure 7 shows that the proposed scheme increases the network throughput by 10% and 24% more than

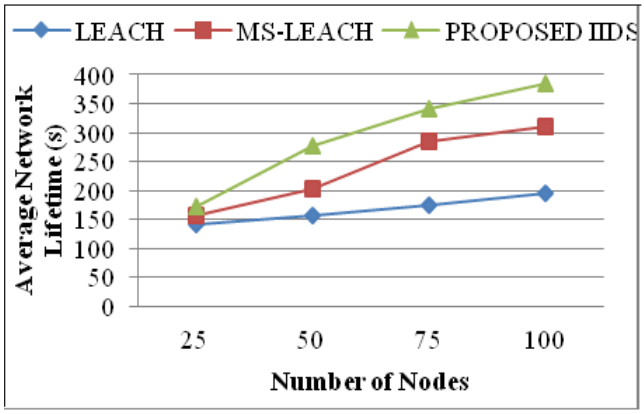

Figure 6. Average network lifetime comparisons.

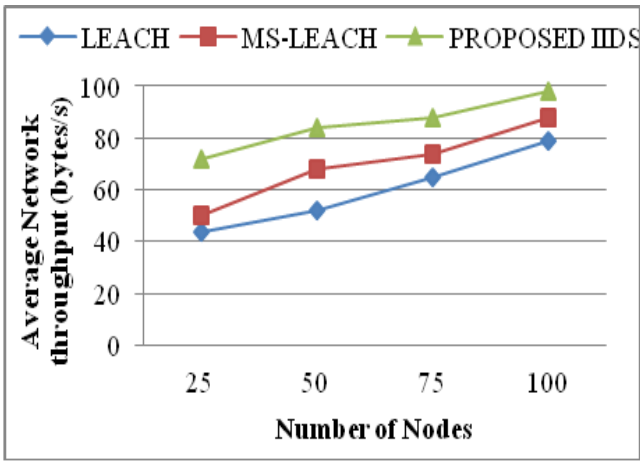

Figure 7. Average network throughput comparison.

MS-LEACH and LEACH, due to its usage of 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 IIDS deals with the packet dropping attack.

4.4 Malicious Activity Comparison

Figure 8 shows the number of malicious behavior occurring in the network when applying LEACH, MS-LEACH and the proposed IIDS. In order to detect malicious node the ID, some key points of each node is verified while transmitting and receiving a data packet. The proposed system maintains and compares a DB to compare the ID, key points for each node in the network. When a node is detected as malicious, it is blocked. The malicious node is reduced to be lower than the existing approach, as the proposed IIDS provides greater prevention instead of detection.

4.5 Detection Rate Comparison

Figure 9 depicts the percentage of malicious node detection by LEACH, MS-LEACH and proposed IIDS methods. The success rate of methods degrades when a large number of malicious nodes (Sinkhole nodes) are present in the network. This is due to the fact that the proposed IIDS work prefers to maximize its own utility and so has to lower the rate of false positives and false negatives detection and eventually it not misses more malicious nodes.

4.6 Prevention Efficiency Comparison

Figure 10 depicts the prevention efficiency comparison between LEACH, MS-LEACH and proposed IIDS methods. Prevention rate of the proposed work is higher than

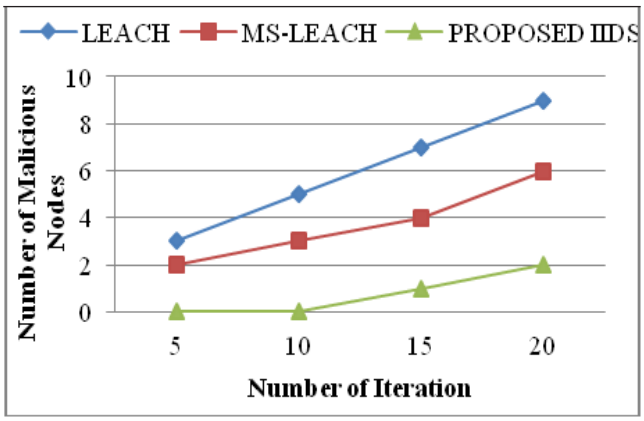

Figure 8. Malicious activity comparisons.

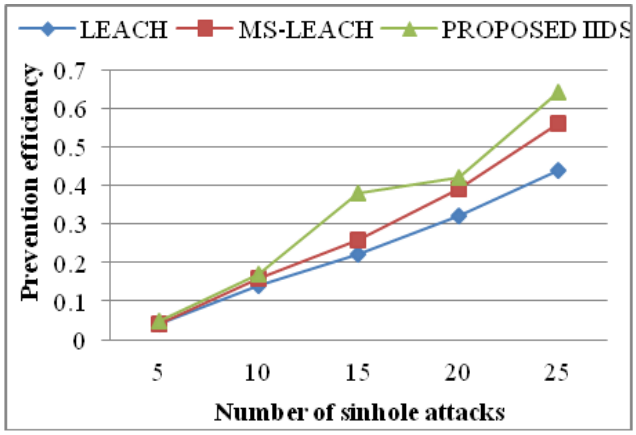

Figure 9. Detection rate comparison results.

