ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

IJESRT
INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

AN ARTIFICIAL INTELLIGENCE BASED LIGHT WEIGHT CRYPTOGRAPHIC ADDRESS GENERATION (LW-CGA) USING OPTIMIZATION FOR IPv6 BASED MANETs

Rakesh Kumar Pal[*1] & Dr. Deepali Gupta[2]
[*1]Maharishi Markandeshwar University, Ambala, India
[2]H.O.D Computer Science Department, Maharishi Markandeshwar University, Ambala, India

DOI: 10.5281/zenodo.1345600

ABSTRACT

Due to rising application requests and also for dependable data transfer, security concern is one the important research areas in the field of mobile ad hoc networks (MANET). As we know that MANET is formed by a number of mobile nodes and each node communicate with each other using their energy capabilities. To solve the security and routing protocol in IPv6 based MANET, the Secure Neighbor Discovery (SeND) routing protocol will be designed with concept of artificial intelligence techniques to overcome the security threats during auto-configuration has proven to face security and technical issues in MANETs. The SeND routing protocol uses RSA and SHA-1 (Secure Hash Algorithm) implementation for ensuring privacy enabled auto-configuration. In Internet Protocol Version (IPv6) based MANETs, the neighbor discovery enables nodes to self-configure and communicate with neighbor nodes through auto-configuration. The Stateless address auto-configuration (SLAAC) has proven to face several security issues during the data transmission form source node to destination node. Even though the SeND uses Cryptographically Generated Addresses (CGA) to address these issues, it creates other concerns such as need for Cryptographic Address (CA) to authenticate hosts, exposure to CPU exhaustion attacks and high computational intensity. In this work, we will present empirically strong Light Weight Cryptographic Address Generation (LW-CGA) using entropy gathered from system states using artificial neural network techniques with route optimization. In this article, we present the effect of attackers in the IPv6 based MANET with their prevention technique. For preventing the network from attacker, genetic algorithm along with the artificial neural network is used and the parameters such as Throughput, Delay, BER and Energy consumptions are measured and compare with the simulator with using genetic algorithm and artificial neural network for prevention of network.

Keywords: IPv6, MANET, Genetic Algorithm, Artificial Neural Network, and Light Weight Cryptographic Address Generation (LW-CGA).

I. INRTODUCTION

Mobile Ad-hoc system is the kind of system, where communication happens in remote medium utilizing an access point. Different systems like WSN (Wireless Sensor Network) are the systems in which communication happens through physical medium. It is a self-designing system, where the numbers of switches are associated through remote connections. All hubs are free to move from one place to another. All the hubs that are associated allowed to move and are sorted out arbitrarily. Restricted to the framework of remote systems where every client straightforwardly corresponds with an access point or base station, a mobile specially appointed system namely, MANET, which is a sort of remote Ad-hoc network [1]. It is a self-arranging system of movable routers joined by remote connections with no entrance point. Each movable device in a system is self-governing as there is no central authority in the MANET. The movable devices are allowed to shift freely and compose themselves subjectively. Ad-hoc is mainly for one specific purpose and it is used in those areas where other means of network are not possible to establish. Ad-hoc network is the best example of MANET, and it is developed whenever required. Ad-hoc network doesn't depend on any fixed infrastructure i.e. the mobile Ad hoc especially mobile Ad hoc network. The Communication in MANET is occurring by utilizing multiple ways [2]. Hubs in the MANET offers the remote medium and the topology of the system changes sporadically also alertly. In movable area, breaking of communication connection is exceptionally less, as hubs are allowed to move to anywhere the thickness of hubs and quantity of hubs are relying on upon the application in which they are utilizing Mobile network. Mobile Ad hoc network have offered ascent to many applications. With numerous applications, there

ISSN: 2277-9655
Impact Factor: 5.164
CODEN: IJESS7

are still some outline issues and difficulties to overcome. In this paper, we introduced effect of attackers in the IPv6 based MANET with their prevention technique using SeND routing protocol. One of the novelties of SeND routing protocol, which is motivated by the huge propagation delay affecting the MANET, is that it is not a pure distributed routing protocol; rather, it is a distributed hybrid routing protocol that combines both SeND and optimization technique to optimize the route and prevent the network from attackers. IPv6 [2] based MANET with SeND and optimization technique aims at achieving three objectives,

1. High network throughput with less bit error rate,
2. Low transmission delay, and
3. Low energy consumption rate.

We demonstrate that IPv6 based MANET with authentication system using Light Weight Cryptographic Address Generation (LW-CGA) to manages the simultaneously achieve these three objectives during the transmission of packet data, which are usually not strictly affected by attackers. MANET is the main area of research because of some challenges and issues that still exist in the network [3]. MANET is the type of wireless network in which each node communicates with other node via wireless medium as shown in below figure. Communication between nodes is performed by direct connection or through multiple hop relays.

