A Novel Prevention Mechanism for Replay Attack in Distance Vector - Hop Localization Scheme

Simarjeet Kaur, Navdeep Kaur, Kamaljit Singh Bhatia

Abstract*: *Securing the process of node localization in Wireless Sensor Network (WSN) is an important area of research. In this paper, we focus on securing Distance Vector (DV)-Hop localization scheme from Replay Attack. The DV-Hop localization algorithm is a limit free hop based reference Wireless Sensor Network architecture. It faces a couple of issues like a route discovery mechanism and threat prevention issues. This paper focuses on the establishment of a prevention mechanism for DV-Hop scheme against a Replay attack. The proposed architecture uses an Artificial Bee Colony (ABC) and Neural Network in order to prevent the attack. To prove the efficacy of the proposed scheme, the network scenario without replay attack, with replay attack and with attack after prevention mechanism is considered. The simulations are conducted for 200 iterations using MATLAB. The evaluation is done on the basis of parameters like localization error and transmission loss. Localization error of the proposed framework is similar to localization error without an attack which is about 0.57, and the maximum localized error is about 0.92. The maximum transmission loss without attack and after prevention is very close and varies by only 2 %, which is very good. The experimental results reveal that the proposed technique successfully prevents replay attack in WSN.

Index Terms*: *DV-Hop, Localization Error, Node Localization, Replay Attack, Transmission Loss, Wireless Sensor Network

I. INTRODUCTION

The multi intersection of science has become a major research factor with the development of high technology. Wireless communication and sensor network technology are the two integral developments which became more mature bypassing of years and are in continuity to evolve [1]. Wireless sensor network (WSN) is an incorporated network technology embedded computing technology and other advanced technologies. Monitoring the climate as well as light, temperature, humidity, monitoring of atmospheric pollution, forecasting, detection of threat, etc the beneficial alternative to this approach could be WSN, which covers the broad aspect of applications. It is crucial to monitor activities and to determine the location by sensor nodes as well as location of incident for WSN due to the fact of size, cost, and consumption of power plus other factors it is next to impossible for each node to determine GPS accuracy positioning capability [2].

Revised Manuscript Received on June 15, 2019.

Simarjeet Kaur, Assistant Professor, Department of Computer Science & Engineering, Chandigarh University, Gharaun, and Research Scholar, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.

Navdeep Kaur, Professor, Department of Computer Science, Sri Guru Granth Sahib World University, Fatehgarh Sahib, Punjab, India.**Kamaljit Singh Bhatia**, Assistant Professor, Department of Electrical Engineering, IK Gujral Punjab Technical University, Batala Campus, Punjab, India.

For that reason, the DV-Hop algorithm has been used in this research for proposing a Novel Prevention Mechanism for Replay Attack. The DV-Hop localization is one of the finest localization schemes in WSN. The hop count is the number of sensor nodes between source and destination. A route is designed to send the packet from end to end. Sensor nodes cannot send the data from the source to the destination directly as the attached sensor of the nodes are never big enough to cover the entire area. This results in a route discovery process. Adding intermediate nodes not only balances the load of the sensor nodes but also ensures the packet delivery process [3, 4]. Any process is never complete in it and hence ends up with some drawback. Keeping multiple hops in a route also has this issue of data leakage and threat. We never know whom to trust and who do not. This paper focuses on the prevention of network from reply attack [5-6]. Basic steps involved in the implementation of DV-Hop method are:

- Calculation of minimum hop counts between each target node and anchor node.
- Calculation of average hop size of each anchor node.
- Co-ordinate calculation of target nodes.

Further, it is used for the discovery of routes and designing process takes place which involves the packet delivery.

