International Journal of Applied Engineering Research ISSN 0973-4562 Volume 15, Number 4 (2020) pp. 328-335
© Research India Publications. http://www.ripublication.com

Power Optimized Stochastic VANET Routing Protocol for Urban Scenarios

Malini[1], Bhuvaneswari[2],

[1]*Department of Computer Science, National Engineering College, Tuticorin, 628502, India.*

[2]*Department of Computer Science, National Engineering College, Tuticorin, 628502, India.*

Abstract

The Vehicular Ad Hoc Network (VANET) is a self-organized communication network where the vehicles act as the mobile nodes, and continuously transmits the data packets between them. Because of the continuous and rapid changing in the topology patterns and the availability of lesser resources, the offering of the power-based routing protocol is a more challenging task. This work introduces a power-based routing protocol considering a prominent model. The algorithm which is used to find the secured path is, the combination of the Grasshopper Optimization Algorithm along with the Krill herd optimization algorithm (GK). Here the prominent model and the power is created for providing a secured path between the source node and the destination node along with the optimization algorithm. The prominent model here comprises of prominent parameters which include node mobility, node capability, node history, and prominence among the neighboring nodes. The prominent parameters had applied to every node in the network. The proposed GK based secured routing contains functions like prominence, power, delay, and distance. The resultant analysis of the given proposed algorithm includes a reliable data transmission notification and are applied to two urban based scenarios and their throughput, delay, power consumed and efficiency was compared.

Keywords: mobility,delay,throughput,power,routing

I. INTRODUCTION

VANETs are self-administered wireless system, which is responsible for creating a self-directed mobile application structure, in which each mobile node can send data starting with one node then onto the next node utilizing wireless interfaces without relying upon other administrations [1]. The VANET hasn't relied upon fixed infrastructures and administrator. The restricted resources are procured by the wireless sensor framework, which includes computational memory, battery abilities, transmission capacity, and memory [2].

VANETs start a protected communication between the nodes, and these nodes move in the range and the direction where it gets the receiving signals which hold the transmitting packets and generates the arbitrary reactions — the attacks in routing lead to the degradation of the protocol. The topologies of the system were changed continuously due to the mobility of nodes [8]. Likewise, power failures lead to more disappointments in VANET topologies [4]. Moreover, the changing topologies caused by the mobility of the nodes impacts the power expended for transmitting the information. Therefore, routing procedures, which contains the parameters like node's mobility, varying topologies and power limitations, are required in VANETs. Besides, the routing conventions must be successful in power utilization and Quality of Service (QoS) for guarantying the transmission of information through the wireless medium.

The attacks happened in the VANET includes routing-based attacks and the security-based attacks in the network. The attacks are of internal and external categories. The external attacks are passive attacks and active attacks. In the passive aggression, the messages transmitted between the two points have not modified while in the active attacks, there might be a severe behavioral change in data transmission [20]. The internal attacks have connected to the interfaces that link the nodes within the network. Generally, the routing algorithms in VANET have compromised by some factors like dynamic topology, power consumption, delay overhead, and neighboring nodes information. The trusted mobile nodes play a vital role in providing a safe route formation by analyzing the multi-hop communication among the mobile nodes.

The reliability capacity of the nodes mainly does this route formation. The cryptography-based security addressing takes a lot of time, and it allows the attackers to gain the users information with the help of powerful computers. The trust management have expertly managed, and the trust value is assigned for each of the mobile nodes dynamically. The critical factor has introduced in the calculation of trust in nodes behavior individually [4]. The introduction of trust management concepts in VANETs can increase security and power optimization in wireless mode communication. The traditional security measures such as firewall, cryptographic techniques provide less protection in VANET communication.

The mobility of the nodes in VANETs creates a high intercommunication challenge. The frequent disconnection of networks results in frequent path disruptions. The time-varying vehicle density results in a rapid change in topology, which makes preserving a route a problematic task. Another challenge includes the hidden terminal problem which results on performance degradation in VANETs, causing a low packet reception rate. Interference from the high-rise building induces issues such as routing loops and forwarding in the wrong path, which subtle delay.

In VANETs the routing protocols should be able to establish dynamic route and also maintains them during the data transmission. Whenever the path was about to disconnect, the alternate path must be found out in a quick manner. Real-time applications demand less delay during data transmission. To avoid congestion in network multiple routes within a network are required. The critical challenge is to design routing protocols to overcome these problems and to provide communication with minimum delay and with minimum overhead [24]. VANETs allow vehicles to form a self-organizing and self-managing network in a distributed fashion without a centralized authority or a server dictating the communication. It was evident that the success of VANE applications dramatically depends on the routing algorithms applied. Better paradigms have required for information dissemination within the estimated time by designing efficient routing algorithms. Some of the routing algorithms discussed in this literature are Ad hoc On-demand Distance Vector (AODV) [9], Link-State Multicast Routing, and OLSR [12]. The fuzzy based models [25] which uses a centroid-based communication is also tested but it results in membership functions.

