Improved Worm hole attack detection and prevention by optimization

Sheenam Rani[1], Er. Abhinash singla[2]
[1,2]*Bhai gurdas institute of engg and technology*
([1]sheenamarora27@gmail.com)

Abstract-A Wireless Sensor Network (WSN) is a collection of petite sensor terminals, capable of sensing and communication. Here topology is dynamic Node developments result in dynamic topology and cause link failures in an Ad-hoc. Here focusing on the using of packet scheduling technique for DSR WITH OPTIMIZATION (Ad Hoc on Demand Distance Vector) routing protocol by weight hop based scheduling in this paper. The transitional node starts the packet scheduling and manages its buffer memory according to data transfer rate. Intermediate store the data packets and repair the broken route and manage overflow of data packets. This proposed system attempt to send the data packet by utilizing backup routes opposed to dropping it. It evaluates the planned procedure on MATLAB. Simulation results show that proposed scheme performance is better than DSR WITH OPTIMIZATION.

Keywords-*wsn;optimization;energy.*

I. INTRODUCTION

Wireless sensor networks are the application based networks which comprise of various sensor nodes. WSN is an arrangement of many sensor gadgets which speak with wireless networks with the assistance of restricted vitality expending steering conventions. Wireless Sensor networks are thick wireless networks of little, cheap, low-control, disseminated self-ruling sensors which amass and proliferate natural information to encourage checking and controlling of physical conditions from remote areas with better exactness [1].

For the most part, it is accepted that every sensor in a system has certain limitations as for its vitality source, power, and memory and figuring capacities. It contains a door that gives wireless network back to the wired world and dispersed nodes. It can likewise be characterized as a system of gadgets that can impart the data accumulated from an observed field through wireless connections. The information is sent through different nodes with an entryway and the information is conveyed to different networks like wireless ethernet. These networks are utilized to control physical or ecological conditions like sound, weight, temperature and so forth.

WSN nodes have constrained battery limit. To build the life expectancy of WSN the usage of vitality in a productive way is a most normal issue. As the utilization of WSN are expanding step by step and has numerous varieties like target following condition observing, air contamination checking and so on. These applications require fast correspondence between sensor nodes [2].

Wireless sensor network is used in various fields for the effective communication process in which user sends their information from one node to another node. Sometimes a user sends the secret information, data on the wireless network, it is very important to send this information very safely. In this network sensor nodes used wireless communication and it is easy to eavesdrop. The attacker can easily inject malicious messages into the network [3].

II. LITERATURE REVIEW

Dema et al. deals with the security issue in the wireless sensor network. The author proposed an algorithm which provides the effective security to the wireless sensor network by identifying the nodes using the node ID. It also provides the Load Balancing feature for monitoring the nodes. In this algorithm, nodes can be rerouted to avoid the attacked nodes. The simulation results show that it works very efficiently on the live attack [1]. Abduvaliyev, Abror, et al. survey of the work done on IDS in wireless sensor network. In this paper author also discussed the various IDS approaches that are used in the detection of anomaly and misuse detection. A brief description of WSN attacks is also available in this paper. The main of the author is to find out the advancements in the area of wireless sensor network. It provides the new topics of the research in this field [2].

Jan, Mian, et al. proposed a lightweight payload-based mutual authentication approach for a cluster based wireless sensor network. This is also called as PAWN approach. During the implementation process, it is implanted in two steps. First, the optimal percentage of the cluster heads are selected, authenticated and allowed to communicate with the neighboring nodes. Second, each cluster head is in a role of server and provides the authentication to the nearby nodes. This scheme is validated with various schemes and the results

show that if performed very well [3]. Salehi, S. Ahmad, et al. in this paper, the author proposed an algorithm to avoid the Sink-Hole attack. In sinkhole attack, the intruder attracts the nearby nodes with unfaithful routing information, and presents change the data through these nodes. For detection of intruders in the sinkhole attack firstly finds the suspected nodes by analyzing the data. The proposed algorithm performance has been evaluated by the simulation process and its provide the results with high accuracy [4].