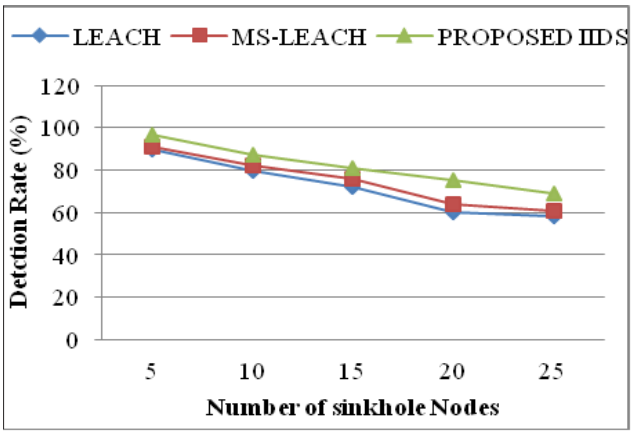

Figure 10. Prevention efficiency comparison results.

the LEACH and MS-LEACH method. When there is a sinkhole attack this is due to the fact that the proposed method having the Key points, so it has to higher the rate of prevention efficiency.

5. Conclusions and Future Work

An IIDS mechanism has been proposed for identification of such attacks and alerting the normal sensor nodes for reduction of data loss rate. The simulation result shows that the vulnerability like sinkhole attacks on WSN drops all the transmitted packets across the Leader. The proposed IIDS captures the sinkhole nodes with the minimum computation and alerts the normal sensor nodes. Since the computation of proposed IIDS is simple, it consumes less energy, whereas the network lifetime can be extended as compared to the existing work, namely, MS-LEACH and LEACH. In addition, experimental analysis proves that the proposed IIDS can help reducing

computational overhead and less energy consumption to the minimum. In future, the proposed algorithm can be extended for the detection of selective forwarding attack which alters a fragment of the data and snooze attack, respectively.

6. Acknowledgement

One of the Author Dr. V. Rajamani acknowledges the DST, India for sponsoring FIST Project, Veltech Multitech.

7. References

1. Padmavathi G, Shanmugapriya D. A survey of attacks, security mechanisms and challenges in wireless sensor networks. International Journal of Computer Science and Information Security. 2009; 4(1-2):1–9.
2. Alrajeh NA, Khan S, Shams B. Intrusion detection systems in wireless sensor networks: A review. International Journal of Distributed Sensor Networks. 2013; 10(1155):1–7.
3. Chaudhry JA, Tariq U, Amin MA, Rittenhouse RG. Dealing with sinkhole attacks in wireless sensor networks. Advanced Science and Technology Letters. 2013; 29(2):7–12.
4. Hemanta KK, Avijit K. Wireless sensor network security analysis. International Journal of Next-Generation Networks. 2009; 1(1):1–10.
5. Singh T, Kaur AH. Detection and correction of sinkhole attack with novel method in WSN using NS2 tool. Int J Adv Comput Sci Appl. 2013; 4(2):32–5.
6. Iqbal S, Aravind SSP, Sudharsan G, Kashyap SAS. Comparison of different attacks on LEACH protocol in WSN. International Journal of Electrical, Electronics and Data Communication. 2014; 2(8):16–9.
7. Krontiris I, Dimitriou T, Giannetsos T, Mpasoukos M. Intrusion detection of sinkhole attacks in wireless sensor network. Algorithm aspects of Wireless Sensor Network. 2008; 4837:150–61.
8. Maidamwar P, Chavhan N. Impact of wormhole attack on performance of LEACH in wireless sensor networks. International Journal of Computer Networking, Wireless and Mobile Communications. 2013; 3(3):21–32.
9. Shun-Sheng W, Kuo-Qin Y, Shu-Cing W, Chia-Wei L. An integrated intrusion detection system for cluster-based wireless Sensor Networks. Expert Syst Appl. 2011; 38(12):15234–43.
10. Shafiei H, Khonsari A, Derakhshi H, Mousavi P. Detection and mitigation of sinkhole attacks in wireless sensor networks. J Comput Syst Sci. 2014; 80(3):644–53.
11. Rohbanian MR, Kharazmi MR, Keshavarz-Haddad A, Keshtgary AM. Watchdog-LEACH: A new method based on LEACH protocol to secure clustered wireless sensor networks. Advances in Computer Science. 2013; 2(3):105–17.
12. Huh EN, Hai TH, Jo M. A lightweight intrusion detection framework for wireless sensor networks. Wireless Comm Mobile Comput. 2010; 10(4):559–72.
13. Bahekmat M, Yaghmaee MH, Yazdi ASH, Sadeghi S. A novel algorithm for detecting sinkhole attacks in WSNs. International Journal of Computer Theory and Engineering. 2012; 4(3):418–21.
14. Lee S, Lee Y, Yoo SG. A specification based intrusion detection mechanism for the LEACH protocol. Inform Tech J. 2012; 11(1):40–8.
15. Gupta S, Grover V. Survey of intrusion detection techniques in LEACH. Int J Comput Trends Tech. 2014; 17(4):166–71.
16. Rassam MA, Zainal A, Maarof MA, Al-Shaboti M. A sinkhole attack detection scheme in mintroute wireless sensor networks. 1st IEEE International Symposium on Telecommunication Technologies in Proceedings. Kuala Lumpur. 2012. p. 71–5.
17. Sharmila S, Umamaheswari G. Detection of sinkhole attack in wireless sensor networks using message digest algorithms. International Conference on Process Automation, Control and Computing in Proceedings; Coimbatore. 2011. p. 1–6.
18. Rajkumar USD, Rajamani V. A leader based monitoring approach for sinkhole attack in wireless sensor network. J Comput Sci. 2013; 9(9):1106–16.
19. Abhishekvarma GNS, Aswanikumarreddy G, Ravitheja Y, Arunkumar T. Cluster Based Multipath Dynamic Routing (CBDR) protocol for wireless sensor networks. Indian Journal of Science and Technology. 2015; 8(s2):17–22.
20. Syed ASS, Senthik KT, Sarfaraz AA. An energy efficient distributed routing algorithm based HAC clustering method for WSNs. Indian Journal of Science and Technology. 2014; 7(S7):66–75.