This paper comprises a scheme based on the prominence factors and power to enable an optimized path in VANET. This includes the technique called GK optimization algorithm, which reduces the complexity of finding the optimal path between the source and the destination. The prominent factors include attributes like power, distance, delay, and prominence. These attributes create a fitness function and have found out as a high valued function. Thus, the proposed scheme increases network performance and also its lifetime. The procedures in the GK are: Finding all the possible paths between the source and the destination and evaluate the best optimal path among the possible paths using the prominent factors. Hence, the crisp detection rate, delay, power, and the throughput were calculated by the proposed GK for sending the data between the source and the destination.

The essential conclusions in the routing scheme derived are as follows,

1) The creation of GK, which is the combination of Krill Herd optimization algorithm and the Grasshopper optimization algorithm used for initiating safe routing in VANET by including security and power.

2) By using the multi-objective model such as power, delay, prominence, and distance, the best optimal route for transmitting data found out from the k-possible paths.

II. PROPOSED GK FOR SECURED VANET ROUTING

A. Topology Description

This section describes the three main steps followed in the GK algorithm, namely path discovery, implement the optimization algorithm, and conclude with the optimal path among the discovered paths. In the initial step, from the source to the destination, what are all the possible paths laid are found. Later, the GK algorithm was applied, and the optimal routes were located. Finally, the information was transferred in the form of data between the source and the destination in the optimal path. The routing among the two points was carried out by the parameters like power, distance, prominent factors, and delay parameters, and a secured environment was created between the two data transmitting nodes. Here a fitness value was calculated in order to comply with factors like maximum prominent factors, reduction of delay, power, the distance between the source, and the destination. For the satisfaction of the above-mentioned values, the fitness value must be high. The main goal of this concluded algorithm was to find the most optimal path between two points i.e., the source and the destination, by setting a maximum fitness value for the selected routing path.

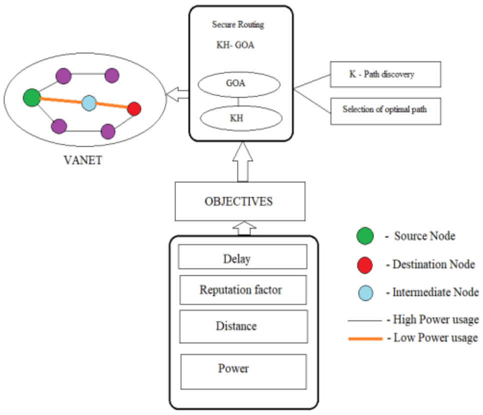

Figure 1. Process of GK Routing Protocol

B. Representation of Solution

The solution was represented for determining the optimal solutions from the given set of possible paths. A tiny encoding process was done to select the optimal path and denote it in the binary module. For a wireless sensor network with a number of routes n, the given GK selects an optimal route, where $1\leq f \leq n$ for data transmission by the fitness value function.

C. Fitness Evaluation

The fitness value calculation is a function used to find the optimised path by evaluating each node's regular factors, namely power, delay, distance and prominence. The fitness value calculated for the concluded GK must be high. The fitness function was given by,

$$\text{Fitness} = \sum_{i=1}^{|a|} F_i \qquad (1)$$

Where, i denote intermediate nodes between the selected routes, $a$denote total nodes and F_i denotes the various factors of each selected nodes.
The various node factors are represented as,

$$F_i = \frac{1}{4} * [X^a + [1 - P^a] + [1 - C^a] + [1 - D^a]] \qquad (2)$$

Where, X^a denotes the prominent factor of a^{th}node, P^arepresents the power consumed by the a^{th}node,C^a

expresses the distance between the a^{th}node and previous node, and D^{a} represents the delay of a^{th}node.

Prominent Factor

The prominent factor deals with selecting the optimal path by rejecting the malicious node. These factors generally progress this statement while doing the discovery of routes between the source and the destination. It also follows up the selection process of the data nodes. The prominent value depends upon the sub actors like, capability of the node, history of the nodes previous movements, mobility factor, and relationship with the neighboring nodes.

$$X_a^w = \frac{1}{4}[E_a^w + [1 - M_a^w] + A_a^w + L_a^w] \tag{3}$$

Where, w denotes the present time, E_a^w denotes the history of the node a in time w, M_a^w denotes the mobility of node a at w, A_a^w denotes the actual capability of a at w, L_a^w denotes relationship of the node a with the neighbors at time t.

