Anomaly-based Detection of Black Hole Attacks in WSN and MANET Utilizing Quantum-metaheuristic Algorithms

Mirsaeid Hosseini Shirvani, Amir Akbarifar
Department of Computer Engineering, Sari Branch, Islamic Azad University, Sari, IRAN
mirsaeid_hosseini@iausari.ac.ir, msc.akbarifar@gmail.com
Corresponding author: *mirsaeid_hosseini@iausari.ac.ir*

***Abstract*- Wireless sensor network (WSN) comprises various distributed nodes that are physically separated. Nodes are constantly applying for sensing their environment. If the information sensitivity coefficient is very high, data should be conveyed continually and also with confidentially. WSNs have many vulnerability features because of data transferring on the open air, self-organization without reformed structure, bounded range of sources and memory, and limited computing capabilities. Therefore, the implementation of security protocols in WSN is inescapable. According to the resemblance between WSN and biotic reaction to the real menace in nature, bio-inspired approaches have variant rules in computer network investigations. In this paper, we exploited an ant colony optimization (ACO) algorithm based on Ad-hoc On-Demand Distance Vector (AODV) protocol for detection of Black hole attacks. Finally, the Grover quantum metaheuristic algorithm is applied to optimize attack paths' detection. The results gained from extensive simulations in WSN proved that the proposed approach is capable of improving some fundamental network parameters such as throughput, end-to-end delay, and packet delivery ratio in comparison with other approaches.**

***Index Terms*-** Security, Meta-heuristic Algorithm, Black hole Attack, Ant Colony Optimization (ACO), Quantum Algorithm.

I. INTRODUCTION

Evolution and proliferation in distributed pervasive systems have emerged novel Tech such as Internet of Things (IoT), smart home system, body area network (BAN), and WSN [1]-[5]. Distributed systems include different heterogeneous fixed and mobile computing nodes [6]. For instance, distributed sensor networks are ambulant and use limited battery sources. A significant feature in pervasive systems is that they are autonomous and independent by the human. This propellant leads wireless sensor utilization to be a great alternative in an expensive, aggressive, and

Manuscript received 4-Feb.-2020 and revised 16-May-2020,
Accepted on 29-June-2020
P- ISSN: 2322-4088
E- ISSN: 2322-3936

harsh environment for human presence such as military and battlefield surveillance, flood detection, habitat monitoring, acoustic and fluctuation detection, identification and detection of biologic, nuclear attacks and etc. [2]. Albeit, WSN has charming abilities such as low configuration expense and uncontrolled network operations, but it has physical lack space in defensive line. It also suffers from vulnerabilities substances based on the limited sources, compromised the security in this network which encounters it with the threats, danger attacks particularly for networks with high information sensitivity coefficient [7]-[9]. For running the WSN in the protected situation, each illegal nodes and traffic alteration should be distinguished efficiently by high true positive rate. To preserve vigilance of WSN with the focus on nature of proposed network and energy consumption challenges, defensive lines including cryptography and intrusion detection system (IDS) should be used. Obviously, other defensive formations such as intrusion prevention system (IPS) , honeypot and other traditional techniques need efficient algorithms to minimize the energy consumption in the networks with high information sensitivity coefficient. WSNs do not use IP address in their network structure. In this regards, traditional network defensive approaches are not compatible with WSNs. In addition to, there are myriad trajectoty paths between each pair of nodes in large sclae WSN. So, tracking all paths for detection of anomally behaviors in this large search space by IDS methods are NP-Hard problem. To solve this combinatorial problem, meta-heuristic algorithms are able to improve the detection rate and Grover quantum's algorithm can be used for search and classification on unsorted list in this ambit [9]-[21]. Therefore, this paper's contribution is to present a hybrid algorithm based on ACO and quantum metaheuritic algorithm for anomaly detection in WAN networks.

This paper is organized as follows. Section II is dedicated to related work. Section III presents problem background. The proposed Algorithm is placed in section IV. Simulation and evaluation are brought in section V. Section VI conclueds the present paper along with future direction.

II. RELATED WORK

In this section, some quantum and bio-inspired algorithms (BIAs) in literature which have been used for IDS are reviewed. BIAs have had successful applications in miscellaneous domains to solve single objective optimization [1], [22]-[26] and multi-objective optimization problems [27]-[30].

In this line, Binitha et al. proposed a broad overview in BIAs domain. They reexamined a range of BIAs drawn from an evolutionary metaphor or natural phenomena including evolutionary algorithms (EAs) such as GA, GP, DE, and FPA, and swarm intelligence (SI) algorithms such as PSO, ACO, ABC, BFA, FFA, AIS, FSA, IWD, SFLA, DEA, and GSO [31] , [46]-[49].

Fu et al. described a biologically inspired anomaly-based detection framework for hierarchical WSNs [32]. Their proposed framework adopts both danger theory and negative selection algorithm. Danger theory corresponds to local danger sensing process. Due to the hierarchical structure and

collaborative mechanism, the proposed model shows more advantages in detection performance than other traditional methods in terms of higher detection rate and lower false detection rate.

Kolias et al. explored the reasons that led to the application of artificial intelligence in IDS; they presented a SI method that have been used for constructing IDS. A major contribution of this work was comperative solutions among several SI-based IDSs in term of efficiency. According to their study, ACO has a low complexity and this ability makes it a compatible candidate for using in IDS area [33].