II. LITERATURE REVIEW

The DV-hop algorithm is not much complicated to implement and the problem associated with it is the improvement to localization accuracy, it can localize target nodes which have no neighbor or few neighbors anchor nodes but with less precision. For that reason, many of enhanced versions of the algorithm has been proposed in the literature [7, 8, 9, 10–17]. Mehrabi et.al implemented an extended version of the DV-Hop algorithm on the basis of SFLA combining GA-PSO. The combination of SFLA and GA-PSO hybridized algorithm is highly complex for that matter convergence becomes slower and it consumes more computational time, in spite of performing well. It does not consider the impact of collinear anchor nodes that engage in the localization process of a particular target node. Kumar et al. [14] also proposed a superior DV-Hop algorithm where the hop size of the anchor nodes is used to evaluate the distance between the anchor and the target nodes. Research focuses on the issue that significant errors are produced in distance estimation when the anchor node is not near from the target node. Other authors Dengyi et al [18] also researched on WSN the improved version of the DV-Hop algorithm in which two methods are employed to improve the localization accuracy in the complete process. Chen et al. [8] give an improved DV-Hop algorithm based on particle swarm optimization (PSO) improving the accuracy rate. Shahzad et al [12] implemented a DV-max-hop localization algorithm for isotropic as anisotropic networks. A control parameter called MaxHop

which was preselected on the grounds of network topology features to improve network localization precision.

III. PROPOSED MODEL

The proposed work aims to identify and block the replay node. A replay attack floods the same data into the network. The receiver gets confused with 'N' number of data packets for one packet value. The probability of receiving correct data packet is 1/N. More the number of flooded packets, less is the chance of getting the correct packet.

$$P(t)=1/N \quad \text{----------(1)}$$

P(t) is a true packet receiving probability and N is the total number of received packets.

The structure of the replay attack is as follows: Figure 1 depicts the source to destination route discovery. At the same time, Figure 2 depicts the architecture of the replay attack.

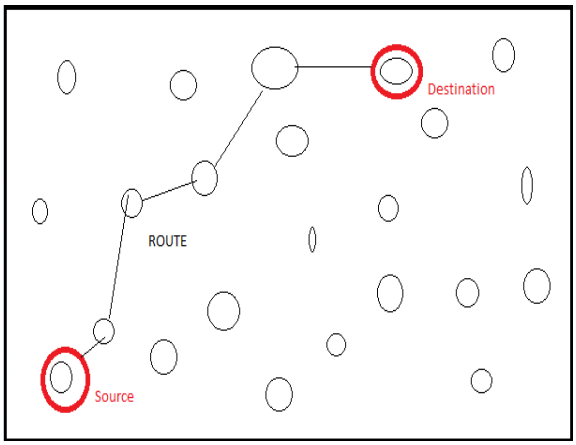

Figure 1: Network route with Source and Destination

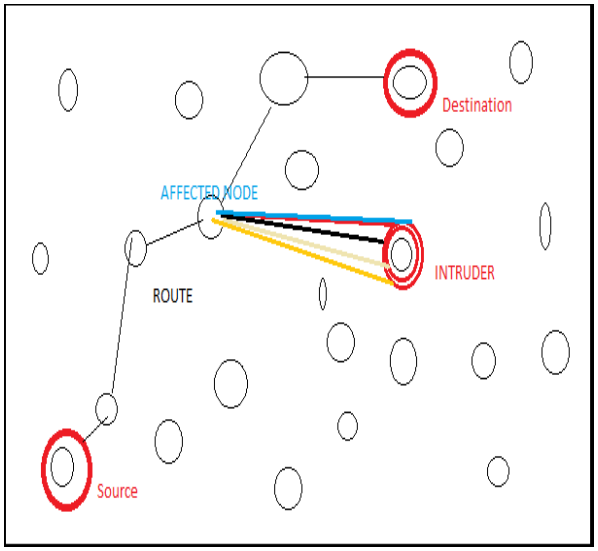

Figure 2: Effect of Replay Attack

Figure 2 demonstrates that the intruder (Replay attacker in this case) attacks on any of the node in the network. Different colors show different types of the affected packet for one packet frame at the same node. Now the affected node will not understand what exactly is going on at the backend and will dump a lot of packets.

