Sinkhole Attack Detection in A Wireless Sensor Networks using Enhanced Ant Colony Optimization to Improve Detection Rate

Kenneth E. Nwankwo
Department of Cyber Security Science,
Federal University of Technology
Minna, Nigeria
soundnwankwo@gmail.com

Shafi'i Muhammad Abdulhamid
Department of Cyber Security Science,
Federal University of Technology
Minna, Nigeria
shafii.abdulhamid@futminna.edu.ng

***Abstract* - Wireless Sensor Networks (WSN) comprises of tiny sensor nodes that are able sense and process data. Sinkhole attack occurs when an attacker node in a wireless sensor network disguises itself as the legitimate node closest to the base station, in order to have all data pass through hence having the opportunity to modify, drop or delay data going to the base station. In this conceptual framework, we propose a sinkhole detection scheme enhancing ant colony optimization to improve sinkhole detection via packet drop, packet delivery rate, energy exchange and throughput in a wireless sensor network. Initial results and expected outcome are shown and further research will also be discussed.**

***Keywords**: Swarm Intelligence, Ant Colony Optimization, Wireless Sensor Network, Sinkhole Detection,*

I. INTRODUCTION

Wireless Sensor Network (WSN) is an interconnection of sensing nodes that can come in different sizes connecting to a base station that makes meaning out of the data received. Being one of the highly utilized network types and applied in many areas such as health care monitoring, area monitoring, earth and environment sensing including industrial monitoring. These sensors monitor the environment, collecting data and sending to the base station. WSN can be used in an environment that is physically without protection or attended to [1]. The peculiar nature of wireless sensor networks makes the vulnerable to security threats of different types and purposes. With the simplicity of their routing techniques, security is the greatest challenge hence making them more susceptible to many network attacks, some of which are Sinkhole attack, Selective Forwarding attack, Wormhole, Hello Flood, sybil attacks, attack node replication, and Blackhole attack[2]. Sinkhole attack is one of the most formidable as it can lead to everyone of the other attacks mentioned above. Figure 1 depicts a typical WSN networks and all it comprises of.

WSN Uses

Sensor networks are generally sent in an assortment of utilization going from military to natural and medicinal research. In numerous applications, for example, target following, war zone reconnaissance and gatecrasher recognition, WSNs regularly work in hostile and unattended situations. In this manner, there is a solid requirement for ensuring the detecting information and detecting readings. In remote situations, an enemy not exclusively can listen in the radio traffic, yet additionally can catch or interrupt the traded messages. In this way, numerous conventions and calculations don't just work in unfriendly conditions without having sufficient safety efforts. Subsequently, security ends up one of the significant concerns while structuring security conventions in asset compelled WSNs. A portion of the uses of WSNs are in war zone surveillance, medicinal services applications, natural observing, shrewd home and vehicular specially appointed systems (VANETs) and some more.

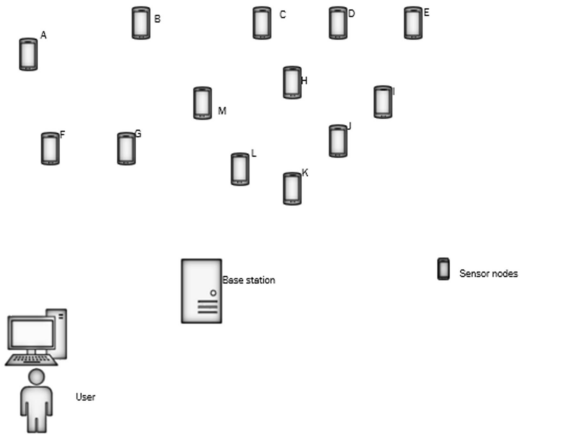

Fig 1. Wireless sensor Network

The major contribution of this conceptual framework paper :

- We describe wireless sensor network and showcase the structure of the WSN architecture

- We analyze and present the sinkhole attack scenario in WSN
- We propose an enhanced ant colony optimization technique (EACO) framework for sinkhole attack detection.