Jamil et al. proposed a Hierarchical Key Establishment scheme called HIKES. The base station in this scheme is the central trusted authority and it issues the private keys to the local authorities. It uses the partial key escrow scheme that enables the sensor node selected as a cluster head to generate the cryptographic key. This scheme reduces the communication cost with the base station. It provides the efficient broadcast authentication. HIKES provide the high addressing flexibility and network connectivity to all sensor networks [5]. Lu, Huang et al. studied the secure data transmission for cluster based wireless sensor network in which clusters are built dynamically and periodically. In this author proposed two data transmission protocol of the cluster based WSN these are SET-IBS and SET-IBOOS, by using identity-based digital signatures (IBS) and the identity-based online/offline digital signature (IBOOS) scheme. These schemes reduce the computational overhead of the security. It provides the security against the various attacks. These protocols performed better than existing protocols [6].

Raje et al. proposed the fuzzy based approach for providing the security to the wireless sensor network. This approach enhanced the routing, security and reliability in the WSNs. In this approach, firstly select the sensor node on the basis of the energy of the node. This node is called as cluster head, which performs the operations like data aggregation. This approach works on the following parameters like packet transmission rate, packet received rate, and a packet drop [7]. Shafiei, Hosein, et al. this proposed two approaches that detect and reduce the attacks in wireless sensor networks. This distributed approach estimates the energy holes in the wireless sensor network. It detects the Sink Hole attacks based on hazard model. The simulation results of this approach provide the effectiveness and correctness [8].

Amish et al. proposed a method of detection and prevention of a Worm Hole attack in the wireless sensor network. The author surveyed the many techniques and analyzed them to provide this approach. Ad-Hoc on Demand multipath distance vector routing is based on the round trip time (RTT) mechanism. NS2 simulator is used to perform the all tasks of simulation [9]. Jiang, Jinfang, et al. in this paper, the author proposed a model Efficient Distributed Trust Model (EDTM) for wireless sensor network. This model analyzed the nodes on the basis of packet received by sensor nodes. This model concerns the communication, trust, energy trust and data trust during the calculation of direct trust. The defined trust improves the accuracy of the model and it performs better than the existing nodes [10].