1. Lack of centralized management

MANET has de-centralized network, so there is no management that helps in detection of attack in the network. In addition, the absence of centralized system makes it difficult to establish trust among communicating nodes [4].

2. Resource Availability

Resource availability is difficult in MANET due to the de-centralized system. The only collaborative system is the system that has security provision to provide resources. Otherwise, because of security reason, resource availability can be difficult.

3. Scalability

As all nodes are connected via a wireless medium, so there is lot of mobility among the nodes that makes difficult to scale the system easily [5].

4. Cooperativeness

Routing algorithms helps in identifying which nodes are cooperating and which are not. So, by viewing in the network, one can estimate that non-cooperating nodes are attack based nodes and that nodes are called attack nodes.

5. Dynamic Topology

As nodes are not centralized in MANET, so they have a dynamic topology as they are changing time to time. The dynamic behavior has to be protected securely.

6. Limited Bandwidth

Infrastructure less networks has higher capacity than a wireless network. Also the wireless communication or infrastructures less networks have less transmission rate, good throughput.

7. Routing Overhead

Location within network is easily changeable in the MANET because of the presence of the old routing tables, which contains old address of route.

8. Hidden Terminal Problem

Collision of packets at a receiving node sometimes called hidden terminal problem, as this problem mainly occurs due to the simultaneous transmission of those nodes. Transmission of nodes mainly occurs because of the direct communication range.

9. Packet losses due to Transmission Errors

Factors like enlarged collisions due to the occurrence of buried terminals, presence of intrusion, uni-directional associates; recurrent path breaks due to mobility of nodes are making a high data packet loss in the network.

10. Mobility-induced Route Change
Suitable to the movement of node network topology is movable in nature. That is the main reason of sudden path breaks in the network.

Battery constraints
There are mainly power concerns in the network.

11. Security threats
The wireless medium is the main reason of adding vulnerabilities to the MANET system [6].

Types of manet
The various types of MANET are shown in figure 1 and are defined below section:

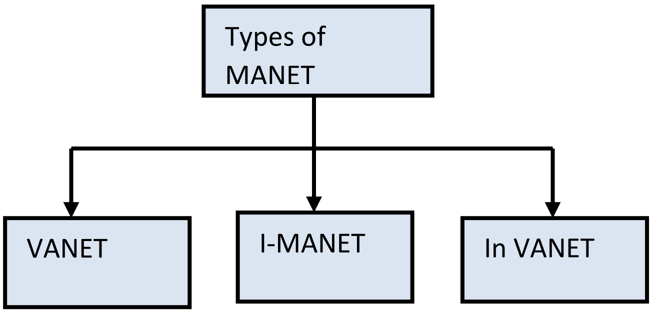

Figure 1: Types of MANET

- Vehicular Ad hoc Networks (VANETs) are used for the communication surrounded by the mobile vehicles. Thus, the communication being carried on even if the vehicles are moving in the different directions within a particular area.
- Intelligent Vehicular Ad hoc Networks (InVANETs) are used in cases like collision of vehicles or any other type of mobility problems.
- Internet Based Mobile Ad hoc Networks (I-MANET) are Ad hoc networks that link mobile nodes and fixed Internet-gateway nodes. Normal Ad hoc routing algorithms don't apply directly in these types of networks.

Routing protocols in manet
Routing protocols settle on a few policies which often governs the particular destination of statement packets by supply in order to purpose spot in the network. Within MANET, you can find several types of routing protocols every one of them is employed based on the network situation. Figure 2 laid bare principle classification from the routing protocols in MANETs.

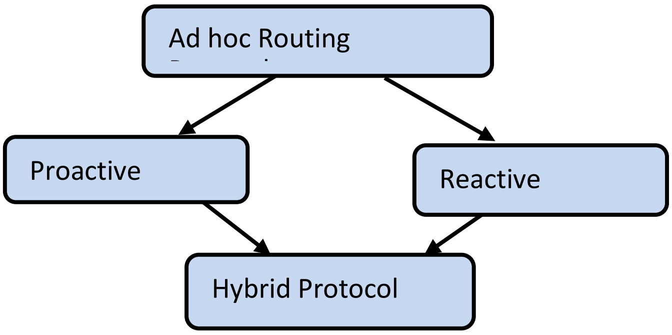

Figure 2: Classification of routing protocols

Above figure represent the classification of routing protocols which helps to find out the better route from source node to destination node using the concept of genetic algorithm and artificial neural network. In previous work "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs" is presented by [1]. In this work main problem occurs due to the limited bandwidth and processing power. So in this work we need to improve the privacy enable auto-configurable in MANET using more light weight techniques by using the concept of route optimization and artificial intelligence technique. The efficiency of proposed system is compared with the existing work and verifies the uses of genetic algorithm and artificial neural network as an artificial intelligence technique. To achieve better performance we need to follow the below mentioned methodology.