The purpose of our proposed paper is to develop a framework to improve sinkhole attack detection by Enhancing Ant Colony Optimization which a swarm intelligence technique using network simulator NS3 as the simulator. The remaining section of this framework paper is arranged as follows: section 2 shows the over view of sinkhole attack, section 3 gives a summary of recent related works, section 4 describes the problem formulation and the design model, section 5 presents the proposed framework for Enhanced Ant Colony Optimization (EACO) for sinkhole detection, section 6 introduces Ant Colony Optimization and the equations, section 7 shows the initial results describes the expected outcome of our model, while section 8 recommends future research direction and lastly, section 9 concludes the paper.

II. SINKHOLE ATTACK OVERVIEW

In Sinkhole attack a compromised sensor node attempts to get information to it from neighboring node. Thus, the sensor node picks up information, and knows what information is being communicated between neighboring nodes. This attack occurs by disguising the compromised node to be the most attractive to its neighboring node with respect to the algorithm by falsely advertising itself as the node closest to the base station. [3]. The figure below clearly illustrates a sinkhole attack in a wireless sensor network. As shown below, nodes with data seeking to transfer to the base station, first sends a route request (RREQ) to all nearby nodes. Normally the node with the quickest path to the base station will be known from the route reply (RREP) respond coming from all the nearby nodes, this is where the sink node (SN) sends (RREP) reply too nodes no matter how far it is but pretends to have the quickest route to base station hence it attracts all data to itself and carries out any number malicious purposes like altering the information, dropping the information or dallying the information from getting to the base station giving birth to other attacks like blackhole, wormhole and grey hole in the wireless sensor network.

An attacker can compromise the integrity, confidentiality and authenticity of the wireless sensor network through a compromised node that becomes the sink node hence the wealth of research on ways to detect and mitigate such an attack on a wireless sensor network.

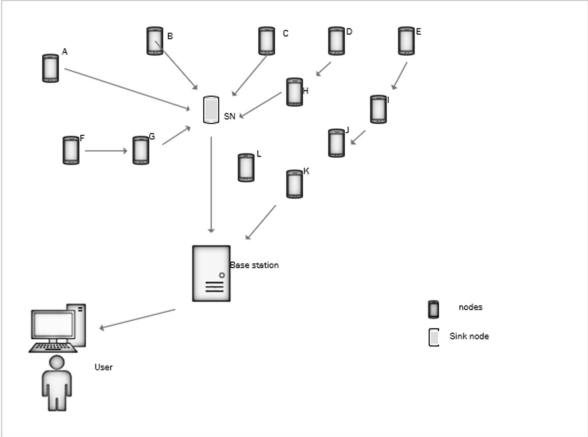

Fig 2. Sinkhole Attack Illustration

III. RELATED WORKS

Sinkhole attack detection and mitigation of in wireless sensor networks have been on for over a decade, the summary of the recent researches include [4] who presented parameter evaluation for ant colony system to obtain the best values for throughput, energy consumption and latency guiding research results to achieve optimal performance for packet routing process. [5] which introduced a detection algorithm using information from data aggregation algorithm to detect a sinkhole attacker in body area network, using omnet++ for simulation achieved a good performance in detection.[6] employed enhanced particle swarm optimization (ESPO) modifying flocking based clustering algorithm that involved separation, alignment and cohesion of clustered nodes in the WSN employed to mitigate and detect sinkhole attack in a larger instance.[7] proposed an algorithm enhancing ant colony system inspired from a variant of ant colony optimization with the global and local pheromone updates to improve path exploitation and exploration with the effect of reduction in packet loss and increase in energy efficiency of sensor nodes.[8] improved the (KMT) technique using ant colony optimization for path panning to deceive intruders, improve and safe guard data collection from node to base station and vice versa, using COOJA to simulate, taking into consideration ACO key protection allocation and ACO-pheromone vanishing mechanism effectively balancing the blending speed and communication of the nodes.[7] proposed an improved ant colony optimization algorithm to solve packet loss problems for nodes carrying more packets than its capacity. Experiment conducted to compare the performance of the proposed Enhanced Ant Colony System (EACS) using Energy Efficient Ant-Based Routing (EEABR) algorithm and Cost-aware Ant-Routing (SC) algorithm and the proposed algorithm is promising for implementation in static WSN systems.[9] proposed a flow based mitigation model with of time variant