Meisel et al. presented a broad overview of biologically inspired research, grouped by topic and classified in two ways: by the biological field that inspired each topic, and by the area of networking in which the topic lies. In each case, they concluded that research efforts are most successful when they separate biological design from biological implementation [34]. In the other words, when they extract the pertinent principle from the former without imposing the limitations of the latter.

Sekhar et al. introduced the various security attacks and proposed the defensive approach in WSN; they compared thier work with an alternative novel approach, i.e., bio-inspired approach. Finally, they discussed about the importance of providing security to WSN [35].

A quantum vaccine immune clonal algorithm with the estimation of distribution algorithm (QVICA-with EDA) has been proposed by Omar et al. [36]. Their approach used as classification algorithm of the new IDS (NIDS) where it was trained and tested using the KDD data set [37]. Their new NIDS was compared with another detection system based on PSO. Their results showed the ability of the proposed algorithm in achieving high intrusions classification accuracy where the highest obtained accuracy was 94.8%.

Butun et al. introduced IDS along their classification, design specification, and its requirements. On the other hand, they presented and discussed the IDS that are proposed for MANETs and their applicability to WSN [43].

Literture review reveals that there is a clear gap for optimzation of black hole detection in WSN and MANET networks in terms of prominent network evalution metrics.

III. PROBLEM BACKGROUND

This section is dedicated to literuatre background to better understanding the proposed paper.

A. Ant Colony Optimization (ACO)

Nature is a great and immense source of inspiration for solving hard and complex problems in computer science since it exhibits extremely diverse, dynamic, robust, complex, and fascinating phenomena. Meta-heuristic algorithms have a broad application range in solving optimization problems. These approaches always find the optimal solution to solve its problem maintaining perfect

balance among its component. Nature inspired algorithms are meta-heuristics that mimic the nature for solving optimization problem opening a new era in computation.

ACO is one of the most wonderful algorithms to find the shortest route which has been firstly devised by Dorigo [38]. ACO gets its inspiration from the real-world action of ants and the scheme they do for obtaining food. ACO is based on the indirect communication of a colony of simple agents, called artificial ants. When an ant moves along a route, it lais a chemical substance called pheromone on it. As more and more ants travel along the same route, the pheromone density of the route increases. The route with the maximum pheromone density is then determined to be the optimal route. To avoid early saturation, the evaporation operation is done to reduce the phoromone level; in this way, the unexplored search space which my have potential solutions will be traversed. One of the abundant applications of ACO is to apply for solving combinatorial optimization problems. The optimization problem is to find specific input candicate which can minimize or maximize objective function.

ACO features a multi-agent organization, stigmergic communication among the agents, distributed operations, use of stochastic decision policy to construct solutions, and stigmergic learning of the parameters of the decision policy. The ACO algorithm is basically interplay of three procedures; namely, 1: *AntBasedSolutionConstruction(.)*, 2: *PheromoneUpdate(.)*, and 3: *DaemonActions(.)*, as represented by algorithm shown in Fig. 1. The schedule activities construct does not specify how these three activities are scheduled and synchronized. The designer is therefore free to specify the way these three procedures should interact.

The *AntBasedSolutionConstruction(.)* procedure performs probability P_{ij}^{k} of choosing the next sub solution of *j* with transition from solution state *i* by *k*-th ant, which is defined by Eq.(1).

$$P_{ij}^{k} = \begin{cases} \dfrac{[\Gamma_{ij}(t)]^{\alpha} \times [\eta_{ij}(t)]^{\beta}}{\sum_{j \in N_i^k} [\Gamma_{ij}(t)]^{\alpha} \times [\eta_{ij}]^{\beta}} & if\ j \in N_i^k;\ P_{ij}^{k} = 0, otherwise \\ 0 & otherwise \end{cases} \quad (1)$$

Where N_i^k is the set of feasible sub solutions that can be selected by *k*-th ant as the next sub-solution of state *i*; Γ_{ij} the pheromone value between the sub-solution of *i* and *j*; and η_{ij} is the heuristic indicationg the quality of the sub-solution *j* that will affect each ant's determination for moving to state *j* when it is at state *i*. The parameter α and β are used to adjust the weight of exploration and exploitation respectively.

The *PheromoneUpdation(.)* procedure is employed for updating the pheromone value Γ_{ij} on each edge, which is defined by Eqs. (2) and (3).

1. Input: An instance *I* of a combinatorial problem *P*
2. Initialize pheromone value (Γ)
3. While termination condition not met Do
   Begin Schedule activities
   $S_{iter} \leftarrow \varphi$
   $for\ j = 1, \ldots\ldots, n_a\ do$
   $S \leftarrow AntBasedSolutionConstruction\ (\Gamma)$
   $S \leftarrow Localserach\ (S)$
   $S_{iter} \leftarrow S_{iter} \cup \{S\}$
   End for
   $PhermoneUpdate\ (\Gamma)$
   $DaemonActions\ (\ )\ \ /*\ Optional\ */$
   End of Schedule activities
   END while
4. Output: Best solution found

Fig. 1. Ant colony optimization algorithm

$$\Gamma_{ij} = (1 - P)\Gamma_{ij} + P \sum_{k=1}^{m} \Delta\Gamma_{ij}^{k} \quad (2)$$

$$\Delta_{ij}^{k} = {}^{1}/_{L^k}\ \rho \epsilon (0,1) \quad (3)$$

Where *m* denotes the number of ants, L^k the quality of solution created by ant k, and parameter ρ denotes the evaporation rate of pheromone value on the pheromone table. The *LocalSearch(.)* procedure improves the quality of the solution gained in previous process. Finally, the optional *DaemonActions*(.) procedure, which is completely problem specific, is called once a route has been constructed before pheromone update process is done. It is called because the single ant in colony cannot encompass the whole optimization problem.