II. PROPOSED METHODOLOGY

There are certain steps that are required to be followed in order to create a simulated network in the IPv6 based MANET environment. These steps are defined as follows:

STEP 1: To design a network on the basis of certain width and height of the network.

STEP 2: Initialize the N number of nodes within the network

STEP 3: Define source node and destination node from the initialized nodes.

STEP 4: Set the coverage area for each node.

STEP 5: Develop a code for SeND routing protocol to create a route from the source node to the destination node with cryptographically concepts.

STEP 6: Analyze the performance of simulation work on the basic of QOS parameters if required the optimized the path using the Genetic Algorithm.

STEP 7: Set the objective function of the Genetic Algorithm according to the requirement.

STEP 8: On the basis of the hybridization of the ANN along with the Genetic algorithm we optimized the route and find out the best and optimal route for the data transmission based on the authentication process.

STEP 9: At last we calculate the performance parameters of proposed simulation work and compare with the existing work.

The used algorithm in the proposed work is given as;

Network deployment algorithm

```
Define height = 1000
Define width = 1000
Define N number of nodes for the simulation of network
For i = 1 to N
    Plot_node(i)=coordinate(X, Y)
    Define node name = N(i)
    Source_Node = random (N)
    Destination_Node = random(N)
    If Source_Node == Destination_Node
        Source_Node = rand(N)
        Destination_Node = rand(N)
    Else
        Source_Node = Source_Node
        Destination_Node = Destination_Node
    End
    Define Source_Node as source
    Define Destination_Node as destination
End
```

Coverage area creation algorithm and routing algorithm

```
$DefineCoverage\_Set = \frac{20 * Network - Width}{100}$
For i = 1 to N
    Cov_set(i) = Coverage_set(N)
    Cov_list(N, i) = Cov_set(i)
End
For i = 1 to N
    Route(1) = Source_Node
    Route(i) = Source_Node(Cov_se(N))
    If Cov_set(Source_Node) == empty
        Next_node = random
    End
    Repeat while destination is not found
    Route (last) = Destination_Node
End
```

Genetic algorithm with ANN

```
Initialize GA in simulator
Define population size, selection function, mutation function, crossover function etc (Default).
Data = Network Properties
$F_s$ = Selected value from the Data
$F_t$ = Threshold value from the Data (Average of Data)
$Fitness\_ \ function = \left| fs.................. \ fs \geq \ ft \right|$
                  $= \left| ft................Otherwies \right|$
No. of variables = 1
For i = 1 to Node within route
    Affected_Node (i) = GA(Fitness_function, Initialize GA, No. of variables)
End
Save the affected node list in the array of Affected_Node
For i = 1 to N
Initialize ANN with parameters
– Epochs (E)
– Neurons (N)
– Performance parameters: MSE, Gradient, Mutation and Validation Points
– Training Techniques: Levenberg Marquardt (Trainlm)
– Data Division: Random
For each set of T
    Group = Categories of Training Data
End
Initialized the ANN using Training data and Group
Net = Newff ($T, G, N$)
Set the training parameters according to the requirements and train the system
Net = Train (Training Data, Group, Neurons)
Classify the attackers
End
    If properties of Attackers Node == true
        Node not consider in the route
    Else
        Create an optimized route
    End
Calculate QOS parameters
End
```

In this work, we will be design an artificial intelligence based Light Weight Cryptographic Address Generation (LW-CGA) using optimization for IPv6 based MANETs. The objectives of this research work has been identified as follows

1) To study the previous routing and privacy mechanisms in IPv6 based MANETs.
2) To develop an optimization algorithm for the route discovery using genetic algorithm according to the objective function.
3) To authenticate the nodes during route discovery, Secure Neighbor Discovery (SeND) routing protocol will be designed with Light Weight Cryptographic Address Generation (LW-CGA) using artificial neural network techniques.
4) To evaluate QOS Parameters and compare with existing work.

