ISSN No:-2456-2165

# Two-way Authentication Algorithm for Sinkhole Attack Isolation in WSN

Semagn Shifere
Department of Computer Science
Woldia University, Ethiopia

Andebet Dessiewu
Department of Information Technology
Woldia University, Ethiopia

Tizazu Bayih
Department of Information Technology
Woldia University, Ethiopia

**Abstract:- Wireless sensor networks (WSN) are networks that are self-configuring and run without any central coordinator. Security and energy consumption are a big problem for wireless sensor networks because of these network properties. The malicious nodes that join the network cause security attacks.In terms of active and passive attacks, it is possible to distinguish attacks. In the active form of attack, the sinkhole assault. The malicious nodes in the sinkhole attack spoof the base station's identity and behave like the base station. Instead of base stations, the sensor nodes start transmitting data to malicious nodes. Cluster heads are chosen on the basis of energy, distance, to minimize energy consumption of the network LEACH protocol, which divides the entire network into clusters and clusters. Therefore, the total life of the network is decreased and the amount of energy consumed is increased when a sinkhole attack occurs.In this research paper, the latest method is designed to identify and isolate malicious nodes from the network. This algorithm works by using recognition to quickly classify attacks. The proposed algorithm is implemented in NS2 and those parameters are evaluated in terms of performance. As opposed to current techniques, our proposed technique performs well in terms of all parameters.**

***Keywords:-*** *Active, Attack, Sinkhole, Malicious, LEACH, WSN*

## I. INTRODUCTION

As of late, cellular network infrastructure and mobile communications have seen a flourishing evolution. A wireless sensor network is the array of various sensing devices in such a way that information relevant to the surrounding environment of a particular region can be known. They have the potential to change life and the complexities of system building. Different programs include sensor-based location detection with sensor networks, personal health screen and movement detection(J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang, 2014). Within these networks, the size of multiple limitations such as battery size, processors, memory storage of information and so on is significant. With the assistance of different optimization algorithms, the use of energy must be progressed within the networks.Inside the detected and routing data sent through the WSNs, different time constraints are present. Sensor nodes typically depend on a battery with a short lifespan, and because of physical constraints, their replacement is impractical.Furthermore, any number of sensor nodes must be able to scale up the design and protocol of the sensor networks. As the lifetime of the battery can be extended on the off chance that one can find out how to minimize the contact calculation(Dr. G. Padmavathi, Mrs. D. Shanmugapriya, 2009). Consumption can be minimized in the sensing energy subsystem by using low-power hardware components for energy-efficient routing protocols, such as Hybrid Energy-Efficient Distributed (HEED).Clustering involves grouping nodes into clusters and regularly selecting cluster heads so that people from a cluster can talk to their cluster heads, and these cluster heads send to a base station aggregated data obtained from their individuals.There is a cluster head in each cluster, and from that cluster there are individual rest nodes. Clustering results in a two-level order in which the higher level is formed by cluster heads while component nodes frame the lower level.(G.H. Raghunandan, IEEE 2011). Compared to component nodes, because the cluster head constantly transmits data over longer separations, they lose more energy. The clustering technique is used to minimize the consumption of resources. LEACH is the protocol that is the most powerful wireless sensor network clustering protocol.The cluster heads in the LEACH protocol are selected randomly on the network. The head of the cluster gets its sensor nodes based on size. Under the cluster head will come the nodes which are nearest to the cluster head. On the basis of energy, the clusters are randomly modified.The cluster heads in the LEACH protocol are picked at random on the network. Based on size, the cluster head gets its sensor nodes. Under the cluster head, the nodes that are nearest to the cluster head will come. On the basis of energy, the clusters are altered randomly.Safety assaults are commonly known as active and passive assaults. Active attacks are those that significantly decrease the efficiency of the network in terms of different parameters. Passive attacks are those that do not impact the efficiency of the network, but can cause active attacks in the future.

**A wormhole attack** enables an attacker to form a tunnel between two distant WSN locations, and the packets are transmitted through an in-band or out-of-band channel using that tunnel. (Dong D, 2008). Thus, the wormhole tunnel forms a pair of attackers. A misapprehension that they are similar to each other makes two distant nodes; however, it is not so in reality. The current wormhole will

then draw a significant amount of network traffic to WSN and move through it.