B. Ant Colony based Routing Algorithm (ARA)

Ant Colony Based Routing Algorithm (ARA) works on the principle of reactive technique in an on-demand way in MANET networks. The main goal of ARA is to reduce the overhead for routing. It is highly adaptive, efficient, and scalable. It does not use any HELLO message to explicitly find its neighbors. When a packet arrives at a node, the node checks it to see if routing information is available for destination on its routing table or not. Route discovery and route maintenance are the phases of ARA. The sender broadcasts a forward ant in the route discovery phase and the ant is relayed by each intermediate node until it reaches the destination.

Ant agents can be divided into two sections: Forward Ant (FANT) and Backward Ant (BANT). It is used to create a new routing path. FANT agent is responsible for establishing the pheromone path to the destination node and BANT agent is responsible for establishing the pheromone path to the source node. During the journey of FANT from source to destination, when the FANT is received at the intermediate nodes for the earlier time, the recipient node getting a FANT for the very first time which builds a record of three parameters, i.e., destination address, next hop, and pheromone value on its routing table.

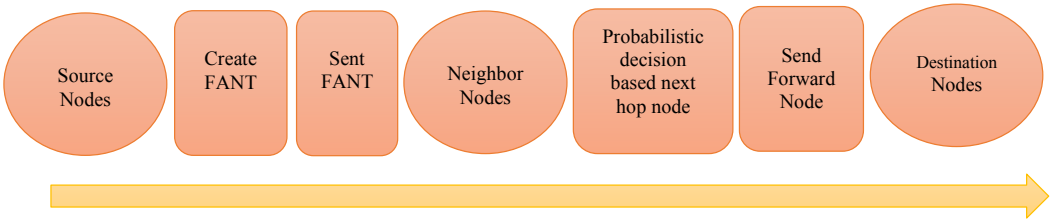

Fig. 2. Transmission of FANT in Ant routing algorithm

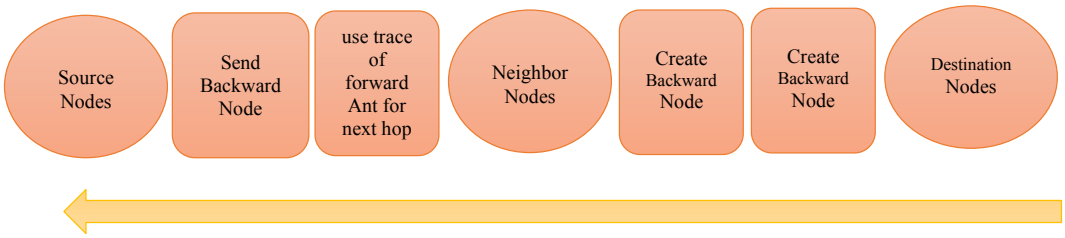

Fig. 3. Transmission of BANT in Ant routing algorithm

At this time, when the FANT reaches at the destination node, it is processed in a special manner. The destination node extracts the information from the FANT and then destroys the FANT. After that a BANT is created at the destination node and sent towards the source node on the reverse path that was followed the FANT. In this manner, the route is established between source and destination; then, data packets can be sent. Fig. 2 shows that the source node creates a FANT and it sends the forward ant intended to route discovery to its neighbor nodes. Using probabilistic decision, it decides the next hop node and forwards the FANT through all the next hop nodes until it reaches the destination. In this regards, Fig. 3 indicates that the destination node creates a BANT and sends the backward ant in the same route traces made by the FANT through the intermediate nodes until it reaches the source node.

ARA fulfills the requirements of distributed operation, loop-freeness, on-demand operation, and sleep period operation. Note that, the nodes are able to sleep when their amount of pheromone reaches to a predetermined threshold. The expected overhead of ARA is very small because there is no routing table information between two nodes. Unlike other routing algorithms, the forward and backward ants do not transmit much routing information. Only a unique sequence number is transmitted in the routing packets. Most route maintenance is performed through data packets, thus they do not have to transmit additional routing information.

C. Attach Scenario

Attack can occur when the malicious node existed in the network intends to materilaize the threats directly on data traffic and intentionally drops, delay or alter the data traffic passing through it. Black

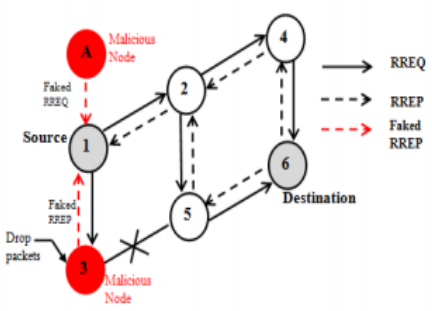

Fig. 4. Black hole attack problem [41]

hole attack is very dangerous active attacks in WSNs and MANETs [39]. In such ad-hoc networks, malicious detection is very hard to recoginize because they lack of central controller, bandwidth limitations, and dynamic topology especially in mobile ad hoc networks [39]. A Black hole attack can intrude the network individually or by group of malice which called selfish nodes [40]. Fig. 4 demostrates how a malicious node acts.