snapshot(FBSD) for sinkhole detection and mitigation. Using the geographical and physical features of the nodes, the base station maintains location details of the nodes enabling it to detect the presence of a sink node in the network. NS-2 simulator was employed for implementation, the proposed method highly reduces over-head generated by flood of control messages. [10] proposed a swarm intelligence algorithm, an Enriched Artificial Bee Colony Optimization (EABC) to observe and detect sink nodes in WSN, monitoring the position of estimated malicious nodes continuously. Implementing this algorithm as an evolutionary algorithm Using MATLAB for performance evaluation shows that with the intimation of the base station, the risk factor of the attacker node it known and hence the sinkhole discovered and its purpose.[11] proposed Artificial Bee Colony (ABC) technique for sink hole detection and compared it with an existing Enhanced Particle Swarm Optimization (EPSO) technique and got better detection rate, false alarm rate, packet delivery ratio and average delay. Using NS-2 as simulator. [12] designed a mechanism for sinkhole detection by first considering three types of sinkhole malicious node in WSN, the sinkhole modification node (SMD), sinkhole message dropping node (SDP), and sinkhole message delay node (SDL), then providing a detection scheme able to detect the different types of sinkhole node in a hierarchical wireless sensor network (HWSN). In this approach the network was divided into clusters with high sensing nodes used as the cluster head (CH) responsible for detecting sinkhole node in the cluster. Using NS-2 for simulation gaining better performance in terms of detection rate.[13] this authors proposed Enhanced Particle Swarm Optimization and the technique tested in a simulated environment. This technique proved to have a better performance than the initial techniques Particle Swarm Optimization (PSO) and Ant Colony Optimization in areas of packet delivery ratio, detection rate and average delay.

IV. PROBLEM STATEMENT

The elusive nature of sinkhole attack in a WSN acting as either a cluster head (CH) or the legitimate node closest to the base station, there still lies the problem of false alarm rate in WSN, With the wealth of research on-going on the detection and mitigation of sinkhole attack in WSN because its malignant nature, there is room for improvement on solution of false alarm rate with the techniques.

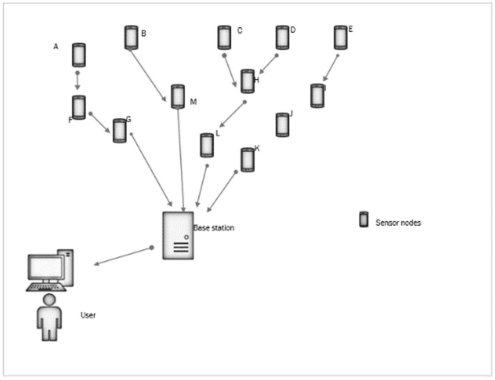

Fig. 3 Scenario I

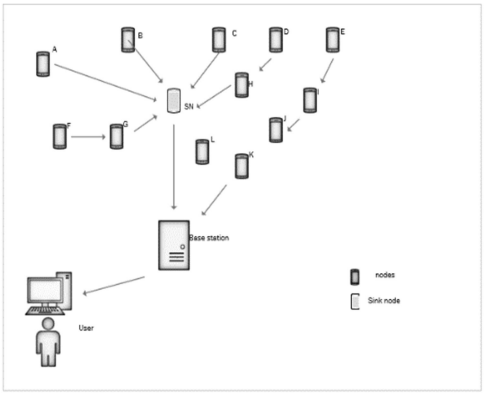

Fig 4. Scenario II

Scenario 1 shows a normal multi-hop many to one WSN node to base station packet delivery nature where the packets are transferred from one node to another based on the node is closest to the base station of the node with stronger link quality. While Scenario 2 shows the presence of an attacker node and it can be seen clearly that it has every packet passing through it giving the attacker the privilege to delay, modify or drop packets. In our proposed enhancement of the Ant Colony Optimization, the sink node is detected and no packet is sent through the compromised node.

V. PROPOSED ENHANCED ANT COLONY OPTIMIZATION FRAMEWORK FOR SINKHOLE DETECTION

This proposed framework comprises of 1st and 2nd stages. The first stage involves problem formulation and planning, dataset description with design and stage two involves implementation which include Enhanced Ant Colony Optimization (EACO) detection on NS-3.29 simulator, flowchart and pseudocode.