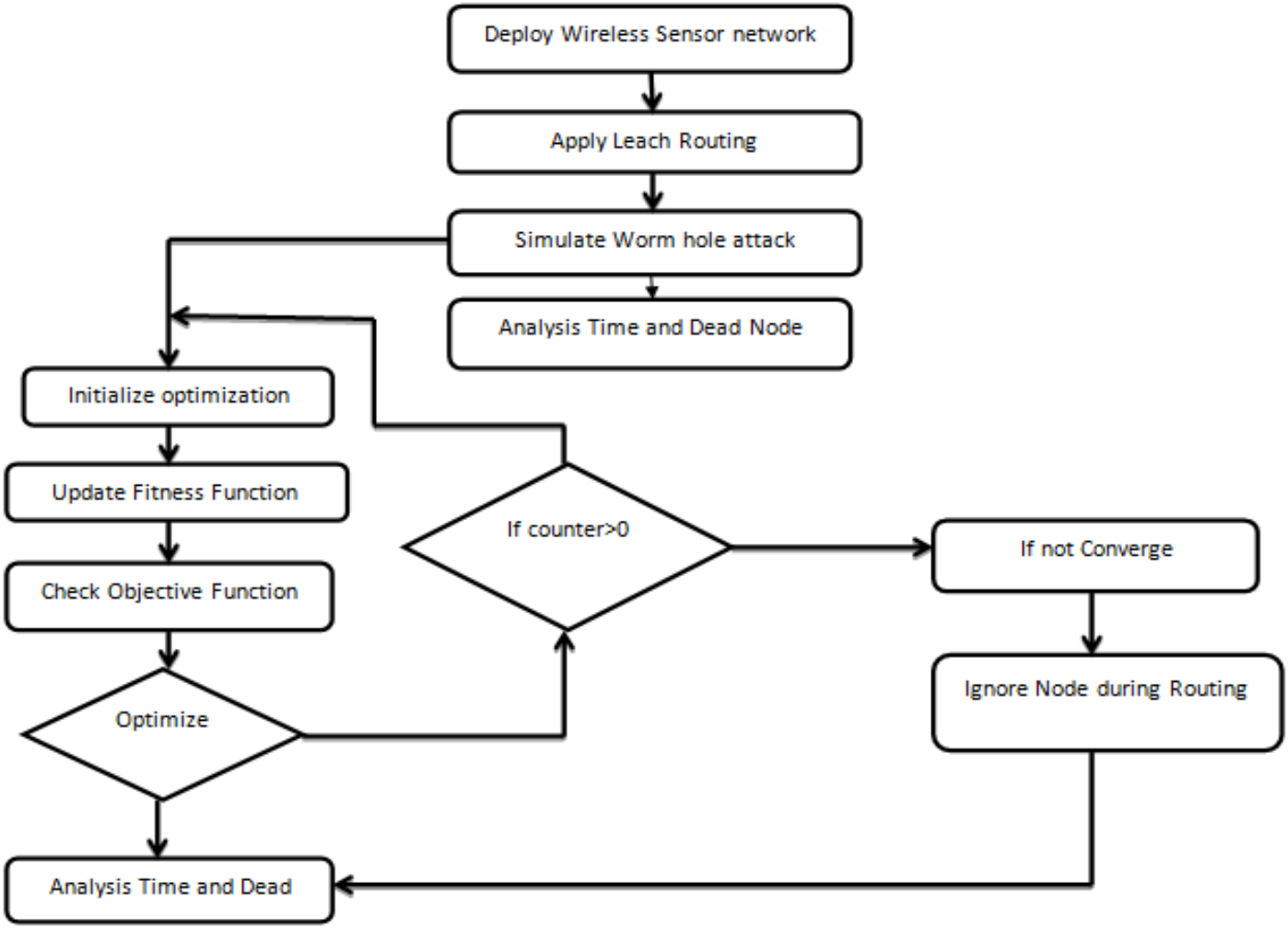
III. PROPOSED WORK

A. Grey Wolf Optimization-It is a meta-heuristic algorithm which simulates the leadership hierarchy and hunting behavior of wolves. The fitness of the wolves measured in the form of alpha, beta and delta. The figure 1.2 given below shows the hierarchy level of the wolves. Grey wolves have the ability of memorizing the prey position and encircling them. The alpha as a leader performs in the hunt. For simulating the behavior of grey wolves hunting in the mathematical model, it is assumed that the alpha (α) is the best solution, the second optimal solution is beta (β) and the third optimal solution is delta (δ). Omega (ω) is assumed to be the candidate solutions. Alpha, beta and delta guides the hunting while position is updated by the omega wolves by these three best solutions considerations.

1) Methodology steps:-

Step 1: Deploy the wireless sensor network and apply the leach routing on it.Low Energy Adaptive Clustering Hierarchy (LEACH) is a media access control protocol which is integrated with the clustering and simple routing protocol in the WSNs. The network is made up of nodes and some of the nodes are called cluster-heads. Leach is basically a dynamic routing algorithm because the job of cluster head rotates. This algorithm reduces the intra-cluster and inter-cluster collisions. The Leach routing algorithm works in two phases that are:

a) Set-up Phase: in this phase cluster heads are chosen
b) Steady State: In this phase cluster head is maintained when the data is transmitted between nodes.