First of all, a network model is established for the route discovery process. There are two algorithms: Algorithm 1generates properties of the nodes and Algorithm 2 finds the coverage set of the nodes.

Algorithm 1: Generation of the Node Properties

```
1. function [energy_consumption_normal, energycpn, packet_drop, delay_normal, network] =
generatenodeproperties(nodes)
// This function generates the node's properties which has to be deployed in the network
2. network=[];
3. foreach I in nodes
4.    energy_consumption_normal(i)=50*rand;
5.    energycpn(i)=10*rand; // this is the consumption of energy of a node if it is involved in any procedure
6.    packet_drop(i)=30*rand; // normally network drops some packets , a random value is initialized
7.   delay_normal(i)=30*rand;
8. End for
9. network.energy_consumption_normal=energy_consumption_normal;
10. network.packet_drop=packet_drop;
11. network.delay_normal=delay_normal;
12. save nodeproperty
13. End function
```

Algorithm 1 generates random values for a random ad-hoc network to be deployed. After applying this, a node network would be prepared which will have random values of the nodes. The random values were taken to generate uncertainty in the network and to demonstrate the efficiency of the suggested algorithm.

Algorithm 2: Find coverage set of network nodes

Function [coverage_set, path] = FindPathandCoverage (Nodes, x, y)

// x and y is the combined GPS(Global Position System) location of a node

// Nodes is the total count of the nodes

1. for countervalue = 1: numel(all_x_location) // total x locations
2. dest = network.destination; // random destination of the network
3. if countervalue ~ = network.destination
4. dist=squareroot((all_x_location(countervalue)-all_x_location(dest))^2+(all_y_values(countervalue)-all_y_values(dest))^2) ;
   a. If dist<200 // the total breadth of the network is 1000 meters, hence the coverage range has been set to be 200 meters
   b. cov_values (cov_valuescount) = countervalue;
   c. cov_valuescoun t= cov_valuescount + 1;
   d. End if
5. End if
6. End for
7. End for

Algorithm 2 is designed to find the coverage set of the network nodes. It's the coverage set which illustrates that which node can be selected as a routing path element.

The prevention technique consists of two parts. The first part is looking for the suspects that are achieved using Artificial Bee Colony optimization algorithm and the second part is to search the actual intruder out of the suspect list that can be achieved using machine learning algorithm.

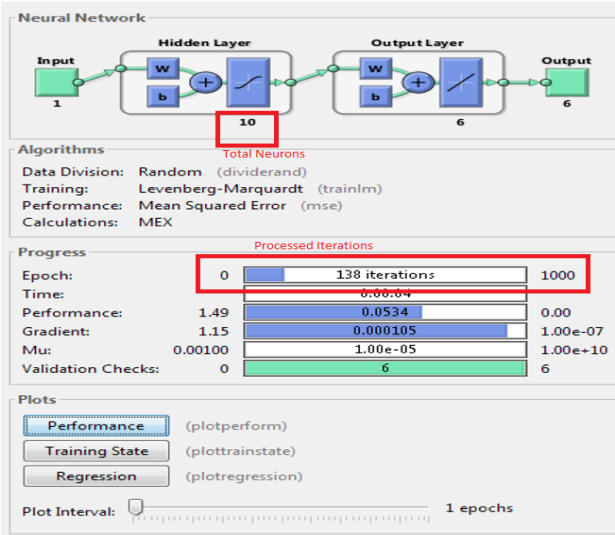

Figure 3: Training Architecture of ANN

Figure 3 defines the training architecture of Feed Forward Back Propagation Neural Network (FFBPNN). The figure has a total of three layers of input, a hidden layer, and an output layer. A single neuron is sending to the hidden layer, where a total of 9 neurons are sending and we obtain 10. The 10 neurons are further sent to the output layer, in which the neurons are subtracted by with the help of weight value and bias value and we will get 6 neurons at the output. Artificial Neural Network (ANN) works on the Levenberg Marquardt algorithm with Mean Square Error (MSE) as a performance metrics. The training of ANN depends upon the performance parameters named as Epoch, time, performance, gradient, mutation and validation check. If any of the parameters is completed the FFBPNN is trained.