**Blackhole and Grayhole**: In this attack, during the path-finding phase or in route update messages, a malicious node falsely advertises good paths to the destination node. The malicious node could have the aim of hindering the path-finding process or intercepting all the data packets sent to the appropriate destination node. The grayhole attack is regarded as a more delicate form of this attack, where the malicious node drops the data packets intermittently, making their detection much more difficult.

**Sinkhole Attack:** An attacker makes a compromised node appear more appealing to its neighbors in a sinkhole attack by forging the routing information. The result is that the neighboring nodes select the compromised node to route their data via the next-hop node.Selective forwarding is very easy for this form of attack, since all traffic from a wide area of the network will pass via the compromised node. For these reasons, the researcher wants to work with a two-way authentication algorithm to build WSN's energy-efficient and more effective sinkhole isolation algorithm that improves network performance.

## II. RELATED WORK

Research works performed by various researchers and connected to these works are presented in this section. There are a number of works in WSN that are carried out in the field of protection.

According to Annie Mathew et.al, within a sensor network, the accumulation of large numbers of sensor nodes becomes easy to sense and communicate with in the shortest range.(Terence, 2017). Security is also a major concern in the wireless sensor network, due to its communication capabilities, among other major problems. There are different attacks that affect the activity of sensor nodes. In WSN, Sinkhole is an attack in which the shortest path between the sink or destination node is shown by the sinkhole node.Many researchers have so far proposed various methodologies for the detection of sinkhole attacks. In this article, the author examined and researched the sinkhole attack and its classification and methods of using different parameters to detect sinkhole attacks.

According to Data consistency and network flow information approach, the approach presented in(Edith C. H. Ngai, 2006)involves the base station in the detection process, resulting in a high communication cost for the protocol. The base station floods the network with a request message containing the IDs of the affected nodes. The affected nodes reply to the base station with a message containing their IDs, ID of the next hop and the associated cost. From the base station, the obtained data is then used to create a network flow graph to define the sinkhole. The algorithm is also robust in dealing with malicious cooperative nodes that attempt to conceal the actual intruder.Through both numerical analysis and simulations, the efficiency of the proposed algorithm was examined. The findings have shown the algorithm's efficacy and accuracy. They also say that for wireless sensor networks, their overheads for communication and computation are relatively low.

According to the device that detects the presence of a sinkhole attack is proposed in conjunction with novel intrusion detection.(Daniel Dallas, 2016). The scheme is focused on control of the hop count. The ADS is easy to implement with a small footprint, since the hop-count function is easily obtained from routing tables.In addition, the proposed ADS is applicable to any routing protocol which, as a measure of distance between source and destination nodes, dynamically maintains a hop-count parameter. In a simulated network, the scheme can detect attacks with 96 percent accuracy and no false alarms using a single detection system.

According to Su, et al. (C.-C. Su, 2010), two methods have been suggested to enhance cluster protection for sensor networks using IDS. The first technique uses an authentication-based model, which can withstand external attacks. Adding a message authentication code (MAC) for each message is the basic technique.Whenever a node wishes to send a message, a timestamp is applied to it and a MAC is created by a key pair or independently based on the sender's key position. The authentication mechanism is used by LEAP so that the recipient can verify the sender. Energy saving is called the second scheme.The emphasis of this method is the identification of wrongdoing in both Member Nodes (MN) and cluster head nodes (CH). The CH broadcasts a warning message encrypted with the cluster key to restrain this particular node when wrongdoing is detected.

According to Kavita Tandon (Tandon, August 2016), several routing and security issues in WSNs based primarily on Sinkhole attacks were introduced in their paper. It also provides different methods for detecting and preventing sinkhole attacks.It finally ends with the countermeasures used against this attack. Anomaly detection can be a better solution if applied with the algorithm that can minimize false alarms, according to most of the research paper.

## III. PROPOSED ALGORITHM

The purpose of the study is to limit the effects of sinkhole attacks on network efficiency. The most vulnerable attack in WSN is the Sinkhole attack on wireless sensor networks, which prevents the base station from collecting full and unmodified data from its roots. Instead of the base station, cluster heads relay the data to the malicious node.The sinkhole attack is the denial of attack type of operation, which decreases the efficiency of the network in terms of different parameters. The two-way authentication mechanism is based on a novel algorithm. There is a unique identifier at the base station, which is the complex Armstrong number.The base station localizes the location of the node and assigns each node in the network a unique number. The cluster head will request their identification

before transmitting the data to the base station.A malicious node would not be able to present the base station's identification number to the head of the cluster. To isolate malicious nodes in the network, the cluster head will implement multi-path routing.