Step 2: Simulate the wormhole attack on the wireless sensor network.
Step 3: Initialize the optimization then Update the fitness function and check the objective function.
Step 4: Check the function is optimized or not if it is optimized analyze the time and dead node otherwise check the counter.
Step 5: If counter is greater than 0 than node is not converged and it is not considered for the routing otherwise go to step 2

IV. RESULTS AND DISCUSSION

This section of the paper represents the results with optimization approach and existing approach on the basis of different parameters. The parameters used to evaluate the performance are Data Transmission, Energy consumption, Total number of Alive and Dead nodes in the present wireless sensor network.

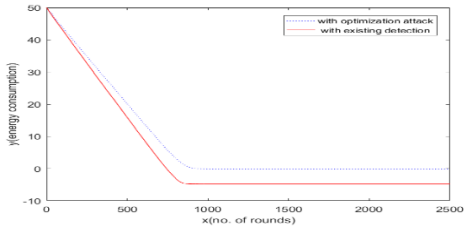


Fig.1.1: Energy comparisons of WSN nodes

In figure 1.1 it depicts the total energy consumption in the number of rounds. The x-axis represents the number of rounds

and y-axis represents the energy consumption per round. The Red curve shows the data transmitted in existing approach and dotted blue line represents energy consumption with optimization .

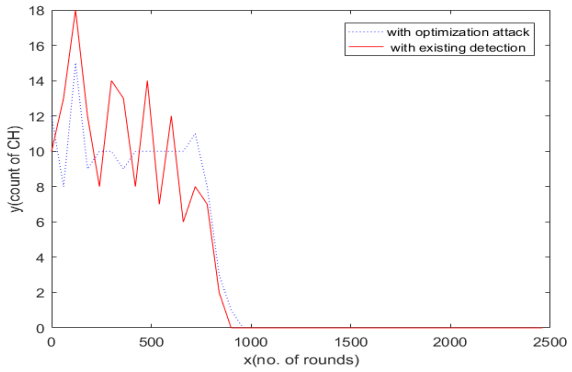


Fig. 1.2: cluster head comparison of WSN nodes

In figure 1.2 it depicts the count of cluster heads in the number of rounds. The x-axis represents the number of rounds and y-axis represents the count of cluster heads. The Red curve shows the data transmitted in existing approach and dotted blue line represents count of cluster heads with optimization.

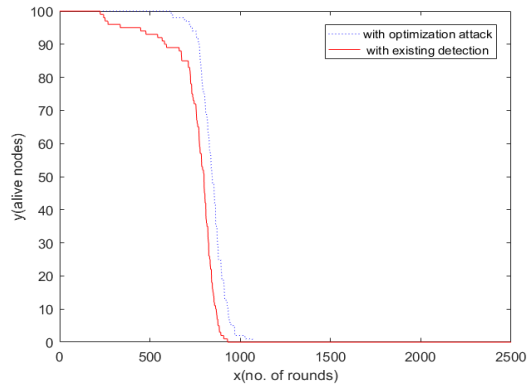


Fig.1.3: Alive node comparisons of WSN nodes

In figure 1.3 it depicts the total alive nodes in the rounds in WSNs. The x-axis represents the number of rounds and y-axis represents alive nodes. The Red curve shows the alive nodes in existing approach and dotted blue line represents alive nodes with optimization.