Using the above mentioned algorithm and methodology step we design a flow chart of proposed IPv6 base MANET to achieve these objectives.

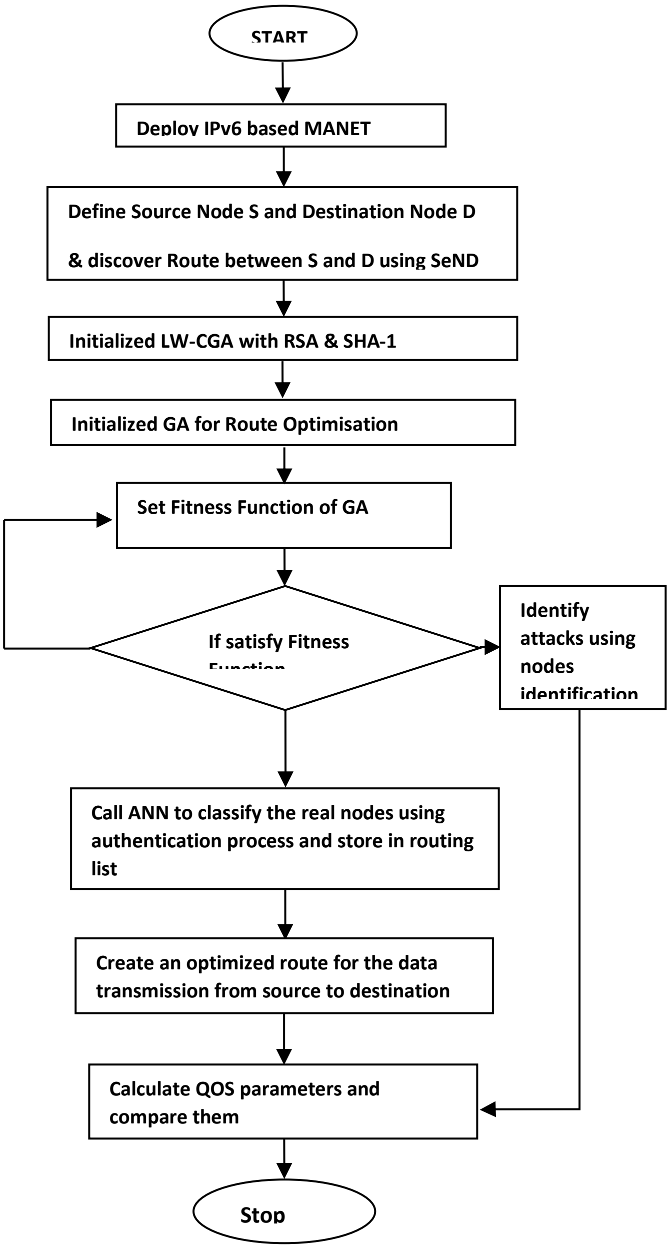
START
Deploy IPv6 based MANET
Define Source Node S and Destination Node D
& discover Route between S and D using SeND
Initialized LW-CGA with RSA & SHA-1
Initialized GA for Route Optimisation
Set Fitness Function of GA
If satisfy Fitness Function
Identify attacks using nodes identification
Call ANN to classify the real nodes using authentication process and store in routing list
Create an optimized route for the data transmission from source to destination
Calculate QOS parameters and compare them
Stop

Figure 3: Proposed Flowchart

III. SIMULATION & RESULTS

The simulation environment of the proposed work is shown in the table and the simulation results are described in the below section.

Table 1: Network Requirements

Number of nodes	**50-100**
Area	**1000-1000 meters**
Simulation Tool	**MATLAB**
Authentication Parameter	**Energy Consumption**
Evaluation Parameter	**Throughput , Error Rate, Energy, Delay**

To simulate the proposed work we need simulator and we design a simulator which is show on the below figure.

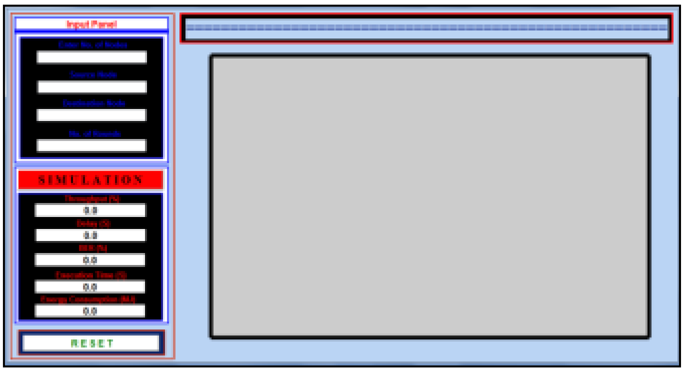

Figure** Error! No text of specified style in document.**: MANET Simulator

The above figure represents the simulator with height and width (1000×1000). In the figure, there are two sections first is "Input Panel" and second is the "Simulator part". In the "Input Panel" we provide the required input data to simulate the designed network and in "Simulator part" we check the performance parameters of proposed work.