VI. ANT COLONY OPTIMIZATION

ACO algorithm is derived from the behavior of ants when they search for food, [14] derived the initial model of the ACO Algorithm. ACO an intelligent

algorithm a type of swarm intelligence technique used to simulate food search process by ants. Ants secrete pheromones as they search for food to help bring them back to their initial location and to help discover the likely fastest distance that will bring success. Since ants have the ability to feel the amount of pheromone, as one ant finds food, others will surely follow the path which it paves to find the same food through the secreted pheromone. Ants always follow paths with high pheromone concentration that hence increases the pheromone secreted on the path which signal success. in Theory, the more the amount of pheromone there are on the path, the more ant connect and follow. The path having the highest amount of pheromone soon becomes the optimal path for the ant colony to the food location.

Formulated model of ACO according to [15] equation below

$$P_{ij}^{k} = \frac{[\tau_{ij}(t)]^{a}.[\delta_{ij}]^{\beta}}{\sum_{k\in\{N-tabuu_k\}}[\tau_{ij}(t)]^{a}.[\delta_{ij}]^{\beta}} \quad [1]$$

$$\tau_{ij}(t+1) = P * \tau_{ij}(t) + \sum_{k=1}^{N} \Delta\tau_{ij}(t)^{k} \quad [2]$$

$$\Delta\tau_{ij} = \frac{Q}{L_k(t)} \quad [3]$$

$$\delta_{ij} = \frac{1}{d_{ij}} \quad [4]$$

$$(X_{lt} - X_{li+1})^2 + (Y_{lt} - Y_{lt+1})^2 = d_{li+1,lt^2} \quad [5]$$

Q being constant, P_{ij}^{k} is probability of following node $d_{l_{i+1}}$ is distance between node l_{i+1} while the end node l_t , the $\tau_{ij}(t)$ is amount of pheromone in the curve (i,j). (x_{l_t}, y_{l_t}) and $(x_{l_{t+1}}, y_{l_{t+1}})$ are respectively coordinates l_t and l_{i+1} . δ_{ij} is the heuristic data in curve. α and β are weight factors of $\tau_{ij}(t)$ and δ_{ij}. where N is number of ants, $L_k(t)$ shows the object function.
Hence the model updating and coverage of pheromone.

Once an ant selects the next node location, the roulette wheel technique is used, which continues till the next node destination is obtained by the ants. At once, pheromones of all the nodes are restructured equation according to [15]

$$\tau_{li,li+1}(k, \aleph+1) = \rho\tau_{li,li+1}(k, \aleph) + \Delta\tau_{li,li+1}(k, \aleph) \quad [6]$$

ρ represents the rate evaporation of pheromones

```
Procedure ACO ( )
{
Input n, α , β , ρ
set the ant colony configuration
set the initial pheromone and heuristic value
get ant colony optimization system based on the
calculated cost matrix
i = 1
while (I <= n)
{               r = 1
While ( r <= i)
{
Reset the ants
Build ant s' solution
initiate local search
Update path best for i
Update pheromones
r = r + 1
}
Choose path best for i
i = i + 1
}
}
```

Pseudo code for ACO

VII. INITIAL RESULTS AND EXPECTED OUTCOME

To show the workability of our framework, a WSN simulation is set up in NS-3.29 using 22 nodes. It supports simulations of TCP and UDP, MAC layer protocols, multicast and routing protocols in Wireless Sensor Networks. Simulation parameter. In this simulated network, standard routing protocol AODV is used. Number of nodes in the network are 22. The Number of sinkhole attacks varies of the total number of s observing there energy levels as they communicate until a sinkhole attack is involved.