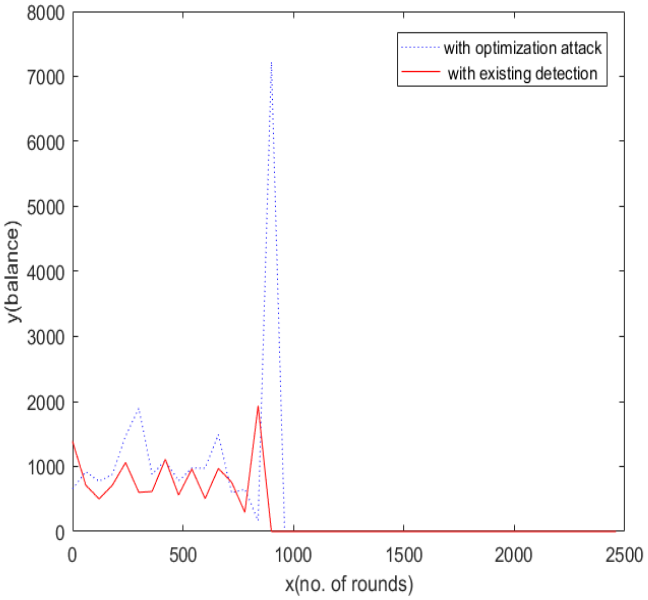


Fig.1.4: balance of node detection comparison of WSN nodes

The figure 1.4 shows the number of balance nodes according to the number of rounds. The x-axis represents the number of rounds and y-axis represents the count the number of balance nodes. The Red curve shows the data transmitted in existing approach and dotted blue line represents the number of balance nodes with optimization. The number of balanced node is always high than the existing approach.

V. CONCLUSION

DSR WITH OPTIMIZATION routing protocol uses Weight hop based packet scheduling in this model. The impact of various scheduling algorithms for DSR WITH OPTIMIZATION and modified DSR WITH OPTIMIZATION was assessed. The routing protocol and portability demonstrate the packets in queue composition. As a result of data traffic, there is a network congestion delay during low mobility whereas in at High mobility, it's influenced by route changes in replication results. Preparing algorithms that give higher weight to data packets with little quantities of hops or shorter geographic separations to their goals diminish normal postponement fundamentally with no extra control parcel trade. This is used for customization DSR WITH OPTIMIZATION. Result demonstrates impressively littler postponement than the other planning Algorithms. The lessening in the normal postpone diminishes as the portability of nodes.

REFERENCES

[1]. Aldhobaiban, Dema, Khaled Elleithy, and Laiali Almazaydeh. "Prevention of Wormhole Attacks in Wireless Sensor Networks." *Artificial Intelligence, Modelling and Simulation (AIMS), 2014 2nd International Conference on*. IEEE, 2014.

[2]. Abduvaliyev, Abror, et al. "On the vital areas of intrusion detection systems in wireless sensor networks." *IEEE Communications Surveys & Tutorials* 15.3 (2013): 1223-1237.

[3]. Jan, Mian, et al. "PAWN: a payload-based mutual authentication scheme for wireless sensor networks." *Concurrency and Computation: Practice and Experience*29.17 (2017).

[4]. Salehi, S. Ahmad, et al. "Detection of sinkhole attack in wireless sensor networks." *Space Science and* Communication *(IconSpace), 2013 IEEE International Conference on*. IEEE, 2013.

[5]. Ibriq, Jamil, and Imad Mahgoub. "HIKES: Hierarchical key establishment scheme for wireless sensor networks." *International Journal of Communication Systems* 27.10 (2014): 1825-1856.

[6]. Lu, Huang, Jie Li, and Mohsen Guizani. "Secure and efficient data transmission for cluster-based wireless sensor networks." *IEEE transactions on parallel and distributed systems* 25.3 (2014): 750-761.

[7]. Raje, Radhika A., and Apeksha V. Sakhare. "Routing in wireless sensor network using fuzzy based trust model." *Communication Systems and Network Technologies (CSNT), 2014 Fourth International Conference on*. IEEE, 2014.

[8]. Shafiei, Hosein, et al. "Detection and mitigation of sinkhole attacks in wireless sensor networks." *Journal of Computer and System Sciences* 80.3 (2014): 644-653.

[9]. Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." *Procedia computer science* 79 (2016): 700-707.

[10]. Jiang, Jinfang, et al. "An efficient distributed trust model for wireless sensor networks." *IEEE transactions on parallel and distributed systems* 26.5 (2015): 1228-1237.