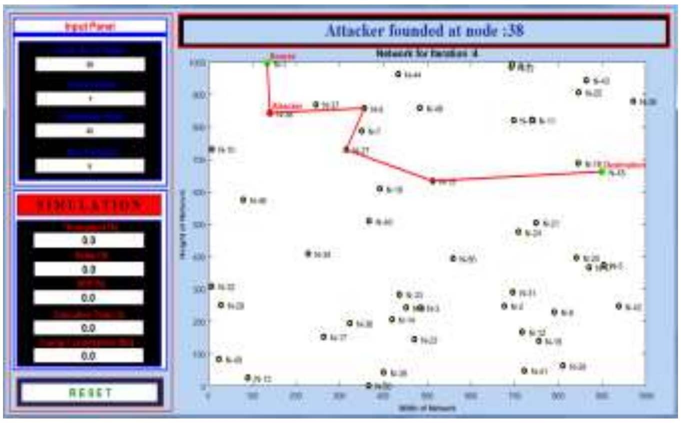

Figure 5: MANET Simulator with Input Data

Above figure represents the deployment of MANET within the network. In the above figure, we enter total 50 numbers of nodes with five iterations. We select a node as a source and as a destination and the 1 is act as a source node and 45 is act as a destination node. After that, define a coverage area to each nodes using above mentioned algorithm. When coverage area is defined then create a route from source node to destination node using the SeND routing protocols with Light Weight Cryptographic Address Generation.

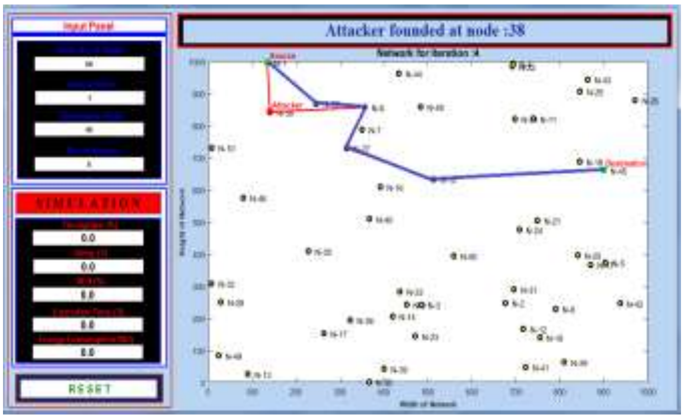

Figure 6: MANET Simulator with Attacks

Above figure represents the optimized route from source node to destination node using the concept of an artificial intelligence based Light Weight Cryptographic Address Generation (LW-CGA) using optimization for IPv6 based MANETs. Here genetic algorithm with artificial neural network is used as a classifier to classify the attacker nodes during the simulation. The QoS parameters of proposed work is given in the below section.

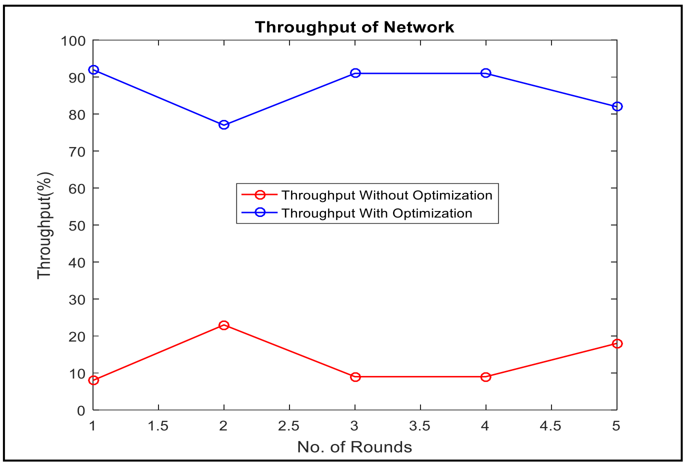

Figure 7: Throughput

Throughput means the number of packets that are transmitting by the source node to the destination nodes or we can say that it is the total number of packets delivered to the destination node within a total simulation time. As it is shown in figure above, the red color line indicates the throughput values obtained from the MANET without optimization i.e. no any algorithm is used to reach the packet at the destination node. Whereas the blue line indicates the throughput values obtained for the MANET with optimization i.e. GA and artificial neural network used to find the accurate path and the packet has to reach at their appropriate position. The process is repeated five times in order to obtained accurate results.