In Fig. 4, legal node labeled "1" intends to send a message to a destination node labeled "6"; then, it starts to make route discovery process. Take a malicious node "3" which claimes it has the information of requested route for determined target right after it receives broadcasted PREQ message from node "1". Then, it replies to the source node "1" very sooner than other nodes. In this time, the source node is decieved and deems that the sender node is an active node on an active route directory which is completed. Hereafter, the source node ignores all other reply feedback packets associated to its route request, but it commences to forward data packets to dummy destination via intermediating of this malicious node. Therefore, the sent packets would be lost in this process. In the other words, the source and destination nodes never communicate. Since AODV treats RREP messages having higher sequence number to be fresher, the malicious node all the time sends the RREP having higher sequence number. So, once the RREP message has been received by source node it is treated as a new packet. The outcome is that there is a high probability of a malicious node effort to organize the Black hole attack in AODV. Black hole attack problem in WSNs could be very serious security problem to be resolved [38].

IV. PROPOSED ALGORITHM

ARA and AODV are evaluated by so many authors in which it is identified that ARA always performs better than AODV. In this section, we have proposed modified AODV to detect and prevent the Black hole attack by using ant colony algorithm such as ARA. Pheromone updates play a significant role in the performance of the ant algorithm. In ARA algorithm, initial pheromone value is

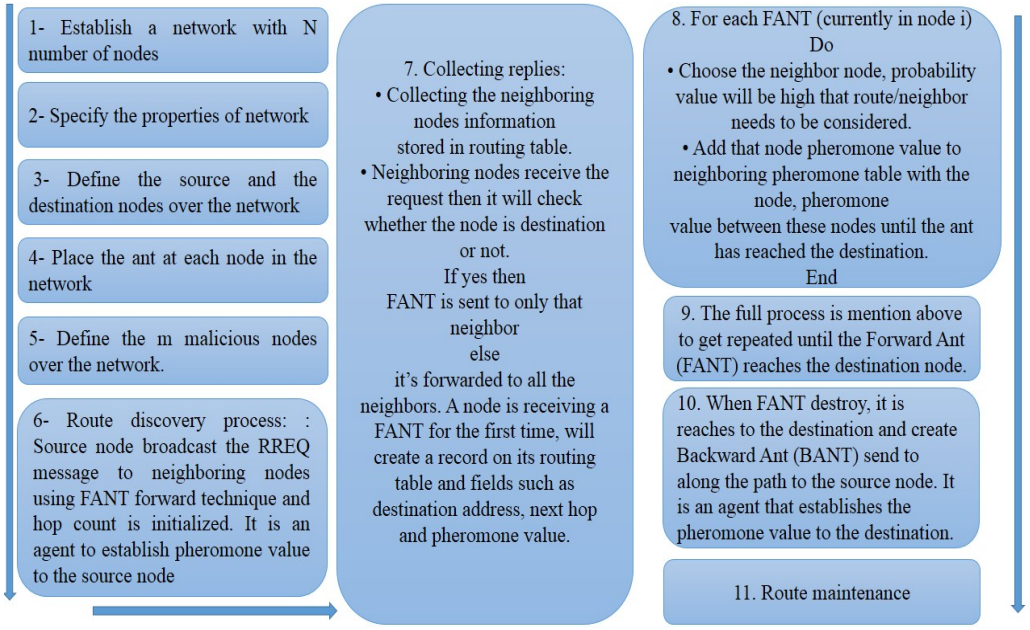

Fig. 5. Proposed algorithm

calculated by number of nodes during the route discovery process. The working principles of the algorithm are depicted in a flowchart of Fig. 5.

To gain better performance, the quamum meta-heuristic algorithm is applied. To use of quantum computing in our bio-inspired approach, we select a Grover algorithm to search on an unsorted list [42]. The Grover algorithm is a quanum meta-heuristic approach which was fistly introduced by Lov Grover in 1996 [42]. It finds a desired input as a blackbox in only $O(\sqrt{N})$ time complexity and produces a particular output where the parameter N is the input size of unsorted list. This achivement is gained on quanutm computers. In contarst with other quantum algorithms, the Grover algorithm performs solely a quadratic speedup which is noticable when the input size N significantly grows because other quantum algorithm incurs exponetially time complexity in large input size. This is because it utilizes 128-bit symmetric cryptographic key in roughly 2^{64} iterations, or a 256-bit key in roughly 2^{128} iterations. In this way, it is resillient against future attacks. This algorithm gives an oppertunity to reach a correct answer with high probabilty near to 1.