History of node

The detailed input is analysed and taken from the nodes precious records for a secured data transmission.

$$E_a^w = [X_a^{w-1} + \frac{1}{2} \times X_a^{w-2}] \times \frac{1}{2} \tag{4}$$

Where, X_a^{w-1} denotes the prominence value at the time w-1, andX_a^{w-2} denotes prominence value at the time w-2.

Capability of Node

The capability of the node is defined as the ratio of number of bytes sent to the total capacity of the node.

$$A_{a_{max}}^w = [\frac{T_s}{V}] \tag{5}$$

Where, T_s denotes the number of bytes, and V denotes the total capacity.

Mobility of Node

In the network the nodes can either move in a fixed path or in a random manner. The mobility of the nodes in VANET has their own functions and move accordingly. Thus, their value is kept as an arbitrary one. The nodes mobility can affect its performance. When the mobility is high, then the performance is too good and in the opposite case results in a good relationship with the neighboring nodes in a network.

$$M_a^w = \frac{Distance(Q_a^{w-1}, Q_a^w)}{\propto} \tag{6}$$

Where, $Distance(Q_a^{w-1}, Q_a^w)$ denotes the distance between the node a between the interval w-1 and w-2 and $\propto$ denotes the normalization factor.

Prominence among Neighborhood

The total number of neighbouring nodes located near the source node is defined as the prominence among neighbourhood.

$$L_a^w = \frac{1}{|F|}\sum_{j=1}^{|F|} F_{j,a} \tag{7}$$

Where, |F| denotes the total neighbors present near the node and j denotes the neighbor node.

D. Power

The battery power consumed by the node is used for the data transmission and was calculated using the equation (1).

E. Distance

The distance between the node a and a-1 which is divided by the normalization factor is defined as the distance.

$$C^a = \frac{Distance(a, a-1)}{\propto} \tag{8}$$

F. Delay

The delay is defined as the ratio of total nodes in the route to the total number of nodes in the network. The value of delay must be less for the effective data transmission.

$$C^a = \frac{e}{q} \tag{9}$$

Where, e denotes total nodes in a particular route and q denotes total nodes.

III. PROPOSED GK ALGORITHM

The resultant of the Krill Herd (KH) algorithm [21] and Grasshopper Optimization Algorithm (GOA) [22] creates the GK algorithm, which is meant to validate the optimal path between the two selected nodes for data transmission. In the KH algorithm, the behavior of the krill is finely tuned based on the time parameter. The krill moved in the groups are divided based on the minimum distance between the krill and the food source and an objective function with the high-density krill groups. The fundamental steps involved in the KH algorithm are Induced Motion, Foraging Motion, and Random Diffusion. The KH algorithm was initially tested for dealing with optimization problems. Meanwhile, the other half includes the GOA method, which mainly dealt with changing the comfort zone area for maintaining the exploration and exploitation process of the nodes using the comfort zone parameters. The GOA is likely to deal with global optima rather than a local medium. The update function of the KH algorithm was applied to the GOA algorithm for presenting an optimal solution with a multi-objective function. Thus, the GK is meant to provide a more efficient path between the source and the destination and thus improve their performance in data transmission. The concluded prominent model includes parameters like the mobility of the node, node capability, history of the nodes traveling path, and prominence among the neighboring nodes. The process includes in GK algorithm are discussed in the given steps.

A. Initialization:

Initially, the parameters and the solution set for the algorithm was well defined. In the initial phase, the solution set R containing l solutions was created in a random manner from which one solution was selected. Each solution in Set R is represented as,

$$R = \{R_1, R_2, \ldots., R_m, \ldots. R_n\} \quad (11)$$

Where, n denotes the size of the total population.

B. Fitness Evaluation

The best solution was computed using the fitness function value. This function was evaluated using the node parameters like power, distance, delay, and prominent factor. The evaluation is done for each individual solution using the equation (2) to find out the best optimal solution until the last iteration of the evaluation.