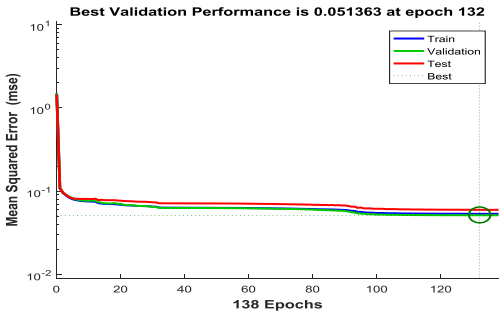

Figure 4: Performance of FFBPNN

The performance of the FFBPNN is represented in the form of a graph as shown in figure 4. FFBPNN's training is finished for 138 iterations. From the above graph, it is noted that there are four distinct lines represented by distinct colors such as blue, green, red and dotted line and each line denotes ANN's preparation, validation, test value, and best value respectively. At 138th iteration, the best value is achieved with MSE less than 0.1. Lower the value of MSE implies better FFBPNN training.

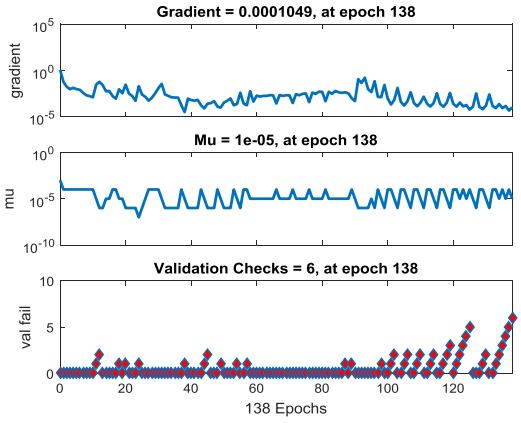

Figure 5: Training State

Figure 5 represents the training state of FFBPNN in graphical form. From the above waveforms it is clear that FFBPNN is trained with gradient, mutation and validation checks of 0.0001049, 1e-05 and 6 respectively for maximum 138 epochs.

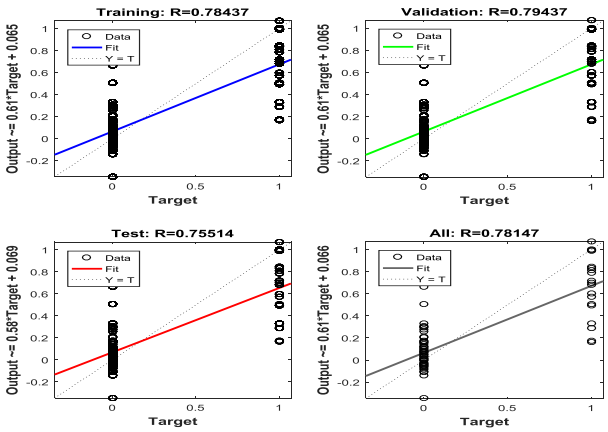

Figure 6: Regression state of ANN

Figure 6 comprises four graphs for validation, testing, and regression training. Figure 6 shows that when the training data is 0.78437, the test information is 0.75514 and the validation value is 0.79437, the regression value acquired is 0.78147.