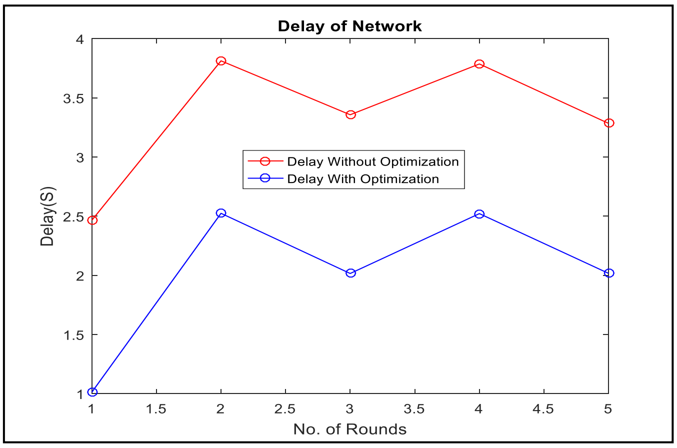

Figure 8: Delay

Delay is the average time a network takes to transmit data packet to reach the destination. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue. This metric is calculated by subtracting time at which first packet was transmitted by source from time at which first data packet arrived to destination. In the above figure, red line shows the delay occurred in case of without optimization and blue line is indicating delay with optimization. Therefore, it is clear from the graph that the delay value obtained for network with optimization when GA and ANN techniques are applied is less than the value obtained for without optimization which means that in without optimization data packets takes more time to reach at the destination than with optimization. The average value obtained for delay without optimization is 3.74 sec whereas with optimization delay of the MANET reduced and become equal to 2.08 sec.

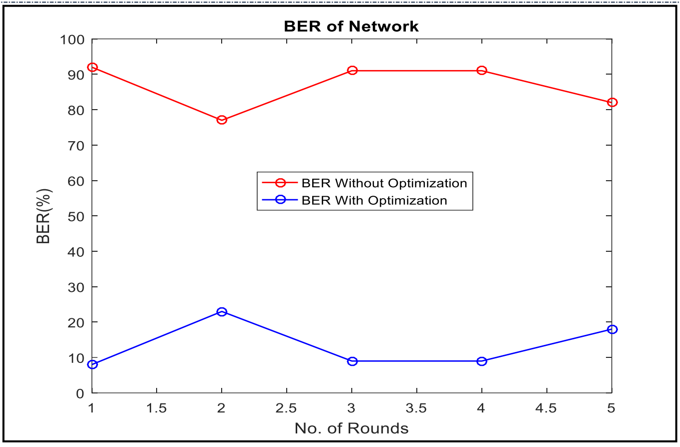

Figure 9: BER

Transmitted bits are correctly received at the sink node if and only if those data bits are received at each intermediate node between source and destination without error as shown in figure above. The total numbers of bit errors occurred in sending data bits from any source node to any destination node calculates the BER of the network. This means that the network must be connected in such a way that we can calculate BER of the network to know its performance. From the above figure, it is clear that the blue line is for the BER when GA and ANN are applied to the network whereas black line indicates the performance when GA and ANN are not applied. Thus, it is concluded that when GA and ANN are applied to the network with Light Weight Cryptographic Address Generation (LW-CGA) technique, Bit error rate is less as compared to the BER obtained for the network without GA and ANN. Therefore, the results obtained for the network using optimization are better than without optimization.