Proposed Algorithm
Input: Use finite node numbers to deploy WSN
Output: Malicious Node Detection

- Deploy WSN with the finite number of sensor nodes
- Divide the network into clusters of fixed size and pick the cluster head in each cluster by applying the LEACH protocol based on distance, energy
- Apply node localization ()
  - Base station send ICMP message to each node in the network
  - The nodes will reply back the hello message on the basis of received message, base station judge location of the sensor node
- Assign unique number ()
  - The base station generate unique number for each node in the network
  - The generate number is the unique Armstrong number which is complex in nature and difficult to break
  - The base station will also send its unique number of each node in the network
- Two-way Authentication ()
  - The cluster head ask unique identification number of base station
  - If (Base station fails to present unique number)
  - Destination node detected as malicious node
  - Else
  - Authentication complete
  - Data transmission starts in the network

## IV. RESULTS AND DISCUSSION

We implemented the proposed work in NS2 and analyzed the findings in relation to certain output parameters by contrasting the proposed work with existing techniques.

| Parameter | Values |
|---|---|
| Type of antenna | Omi-directional |
| Area | 800X800meters |
| No. of nodes | 38 |
| Routing Protocol | LEACH |
| Channel type | Wireless channel |
| Packet size | 512byte |
| Mobility model | Two ray ground propagation model |
| Simulation Time | 50s |
| Traffic Type | CBR(UDP) |

Table 1:- Simulation Parameters

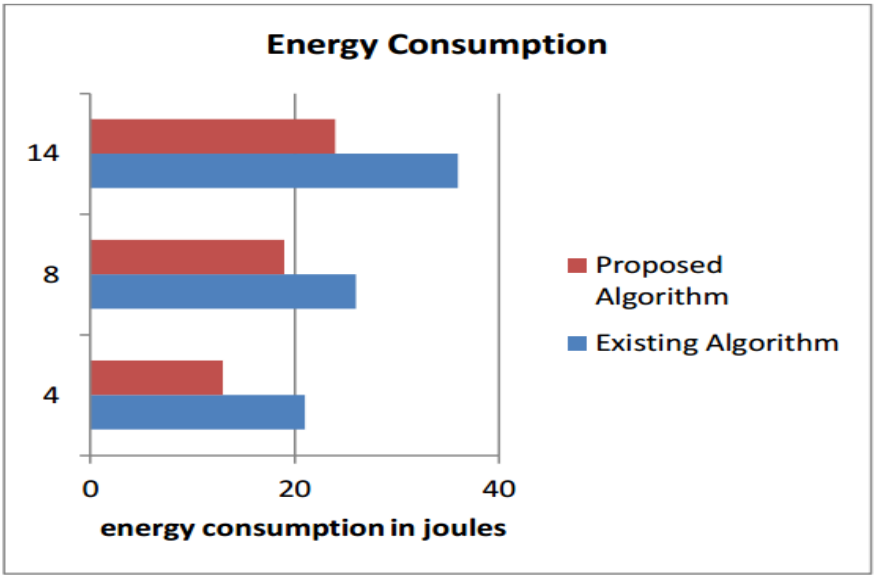


Fig 1:- Comparison of energy consumption

ISSN No:-2456-2165

The energy consumption of the proposed algorithm has been compared to the current algorithm, as shown in figure 1. It has been studied that the proposed algorithm's energy consumption is lower because of sink hole attack isolation in the network.

| Time | Existing Algorithm | Proposed Algorithm |
|---|---|---|
| 4 second | 21 joules | 16 joules |
| 8 second | 26 joules | 19 joules |
| 14 second | 38 joules | 24 joules |