On the other side, IBM corporation gives us a valuable repository to simulate quantum gates in a GUI interface with QASM code in a cloud with 5 quantum bit computer [44]. So, for more analysis of our Grover algorithm, we simulate it on IBM quantum cloud and the results are proposed on Fig. 6 and Fig. 7 [44]. The basic scenario of the Grover algorithm is run on card game. We should search in

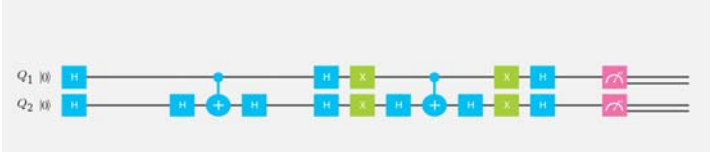

Fig. 6. Grover algorithm with 2 quantum-bit

```
// Name of Experiment: Grover algorithm v1
IBMQASM ; 2.0
include "qelib1.inc;"
h q;[1]
h q;[2]
h q;[2]
cx q[1], q[2]
h q;[2]
h q;[]
h q;[٢]
x q;[١]
x q;[٢]
h q;[٢]
cx q[1], q;[2]
h q;[2]
x q;[1]
x q;[2]
h q;[1]
h q;[2]
measure q;[1]
measure q;[2]
```

Fig. 7. QASM code of Grover algorithm with 2 quantum-bit in IBM 5 qubit Quantum computer [44].

```
quantum_reg
{
  int width;            /* number of qubits in the register */
  int size; /* number of non-zero vectors */
  int hashw;          /* width of the hash array */
  COMPLEX_FLOAT *amplitude;
  MAX_UNSIGNED state;
  int *hash;
};
```

Fig. 8. Quantum register

a space with 4 cards, i.e., ex 2, queen, king, and queen. We need to find the both of queens in 1 search step. Grover algorithm will help us as bellows:

Libquantum is a C library for the simulation of quantum mechanics, especially of quantum computing. It provides a structure for a quantum register (the memory of a quantum computer) and operations for the manipulation of a quantum register [45]. This library has great features for default quantum simulation with high performance and low memory consumption valuable support for quantum process. Libquantum is an open source software with GPL v3 license. Quantum computing will be formed by quantum registers [45]. So, quantum lib has a structure for quantum registers which Fig. 8 depicts.

V. SIMULATION AND EVALUATION

The proposed methodology is compared with the existing algorithms of safe route method upon the ant colony based routing algorithm on the basis of throughput, packet delivery ratio (PDR), and end-to-end delay parameters. The simulation process was run on an area with 500*500 m^2 by NS-2 simulator with 21 node with the AODV presence. The proposed algorithm has been run 20 times; then, the average results are reported. The performance evaluateion metrics and results of the routing algorithm are as below:

- The throughput is the number of bytes transmitted or received per second. This parameter is obtained via Eq. (4). The percent throughput is denoted by *T*, which is gained by Eq. (5).

$$Throughput = \frac{Average\ Recieved\ Node}{Simulation\ Time} \tag{4}$$

$$T = \frac{\sum_{i=1}^{n} N_i^r}{\sum_{i=1}^{n} N_i^r} * 100\% \tag{5}$$

- Packet Delivery Ratio (PDR) can be measured as the ratio of the received packets by the destination nodes to the packets sent by the source node; it can be calculated by Eq. (6).

$$\text{Packet Delivery Ratio} = \frac{Number\ of\ Recieved\ Packet}{Number\ of\ Sent\ Packet} \times 100 \tag{6}$$

- End to end delay represents the time required to move the packet from the source node to the destination node. In E-2-E delay: [packet_ id] = received time [packet_ id] – sent time [packet_ id]; the average end-to-end delay can be calculated by summing the times taken by all received packets divided by its total numbers.
- Dropped packet represents the number of packets that sent by the source node and fail to reach to the destination node. Dropped packets = sent packets– received packets.

For evaluation, Fig. 9 through Fig. 14 illustrates the comparison of proposed algorithm versus other approaches in terms of performance evaluation metrics in this ambit.

Fig. 9 shows that our algorithm on the AODV routing with attack presence has ability to improve the throughput ratio.

Also, Fig. 10 proved that our algorithms packet delivery ratio is more than AODV routing protocol with attack presence.

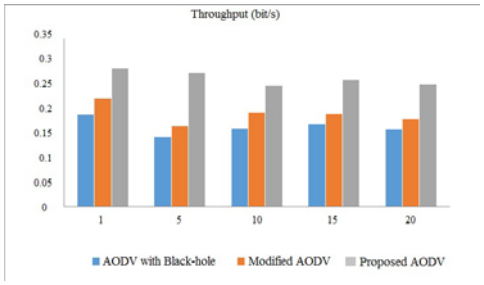

Fig. 9. Algorithms' Comparison in term of throughput

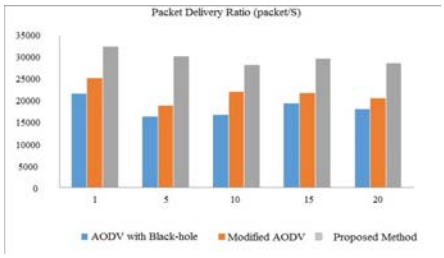

Fig. 10. Algorithms' Comparison in term of Packet Delivery ratio

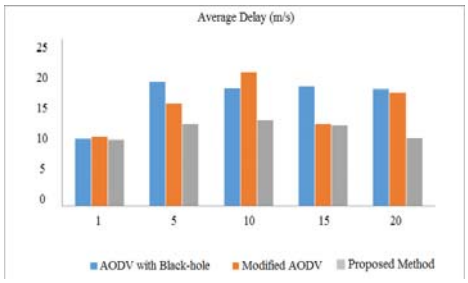

Fig. 11. Algorithms' Comparison in term of end-to-end delay

In this line, Fig. 11 depicts that the proposed approach has a minimum delay against the Black hole attack based on the AODV routing protocol. The comparison is based on time intervals among the packet traffic that is implemented with the NS-2 CMU-GENs directory, located on "~/NS/indep-utils/cmu-scen-gen" in the same periods [50].