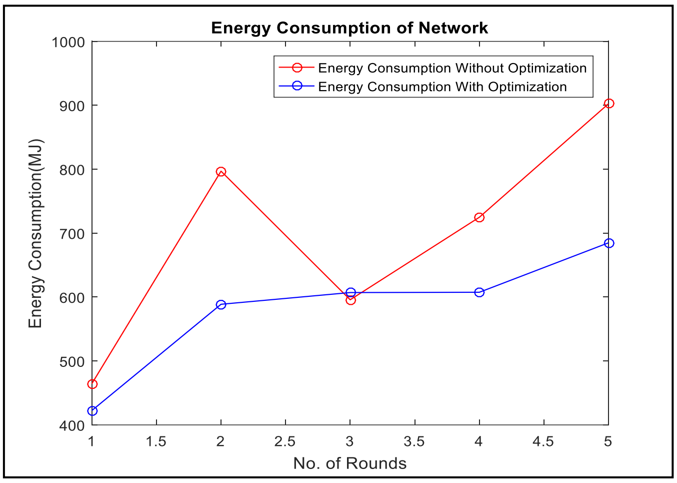

Figure** Error! No text of specified style in document.**-1 Energy Consumption

When data is transmitted from one node to the other node within the IPv6 based MANET, all the nodes consume some amount of energy. Thus it is necessary to find the optimal route that will consume less energy and the data has been transmitted to appropriate destination. For finding route SeND routing protocol with Light Weight Cryptographic Address Generation (LW-CGA) is used and for optimizing route GA is used along with the artificial neural network. It is concluded that more energy is consumed without GA and ANN algorithm than with GA and ANN algorithm being applied to the network. Without optimization, the maximum value of energy consumption is 900 milli joules whereas; with optimization the energy consumption reduced and become 683 milli joules which is less as compared to without optimization.

IV. CONCLUSION

Ad hoc network consists of individual devices for the communication purpose with each other. The concept of Ad hoc network is not that familiar to end users who have a typical router for sending the wireless signals. For deploying the network in Ad hoc network, configuration of network is considered on the behalf of some physical parameters. SeND routing protocol is prone to countless attacks similar to alteration in the sequence quantities or hop counts, source route channeling, spoofing in addition to construction in the error messages. For the improvement of energy range in the MANET, IPv6-enabled nodes are demanded to outline a multi-hop network with IPv6 data packets are transmitted by the central nodes on the route in the packet's target. To solve the routing protocol in IPv6 based MANET, the Secure Neighbor Discovery (SeND) routing protocol will be designed with concept of artificial intelligence techniques to overcome the security threats during auto-configuration has proven to face security and technical issues in MANETs. The SeND routing protocol uses RSA and SHA-1 (Secure Hash Algorithm) implementation for ensuring privacy enabled auto-configuration. In IPv6 based MANETs, the neighbor discovery enables nodes to self-configure and communicate with neighbor nodes through auto-configuration. The Stateless address auto-configuration (SLAAC) has proven to face several security issues during the data transmission form source node to destination node. Even though the SeND uses Cryptographically Generated Addresses (CGA) to address these issues, it creates other concerns such as need for Cryptographic Address (CA) to authenticate nodes, exposure to CPU exhaustion attacks and high computational intensity. In this work, we proposed empirically strong Light Weight Cryptographic Address Generation (LW-CGA) using entropy gathered from system states using artificial neural network techniques with route optimization. It has been concluded that the throughput rate when measured without attack is more than the attack occur in the IPv6 network. Also the energy consumed by network node is compared with attack and when ANN algorithm is applied to prevent the node. It is concluded that the average of Throughput, Delay, BER and Energy consumption when attack occur is 22, 3.74, 93 and 780 respectively. When GA and ANN algorithm is applied to the network the Throughput, Delay, BER and Energy consumption improved and it is 94, 2.08, 13 and 574 respectively. The energy consumption rate is reduced when GA and ANN is applied to prevent the network form the attacker nodes based on the Light Weight Cryptographic Address Generation (LW-CGA).

In future, to increase the efficiency of the proposed work we can use combination of any two optimization algorithm such as Genetic algorithm along with artificial bee colony algorithm based on the hybrid cryptography techniques.

REFERENCES

[1] Reshmi, T. R., and K. Murugan. "Light weight cryptographic address generation (LW-CGA) using system state entropy gathering for IPv6 based MANETs." China Communications 14.9 (2017): 114-126.

[2] JeeHyeon Na, Yun Won Chung, Jaewook Shin, Sangho Lee, Sang-Ha Kim, "A Novel Routing Path Discovery and Data Delivery Scheme for Ubiquitous Internet Connectivity Based on Hierarchical Mobile AODV6 Networks", *Vehicular Technology Conference 2007. VTC2007-Spring. IEEE 65th*, pp. 61-65, 2007, ISSN 1550-2252.

[3] Nadeem, A., & Howarth, M. P. (2013). A survey of MANET intrusion detection & prevention approaches for network layer attacks. *IEEE communications surveys & tutorials*, *15*(4), 2027-2045.

[4] Kavitha, P., Keerthana, C., Niroja, V., & Vivekanandhan, V. (2014). Mobile-id Based Sybil Attack detection on the Mobile ADHOC Network. *International Journal of Communication and Computer Technologies*, *2*(02).

[5] Sun, Y., Han, Z., & Liu, K. R. (2008). Defense of trust management vulnerabilities in distributed networks. *IEEE Communications Magazine*, *46*(2), 112-119.