Table 2:- Energy consumption comparison

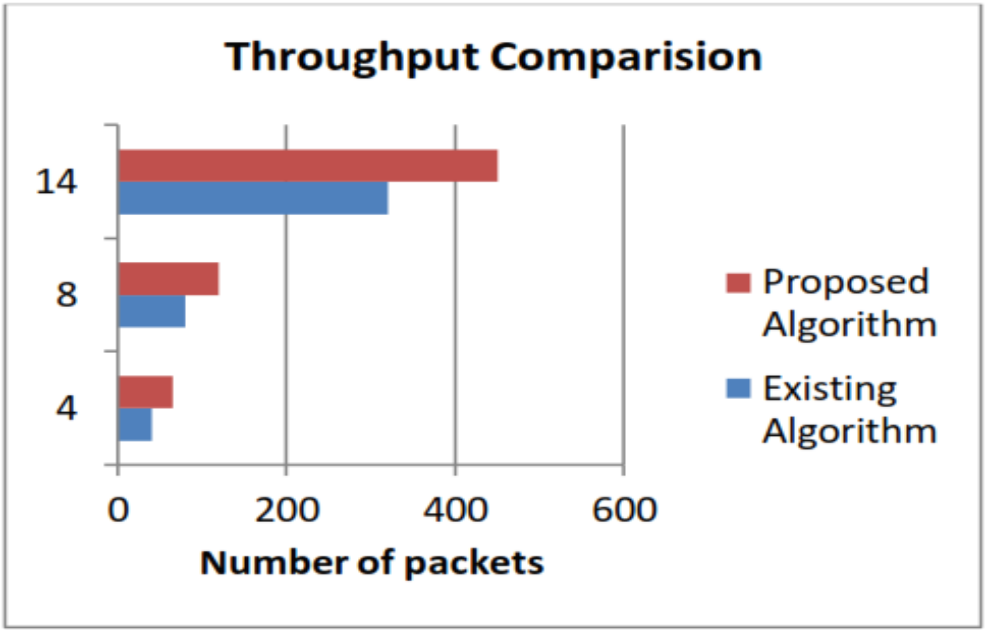


Fig 2:- Throughput Comparisons

The performance of the proposed and current algorithm is compared, as shown in Figure 2, so that it is analyzed that throughput will be increased at a steady rate due to the isolation of the sink hole attack in the network.

| Time | Existing Algorithm | Proposed Algorithm |
|---|---|---|
| 4 second | 68 packets | 76 packets |
| 8 second | 140 packets | 172 packets |
| 14 second | 260 packets | 420 packets |

Table 3:- Throughput Comparisons

## V. CONCLUSION

WSN is the network in this study in which different sensor nodes are installed so that it is possible to monitor the surrounding environmental conditions. The sinkhole attack decreases the efficiency of the LEACH protocol and the sinkhole attack is detected and isolated by our approach.We get the output analyzed in terms of energy consumption is minimized by 26 percent and throughput is increased by 20 percent by conducting experiments in WSN including sinkholes in the code.The findings show that the proposed malicious node isolation work improves network performance in terms of energy consumption and throughput. The study can be expanded in the future to enhance the detection of sinkhole attacks using the key exchange mechanism.

## REFERENCES

[1]. C.-C. Su, K.-M. C.-H.-F. (2010). The new intrusion prevention and detection approaches for clustering-based sensor networks . *IEEE Wireless Communications and Networking Conference*.

[2]. Daniel Dallas, C. L. (2016). Hop-Count Monitoring: Detecting Sinkhole Attacks in Wireless Sensor Networks. *15th IEEE International Conference on Networks, ICON*, (pp. 176-181).

[3]. Dong D, L. M. (2008). Topological detection on wormholes in wireless ad hoc and sensor networks. *IEEE Transactions on Mobile Computing*, pp. 698–711.

[4]. Dr. G. Padmavathi, Mrs. D. Shanmugapriya. (2009). A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. *International Journal of Computer Science and Information Security, 4*, 1-9.

[5]. Edith C. H. Ngai, J. L. (2006). On the Intruder Detection for Sinkhole Attack in Wireless Sensor Networks. *IEEE International Conference on Communications, 8*, p. 33833389.

[6]. G.H. Raghunandan, B. L. (IEEE 2011). A Comparative Analysis of Routing Techniques for Wireless Sensor Networks. *Proceedings of the National Conference on Innovations in Emerging Technology*.
[7]. J.-C. Wang, C.-H. Lin, E. Siahaan, B.-W. Chen, and H.-L. Chuang. (2014, Feb). Mixed sound event verification on wireless sensor network for home automation. *IEEE Trans. Industrial Informatics, 10*, pp. 803- 812.
[8]. Tandon, K. (August 2016). Sinkhole Attacks in Wireless Sensor Network Routing: A Survey. *Research Journal of Computer and Information Technology Sciences, IEEE , 4*(8), 4-7.
[9]. Terence, A. M. (2017, April). A Survey on Various Detection Techniques of Sinkhole Attacks in WSN. *International Conference on Communication and Signal Processing*, 6-8.