IV. RESULTS AND DISCUSSION

The experimental results are obtained based on the following parameters:

- Localization error
- Transmission Loss

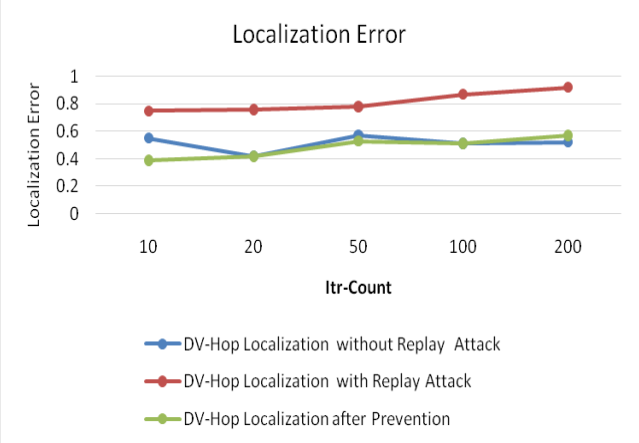

Figure 7: Localization Error

The localization error of the proposed model is close to the value which is before the attack. This satisfies the significance of the proposed algorithm. The maximum localization error of the proposed framework is .57 and the maximum localization error without an attack is also .57 whereas the localization error with the attack is .92. Figure 7 represents the graphical pattern of Localization error for all three conditions.

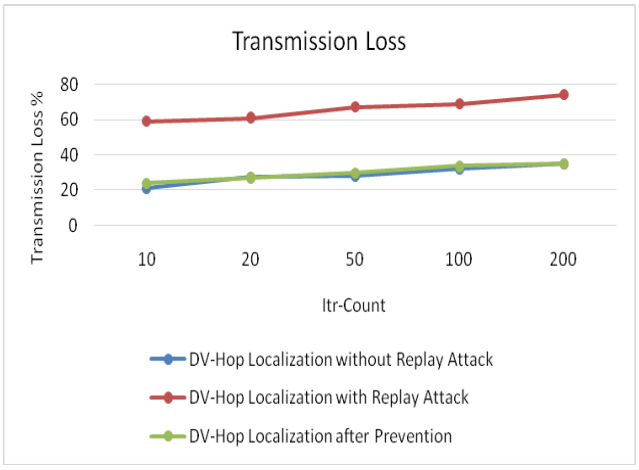

Figure 8: Transmission Loss

Figure 8 represents the transmission loss. The maximum transmission loss without attack and after prevention is very close and they only vary by 2%.

V. CONCLUSION AND FUTURE WORK

This paper focuses on the development of a prevention mechanism based on ABC and Neural Network. An iterative structure of Neural Network is presented. The prevention algorithm is based on the fitness function of ABC and neuron structure of ANN. The evaluation is based on localization error and transmission loss. The prevention structure of Replay attack gains quite an improvement. The difference in the normal network and prevention structure is only 2%. The current research work opens a lot of future gates. The variation of a number of neurons can play a vital role in the improvement.

REFERENCES

1. S. Biswas, R. Das, and P. Chatterjee, "Energy-efficient Connected Target Coverage in Multi-hop Wireless Sensor Networks" In *Industry Interactive Innovations in Science, Engineering and Technology*,2018, pp.411-421, Springer, Singapore.
2. V. Mittal, S. Gupta, and T. Choudhury, "Comparative Analysis of Authentication and Access Control Protocols against Malicious attacks in Wireless Sensor Networks" In *Smart Computing and Informatics*,2018, pp. 255-262, Springer, Singapore.
3. N. Jain, S. Madan and S. K. Malik, "A Charge System Search based DV Hop Algorithm for Wireless Sensor Networks" International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2018, 3(1),pp.568-576.
4. O. Cheikhrouhou, G M Bhatti and R. Alroobaea, "A Hybrid DV-Hop Algorithm Using RSSI for Localization in Large-Scale Wireless Sensor Networks" *Sensors*, 2018, *18*(5),pp. 1-14.
5. L. Cui, C. Xu, G. Li, Z. Ming, Y. Feng and N. Lu, " A High Accurate Localization Algorithm with DV-Hop and Differential Evolution for Wireless Sensor Network" *Applied Soft*

Computing, 2018, *68*, pp.39-52.