[6] Vasudeva, A., & Sood, M. (2012). Sybil attack on lowest id clustering algorithm in the mobile ad hoc network. *International Journal of Network Security & Its Applications*, *4*(5), 135.

[7] D. Sivakumar, B. Suseela and R. Varadharajan, "A survey of routing algorithms for MANET", *IEEE-International Conference on Advances in Engineering, Science and Management (ICAESM -2012)*, Nagapattinam, Tamil Nadu, 2012, pp. 625-640.

[8] Macker, J. (1999). Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations.

[9] Garg, N., & Mahapatra, R. P. (2009). Manet security issues. *IJCSNS*, *9*(8), 241.

[10] Douceur, J. R. (2002, March). The sybil attack. In *International Workshop on Peer-to-Peer Systems* (pp. 251-260). Springer, Berlin, Heidelberg.

[11] Piro, C., Shields, C., & Levine, B. N. (2006, August). Detecting the sybil attack in mobile ad hoc networks. In *Securecomm and Workshops, 2006* (pp. 1-11). IEEE.

[12] Abolhasan, M., Wysocki, T., & Dutkiewicz, E. (2004). A review of routing protocols for mobile ad hoc networks. *Ad hoc networks*, *2*(1), 1-22.

[13] Marwaha, S., Tham, C. K., & Srinivasan, D. (2002, November). Mobile agents based routing protocol for mobile ad hoc networks. In *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE* (Vol. 1, pp. 163-167). IEEE.

[14] Alba, E., Dorronsoro, B., Luna, F., Nebro, A. J., Bouvry, P., & Hogie, L. (2007). A cellular multi-objective genetic algorithm for optimal broadcasting strategy in metropolitan MANETs. *Computer Communications*, *30*(4), 685-697.

[15] Kaaniche, H., & Kamoun, F. (2010). Mobility prediction in wireless ad hoc networks using neural networks. *arXiv preprint arXiv:1004.4610*.

[16] Ahmed Sherif, Maha Elsabrouty, Amin Shoukry,"A Novel Taxonomy of Black-Hole Attack Detection Techniques in Mobile Ad-hoc Network (MANET)", IEEE, pp: 346-352, 2013

[17] Bikramjeet Singh, Dasrari.S,C.R. Skitishn kumar,"Mitigating effects of Black hole Attack in Mobile Ad-hoc Networks: Military Perspective", 2nd IEEE International Conference on Engineering and Technology (ICETECH), 17th & 18th March 2016, Coimbatore, TN, India.

[18] 7. Paul, A., Sinha, S., & Pal, S. (2013, December). An efficient method to detect sybil attack using trust based model. In *Proc. of Int. Conf. on Advances in Computer Science, AETACS, Elsevier*.

[19] Pooja ,Dr.R.K.Chuhan, "An Assessment Based Approach To Detect Black Hole Attack In MANET", International Conference on Computing, Communication and Automation (ICCCA2015) ,IEEE2015.

[20] . Abbas, S., Merabti, M., Llewellyn-Jones, D., & Kifayat, K. (2013). Lightweight sybil attack detection in manets. *IEEE systems journal*, *7*(2), 236-248.

[21] Vimal Kumar a , Rakesh Kumar , " An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network",ELSEVIER , nternational Conference on Intelligent Computing, Communication & Convergence (ICCC-2014).

[22] Yibeltal Fantahun Alem,Y.C.Xeun , "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2010 IEEE.

[23] Siddharth Dhama, Sandeep Sharma, Mukul Saini, "Black Hole Attack Detection and Prevention Mechanism for Mobile Ad-Hoc Networks", 978-9-3805-4421-2/16/$31.00_c 2016 IEEE

[24] Z. Li and Y. Wu, "Smooth Mobility and Link Reliability-Based Optimized Link State Routing Scheme for MANETs," in *IEEE Communications Letters*, vol. 21, no. 7, pp. 1529-1532, July 2017.

[25] Y. Fang, Y. Zhou, X. Jiang and Y. Zhang, "Practical Performance of MANETs Under Limited Buffer and Packet Lifetime," in *IEEE Systems Journal*, vol. 11, no. 2, pp. 995-1005, June 2017..

CITE AN ARTICLE

Pal, R. K., & Gupta, D., Dr. (2018). AN ARTIFICIAL INTELLIGENCE BASED LIGHT WEIGHT CRYPTOGRAPHIC ADDRESS GENERATION (LW-CGA) USING OPTIMIZATION FOR IPv6 BASED MANETs. *INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY*, *7*(8), 251-261.