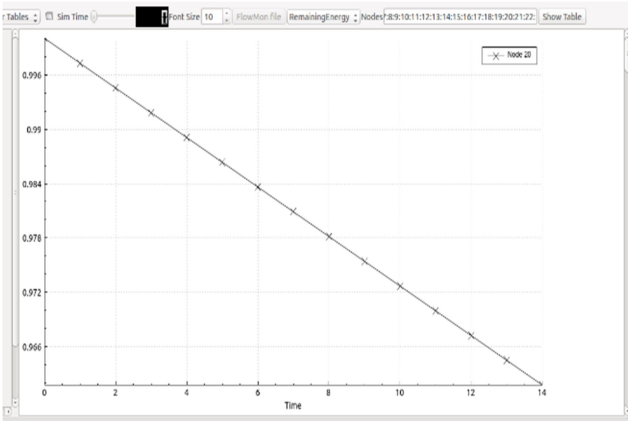

Fig 5. Energy change rate

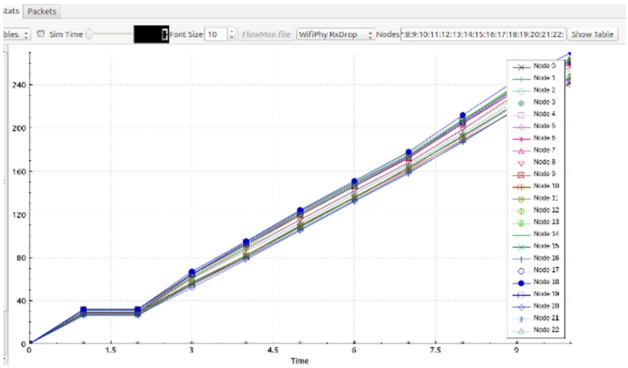

Fig 6. Packet drop ratio

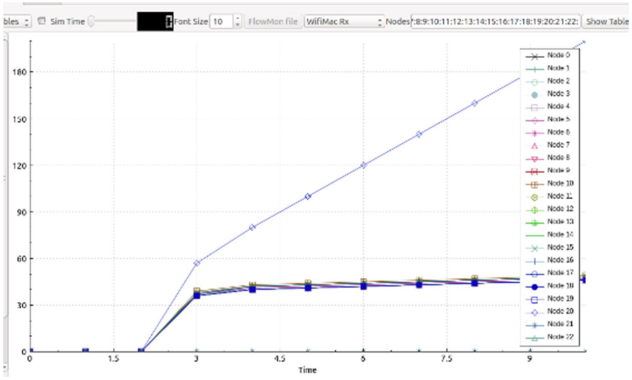

Fig 7. Throughput rate

From the simulation, introduction of the sink node changed throughput, energy level, packet delivery ratio of the nodes.

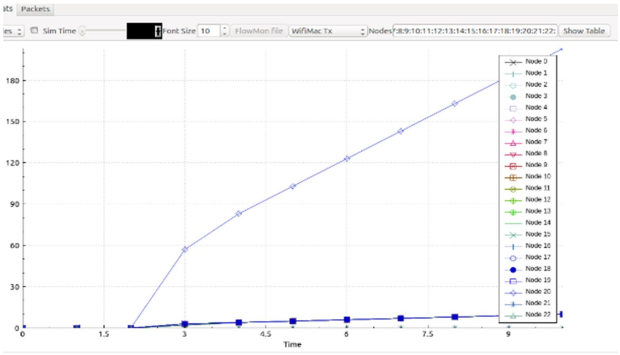

Fig 8. Packet delivery rate

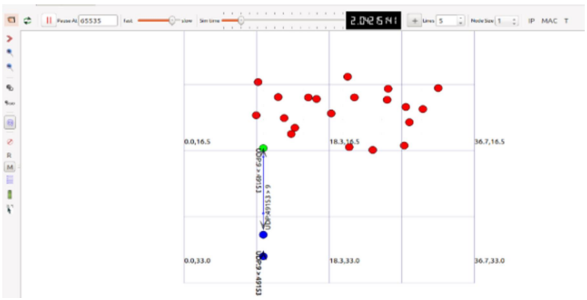

Fig 9. WSN simulation

VIII. FURTHER RESEARCH

With the framework on ground, the future direction is to proceed to apply the EACO algorithm in the wireless sensor network simulation in the NS-3.29, taking note on the effect of the detection rate and false alarm reduction rate and then compare with other known algorithm.