Fig. 12 shows that the proposed algorithm can enhance the throughput rate of WSN in comparison with other approaches.

Also, Fig. 13 shows that the proposed algorithm has more received packet ratio on WSN. We should consider that the Black hole attack presence can cause the increase of packet received ratio. The proposed algorithm has a minimum of delay among the higher time intervals which Fig. 14

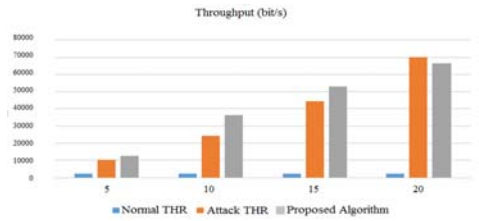

Fig. 12. Throughput in WSN

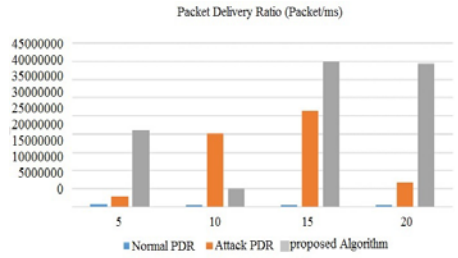

Fig. 13. Packet delivery ratio in WSN

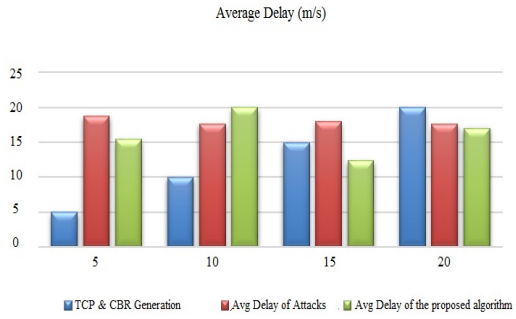

Fig. 14. Received packet in WSN

depicts. It shows that the proposed algorithm is high potentially scalable. Note that, the results of the simulation are taken by AWK in the command line.

Finally, we use of Grover algorithm to speed-up on search operation in a specific rate or event in an unsorted list. According to information of Table I, the delay ratio in clear scenario is equal to 8997 kbps. On the other side, with Black hole attack presence, this rate is about 381315 kbps. So, we assume to search on an event in the 35000 rate. According to Grover results and also optimization in search scenario, this rate can be successfully found with 5 quantum bit in 21 iterations with 0.99 probability.

TABLE I. Results of the proposed approach in wireless sensor network.

Time interval for traffic generating	Normal	Attacks	Modified
Throughput (bit/s)			
5	2221.36	10434.9	12738.2
10	2167.06	24548.4	35975.4
15	2151.76	44356.1	52992.8
20	2182.18	70081.2	66567.2
Packet delivery ratio (Packet/s)			
5	712000	2693360	21181800
10	594500	20029900	4.75E+06
15	562500	26558100	39856300
20	504800	6672780	39406300
End to end delay (m/s)			
5	8997.43	381315	647997
10	8997.49	381318	647983
15	8996.13	381315	589677
20	8997.96	381318	479251
Normalized routing load (packet/ms)			
5	0.862	0.026	0.038
10	0.939	0.013	0.018
15	0.559	0.01	0.029
20	0.602	0.009	0.029

VI. CONCLUSION

WSN is one of the most promising technologies that has applications ranging from health care to tactical military. Although WSNs have appealing features such as low installation cost, unattended network operation due to the lack of a physical line of defense, and no gateways or switches to monitor the information flow, the security of such networks is a major concern especially for the mission critical applications where confidentiality is the first class concern. Therefore, in order to operate WSNs in a secure way, any kind of intrusions should be detected before attackers can harm and disrupt the network. Regarding to WSN natures, their energy consumption challenges, and also the network importance, defensive techniques such as IDS and IPS approaches must be selected. Each attack will increase the network's energy consumption, throughput, packet delivery ratio, and other important parameters. In this article, we applied the ACO algorithm based on AODV protocol for an optimization of Black hole attacks detection. To get better performance, it has been run based on quantum computing which has low time complexity in searching space even in unsorted lists. The results of simulations in WSN proved that the proposed approach is capable of improving some fundamental parameters of networks evaluation such as throughput, end to end delay, and packet delivery ratio in comparison with other approaches. For future work, we envisage to present power model of malicious detector algorithm and formulate it as an optimization problem to be solved.

REFERENCES

[1] Sh. Azimi, C., Pahl, and M. Hosseini Shirvani, "Particle Swarm Optimization for Performance Management in Multi-Cluster IoT Edge Architecture," *10th international Conference on Cloud Computing and Service Sciences (CLOSER)*, pp. 1-10, May 2020.

[2] M. Hosseini Shirvani and S. Ehsani, "A novel sleep/wakeup power management in wireless sensor network: A Fuzzy TOPSIS approach," *Journal of Advances in Computer Research*, vol. 8, no. 4, pp. 95-105, Autumn 2017.