6. W. Zhao, S. Su and F. Shao, " Improved DV-Hop Algorithm Using Locally Weighted Linear Regression in Anisotropic Wireless Sensor Networks" *Wireless Personal Communications*, 2018, *98*(4), pp.3335-3353.
7. B. Peng and L. Li, "An Improved Localization Algorithm based on Genetic Algorithm in Wireless Sensor Networks", Cognitive Neurodynamics, 2015, 9(2),pp. 249–256.
8. X. Chen and B. Zhang, "Improved DV-Hop node Localization Algorithm in Wireless Sensor Networks" International Journal of Distributed Sensor Networks, 2012, pp.1-7.
9. Q. Qian, X. Shen and H. Chen, "An Improved Node Localization Algorithm based on DV-Hop for Wireless Sensor Networks" Computer Science and Information Systems, 2011, 8(4), pp.953–972.
10. X. Chen and B. Zhang, "Improved DV-Hop Node Localization Algorithm in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2012, pp.1-7.
11. L. Gui, T. Val, A. Wei, and S. Taktak, "An adaptive range free localisation protocol in wireless sensor networks", International Journal of Ad Hoc and Ubiquitous Computing, 2014, 15(1–3),pp. 38–56.
12. F. Shahzad, T. R. Sheltami and E. M. Shakshukhi, " DV-maxHop: A Fast and Accurate Range-Free Localization Algorithm for Anisotropic Wireless Networks. IEEE Transactions on Mobile Computing, 2017, 16(9), pp. 2494-2505.
13. S. Kumar and D. K. Lobiyal, "Power Efficient Range-Free Localization Algorithm for Wireless Sensor Networks", Wireless Networks, 2014, 20(4), pp. 681–694.
14. S. Kumar and D. K. Lobiyal, "An Advanced DV-Hop Localization Algorithm for Wireless Sensor Networks. Wireless Personal Communications, 2013, 71(2), pp.1365–1385.
15. W. Ren and C. Zhao, "A Localization Algorithm based on SFLA and PSO for Wireless Sensor Network" Information Technology Journal, 2013, 12(3), pp.502–505.
16. M. Mehrabi, H. Taheri and P. Taghdiri, "An improved DV-Hop Localization Algorithm based on Evolutionary Algorithms", Telecommunication Systems, 2017, 64(4), pp.639–647.
17. G. Zhou, T. He, S. Krishnamurthy and J. A. Stankovic, "Models and Solutions for Radio Irregularity in Wireless Sensor Networks", ACM Transactions on Sensor Networks (TOSN), 2006, 2(2),pp. 221–262.
18. Z. Dengyi and L. Feng, "Improvement of DV-Hop localization algorithms in wireless sensor networks" In Int Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), IEEE, 2012,vol. 2, pp. 567–569.

AUTHORS PROFILE

Simarjeet Kaur completed her BTech(Information Technology) in 2010 and MTech(CSE) in 2012. Currently she is pursuing her PhD (CSE) in Wireless Sensor Networks from Sri Guru Granth Sahib World University and is also serving as an Assistant Professor (CSE) at Chandigarh University, Gharuan. She has published 20 research papers in various national and international journals.

Dr Navdeep Kaur did her PhD from Indian Institute of Technology (IIT) Roorkee and now she is working as Professor in Computer Science Department at Sri Guru Granth Sahib World University. Her area of research are Information Security and Mobile Computing. She has published 136 research papers in various refereed International journals and conferences. She is a life member of Indian Society of Technical Education (ISTE).

Dr Kamaljit Singh Bhatia is working as an Assistant Professor at IK Gujral Punjab Technical University Batala Campus. He has published more than 60 research papers in various refereed International journals and conferences. He has guided many MTech and PhD students for their research work. He has also published four books and has membership of various professional bodies.