IX. CONCLUSION

We discussed wireless sensor network, highlighting its uses in the world around us and focused on one of the most malignant security challenges sinkhole attack. Presented a framework of our proposed enhancement of the Ant Colony Optimization algorithm to improve sinkhole detection rate and reduce false alarm in wireless sensor network. Presented initial results and future research direction.

X. ACKNOWLEDGEMENT

Our acknowledgement and appreciation are to every staff in the department of computer science and cyber security department, Federal University of Technology Minna.

REFERENCE

[1] G. Sanjeev Kumar and S. Poonam, “Overview of Survey on Security of Wireless Sensor Network,” vol. 3, no. 1, pp. 5201–5207, 2013.

[2] S. Mohammadi and H. Jadidoleslamy, “A Comparison of Link Layer Attacks on Wireless Sensor Networks,” *Int. J. Appl. Graph Theory Wirel. Ad Hoc Networks Sens. Networks*, vol. 3, no. 1, pp. 35–56, 2011.

[3] C. Karlof, N. Sastry, and D. Wagner, “TinySec: A link layer security architecture for wireless sensor networks,” in *Proceedings of the 2nd international conference on Embedded networked sensor systems - SenSys ’04*, 2004.

[4] H. Jamal, A. Nasir, and K. R. Ku-mahamud, “How to cite this article: Nasir, H. J. A., Ku-Mahamud, K. R., & Kamioka, E. (2019). Parameter adaptation for ant colony system in wireless sensor network.,” vol. 2, no. 2, pp. 167–182, 2019.

[5] A. Nadeem and T. Alghamdi, “Detection Algorithm for Sinkhole Attack in Body Area Sensor Networks using local information,” no. September 2018, 2019.

[6] N. Nithiyanandam, P. L. Parthiban, B. Rajalingam, and R. Scholar, “Effectively Suppress the Attack of Sinkhole in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique,” vol. 118, no. 9, pp. 313–329, 2018.

[7] H. J. A. Nasir, K. R. Ku-Mahamud, and E. Kamioka, “Enhanced Ant Colony System for Reducing Packet Loss in Wireless Sensor Network,” *Int. J. Grid*

Distrib. Comput., 2018.

[8] C. Iwendi, Z. Zhang, and X. Du, "ACO based key management routing mechanism for WSN security and data collection," *Proc. IEEE Int. Conf. Ind. Technol.*, vol. 2018-Febru, pp. 1935–1939, 2018.

[9] K. Devibala, S. Balamurali, A. Ayyasamy, and M. Archana, "Flow Based Mitigation Model for Sinkhole Attack in Wireless Sensor Networks using Time-Variant Snapshot," *Int. J. Adv. Comput. Electron. Eng.*, vol. 2, no. 5, pp. 14–21, 2017.

[10] R. S. Raghav, S. Pothula, and D. Ponnurangam, "An enriched artificial bee colony (EABC) algorithm for detection of sinkhole attacks in Wireless Sensor Network," *Int. J. Mech. Eng. Technol.*, vol. 8, no. 8, pp. 193–202, 2017.

[11] Y. N. Dharshini and c N. Chinnaswamy, "SWARM INTELLIGENCE TECHNIQUE FOR SINKHOLE ATTACK DETECTION IN WIRELESS SENSOR NETWORK Performance Comparison of the Algorithms," no. 4, pp. 647–656, 2017.

[12] S. K. and M. K. K. Mohammad Wazid, Ashok Kumar Das, "Design of sinkhole node detection mechanism for hierarchical wireless sensor networks," *Wiley Online Libr.*, vol. 9, no. 19, pp. 4596–4614, 2016.

[13] G. Keerthana, "Detecting Sinkhole Attack in Wireless Sensor Network using Enhanced Particle Swarm Optimization Technique ," *Int. J. Secur. Its Appl.* , 2016.

[14] M. Dorigo and D. C. Gianni, "Ant Colony Optimization: A New Meta-Heuristic." 1992.

[15] J. Zhao, D. Cheng, and C. Hao, "An Improved Ant Colony Algorithm for Solving the Path Planning Problem of the Omnidirectional Mobile Vehicle," *Math. Probl. Eng.*, vol. 2016, pp. 1–10, 2016.