[3] F. Rad, M. Reshadi, and A. Khademzadeh, "Design of a Low-Latency Router Based on Virtual Output Queuing and Bypass Channels for Wireless Network-on-Chip," *Journal of Communication Engineering*, vol. 8, no. 2, pp. 179-196, Summer & Autumn 2019. doi: 10.22070/jce.2019.3882.1117.

[4] R. Yarinezhad and A. Sarabi, "MLCA: A Multi-Level Clustering Algorithm for Routing in Wireless Sensor Networks," *Journal of Communication Engineering*, vol. 8, no. 2, pp. 249-265, Summer & Autumn 2019. doi: 10.22070/jce.2020.4009.1124.

[5] M. Sadeghizadeh, and O. Marouzi, "Securing Cluster-heads in Wireless Sensor Networks by a Hybrid Intrusion Detection System Based on Data Mining," *Journal of Communication Engineering*, vol. 8, no. 1, pp. 1-19, Winter & Autumn 2019. doi: 10.22070/jce.2019.3687.1105.

[6] M. Hosseini Shirvani, N. Amirsoleimani, S. Salimpour and A. Azab, "Multi-criteria task scheduling in distributed systems based on fuzzy TOPSIS," *IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE),* pp. 1-4, April 2017.

[7] A. S. Tanenbaum, *Distributed operating systems*, 3rd Edition, Pearson Education India, 1995

[8] S. S. Iyengar and R. R. Brooks, *Distributed sensor networks: sensor networking and applications*, CRC press, 2016

[9] P. S. Mohanty, S. Panigrahi, N. Sarma and S. S. Satapathy, "Security issues in wireless sensor network data gathering protocols: a survey," *Journal of Theoretical & Applied Information Technology*, vol. 13, no. 1, pp. 14-27, March 2010.

[10] M. Kazemitabar Amirkolaei, *Enhancing Bio-inspired Intrusion Response in Ad-hoc Networks*, Edinburgh Napier University, 2013.

[11] B. Bahrami and M.S. Hosseini Shirvani, "Prediction and Diagnosis of Heart Disease by Datamining Techniques," *Journal of Multidisciplinary Engineering Science and Technology*", vol. 2, no. 2, pp. 164-168, Feb. 2015.

[12] Y. Maleh, and A. Ezzati, "A review of security attacks and Intrusion Detection Schemes in Wireless Sensor Networks," *International Journal of Wireless and Mobile Networks*, vol. 5, no. 6, pp.1-12, Dec. 2013.

[13] P. Mokaripoor, M. Hosseini Shirvani, "A state of the art survey on DVFS techniques in Cloud Computing Environment," *J. Multidiscip. Eng. Sci. Technol*, vol. 3, no. 5, pp. 4740-4743, May 2016.

[14] K. Chaitanya and A. Ghosh, "Analysis of Denial-of-Service attacks on Wireless Sensor networks using simulation," Middlesex University, 1-13, 2010.

[15] L. Kaur and J. Malhotra, "Review on Security Issues and Attacks in Wireless Sensor Networks," *International Journal of Future Generation Communication and Networking*, vol. 8, no. 4, pp. 81-88, Sep. 2015.

[16] A. Akbarifar and H. Abbasi Neyshabouri, "*Analysis of Security in Wireless Sensor Networks," Paper presented at the 11 Symposium on Advances in Science & Technology*, Mashhad, IRAN (in persian), 2017.

[17] A. Akbarifar and H. Abbasi Neyshabouri, "*A survey on Intrusion Detection System in Wireless Sensor Networks," Paper presented at the 11 Symposium on Advances in Science & Technology,* Mashhad, IRAN, 2017.

[18] A. Haghighi, K. Mizanian and G. Mirjalily, " Improved MCBDS for defending against gray hole and black hole attacks in MANETs,, *Advances in Science and Technology Research Journal,* vol. 10, no. 30, June 2016.

[19] K. Somasundaram, "An Effective CBHDAP Protocol for Black Hole Attack Detection in MANET," *Indian Journal of Science and Technology*, vol. 9, no. 36, Sept. 2016.

[20] D. Nitnaware and A. Thakur, "Black hole attack detection and prevention strategy in DYMO for MANET," *Paper presented at the Signal Processing and Integrated Networks (SPIN), 3rd International Conference* on, 2016.

[21] F. A. Khan, M. Imran, H. Abbas, and M.H. Durad, "A detection and prevention system against collaborative attacks in Mobile Ad hoc Networks," Future Generation Computer Systems, vol. 68, pp. 416-427, March 2017.

[22] M. Hosseini Shirvani, "A new Shuffled Genetic-based Task Scheduling Algorithm in Heterogeneous Distributed Systems," *Journal of Advances in Computer Research*, vol. *9, no.* 4, pp. 19-36, 2018. http://jacr.iausari.ac.ir/article_660143.html.

[23] M. Hosseini Shirvani and A. Babazadeh Gorji, "Optimisation of automatic web services composition using genetic algorithm," *Int. J. Cloud Computing*, vol. 9, no. 2, pp. 1-15, 2020.

[24] M. Hosseini Shirvani, "A hybrid meta-heuristic algorithm for scientific workflow scheduling in heterogeneous distributed computing systems," *Engineering Application of Artificial Intelligence,* vol. 90, pp. 1-20, April 2020.

[25] A. Javadian Kootanaee, A. Poor Aghajan and M. Hosseini Shirvani, "A hybrid model based on machine learning and genetic algorithm for detecting fraud in financial statements," *Journal of Optimization in Industrial Engineering*, vol. 14, no. 1, pp:1-10, 2020. doi: 10.22094/joie.2020.1877455.1685.

[26] F. Razavi, F. Zabihi and M. Hosseini Shirvani, "Multi-layer Perceptron Neural Network Training Based on Improved of Stud GA," *Journal of Advances in Computer Research*, vol. 7, no. 3, pp. 1-14, 2016.

[27] M. Hosseini Shirvani, A.M. Rahmani and A. Sahafi, "An iterative mathematical decision model for cloud migration: A cost and security risk approach," *Software: Practice and Experience*, vol. *48, no.* 3, pp. 449-485, 2018. https://doi.org/10.1002/spe.2528.

[28] M. Hosseini Shirvani, "Web Service Composition in multi-cloud environment: A bi-objective genetic optimization algorithm," In *2018 Innovations in Intelligent Systems and Applications (INISTA)*, pp. 1-6, 2018. IEEE. https://doi.org/10.1109/INISTA.2018.8466267.

[29] M. Hosseini Shirvani, "Bi-objective web service composition problem in multi-cloud environment: a bi-objective time-varying particle swarm optimisation algorithm," *Journal of Experimental & Theoretical Artificial Intelligence*, Feb. 2020. DOI:10.1080/0952813X.2020.1725652.

[30] S. Farzai , M. Hosseini Shirvani and M. Rabbani , "Multi-Objective Communication-Aware Optimization for Virtual Machine Placement in Cloud Datacenters," *Sustainable Computing: Informatics and Systems, no. 28, Dec.* 2020, doi: https://doi.org/10.1016/j.suscom.2020.100374.

[31] S. Binitha and S. S. Sathya, "A survey of bio inspired optimization algorithms," I*nternational Journal of Soft Computing and Engineering,* vol. 2, no. 2, pp. 137-151, 2012.

[32] R. Fu, K. Zheng, "Biologically inspired anomaly detection for hierarchical wireless sensor networks," *Journal of Networks,* vol. 7, no. 8, pp. 1214-1219, Aug. 2012.

[33] C. Kolias, G. Kambourakis and K. Maragoudakis, "Swarm intelligence in intrusion detection: A survey," *Computers & Security*, vol. 30, no. 8, pp. 625-642, Nov. 2011.

[34] M. Meisel, V. Pappas and L. Zhang, "A taxonomy of biologically inspired research in computer networking," *Computer Networks,* vol. 54, no.6, pp: 901-916, April 2010.

[35] S.M. Sekhar, S. Abhijth and C. Janiwarad, "A survey on bio-inspired security in wireless sensor networks," *International Journal of Research in Engineering and Technology*, 2015.

[36] O.S. Soliman, R. Bahgat, A. Adly, "Associative classification using a bio-inspired algorithm," *Proceedings of the Tenth Australasian Data Mining Conference-Volume 134, Australian Computer Society, Inc*., December 2012.

[37] https://www.unb.ca/cic/datasets/nsl.html, [Accessed 15 Sep. 2020].

[38] M. Dorigo, "Optimization, Learning and Natural Algorithms,″ PhD dissertation, Dep. of Comp. Politecnico di Milano, Italy, 1992.

[39] S. Bhimla, "Ant Based Black Hole Detection and Protection in MANET," North South University; Mr. Sunil Gupta, North South University.

[40] N. Khemariya, "An Efficient Algorithm for Detection of Black Hole Attack in AODV based MANET", Int. journal of com. applications, vol. 66, no. 18, pp. 18-24, March 2013.

[41] I. Ullah, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocol", Master Thesis, 2010.

[42] https://en.wikipedia.org/wiki/Grover%27s_algorithm, [Accessed 15 Sep. 2020].

[43] I. Butun, S. D. Morgera and R. Sankar, "A survey of intrusion detection systems in wireless sensor networks", Communications Surveys & Tutorials, IEEE, vol. 16, no. 1, pp. 266-282, May 2014.

[44] IBM 5 qubits qunatum computer. "www.research.ibm.com/quantum", [Accessed 27 February 2017].

[45] Libquantum," http://www.libquantum.de/api/1.1/index.html", [Accessed 27 February 2017].

[46] S. Farzai, M. Hosseini Shirvani, M. Rabbani, "Communication-Aware Traffic Stream Optimization for Virtual Machine Placement in Cloud Datacenters with VL2 topology", *Journal of Advances in Computer Research*, vol. 11, no. 3, pp. 1-21, Sep. 2020.

[47] G. R. Amin and M. Hosseini Shirvani, "Evaluation of scheduling solutions in parallel processing using DEA FDH model," *J. Ind. Eng. Int*, vol. 5, no. 9, pp. 58–62, June 2009.

[48] M. Hosseini Shirvani, "Evaluating of Feasible Solutions on Parallel Scheduling Tasks with DEA Decision Maker," *J. Adv. Comput. Res.*, vol. 6, pp. 109–115, 2015.

[49] S. Hosseinzadeh, M. Hosseini Shirvani, "Optimizing energy consumption in clouds by using genetic algorithm", Journal of multidisciplinary engineering science and technology, vol. 2, no. 6, pp. 1431-1434, June 2015.

[50] www.stackoverflow.com/questions [Accessed 15 Sep. 2020].