C. Updating of positions and evaluation

Considering the iterations, both the best and the worst solutions are created. Here the total solutions obtained are l. The updating of the solution considers only the parameter generally the parameter position, which takes it to the best optimal solution and gradually discards the worst optimal solution Based on the KH algorithm, the position vector of krill in particular interval s and Δs is formulated as follows,

$$R_m(s + \Delta s) = R_m(s) + \Delta s \frac{dR_m}{dk} \quad (12)$$

Where, $R_m(s)$ denotes the m^{th}solution during s^{th} interval. The Δs is a scaling parameter used as a speed factor. The equation (4) can be rearranged as,

$$R_m(s) = R_m(s + \Delta s) - \Delta s \frac{dR_m}{dk} \quad (13)$$

Based on GOA algorithm, the next location of the node was found out using the current location, target location and location of the grasshopper. The first part of the given equation deals with the current grasshopper position with respect to the neighboring grasshoppers. The status of grasshoppers implies the location of search agents around the target. The update equation is given by,

$$R_m^r(s + \Delta s) = g(\sum_{\substack{n=1 \\ n \neq m}}^{l} g \frac{U_r - Y_r}{2} t(|R_n^r - R_m^r|) \frac{R_n - R_m}{h_{mn}} \quad (14)$$

Where r denotes the dimension of the search space, g denotes the reducing coefficient, n denoted the total number of grasshoppers in r dimension and n, m denote the location of the grasshoppers in r dimension, $U_r$and Y_r denotes the upper and the lower bound in r dimension, t represents the social forces strength, $h_{m,n}$ represents the distance between two grasshoppers in dimension r, $\hat{p}_r^*$ represents the best solution obtained so far. Assuming l =1 and substituting (5) in (6)

$$R_m^r(s + \Delta s) = g^2 \frac{U_r - Y_r}{2} t(|R_1^r(s) - R_m^r(s)|) * \frac{R(s) - R_m(s + \Delta s)\frac{dR_m}{ds}}{h_{m1}} + \hat{p}_r^* \quad (15)$$

$$R_m^r(s + \Delta s)\left[1 + g^2 \frac{U_r - Y_r}{2} t(|R_1^r(s) - R_m^r(s)|)\right] = g^2 \frac{U_r - Y_r}{2h_{ml}} g(|R_1^r(s) - R_m^r(s)|) + \left[(R_1(s) + \Delta s)\frac{dR_m}{dk}\right] + \hat{p}_r^* \quad (16)$$

The final expression for proposed GK for finding the optimal path is given by,

$$R_m^r(s + \Delta s) = \frac{2h_{ml}}{2h_{ml} + g^2 U_r - Y_r\, t\left(\left|R_1^r(s) - R_m^r(s)\right|\right)} * \{g^2 \frac{U_r - Y_r}{2h_{ml}} g(|R_1^r(s) - R_m^r(s)|) + \left[(R_1(s) + \Delta s)\frac{dR_m}{dk}\right] + \hat{p}_r^*\} \quad (17)$$

D. Replace with best solution

After the position was updated, the fitness of each solution was calculated and the solution with the maximum fitness value was selected as a best solution.

E. Termination

The progress was done till the best solution was calculated and the algorithm was halt in two cases like till it reaches the K_{max} iteration or no such best solution was obtained. When the optimal path was found, the data transmission was start through that path and a notification was sent to the sender via the same path of successful data transmission.

The pseudo code for the proposed GK algorithm is discussed below,

F. GK Algorithm

```
Input: Population R
Output: Optimal solution $\hat{p}_r^*$
Start
    Set the population
    Update $U_r, Y_r, g, t$ and $h$
    while (k <$k_{max}$ )
    for each solution in R
    Find the fitness using equation (6)
    Update location using equation (17)
    Create new solution set
    Find the fitness for the new solutions
    Select the maximum fitness solution $\hat{p}_r^*$
    Increment k
    end while
return $\hat{p}_r^*$
Send notification to sender
Stop
```

IV. RESULTS AND DISCUSSION

The performance of the proposed GK routing algorithm is evaluated for two scenarios namely, NH based network (National Highway) and Urban based network. Here the throughput, delay and the power consumption of the mobile nodes with and without attack of malicious nodes in the path between the source and the destination was compared. All the three parameters have high values for the NH based scenario than the urban based scenario.

A. Experimental Setup

The proposed algorithm has experimented using the NS2 simulator using metrics like throughput, delay, and energy efficiency whereas, the input was obtained from SUMO (Simulation of Urban MObility) simulator and executed in the Windows 10 OS, 4 GB RAM, and Intel CPU 2.16 GHz processor.

B. Performance Validation

The three main parameters used for computing the algorithm in two different scenarios are power, delay, and energy [23].

Power: The total energy consumed by the nodes in the network. It has found out using equation (1).

Throughput: The ratio of the total number of data packets received per unit time between the two points of the network.

$$\text{Throughput} = \frac{a}{k}$$

Where, a is the total number of packets received per simulation time k.

Delay: The time in which the response has sent for a particular request over the network.

The Table 1 and Table 2 describes about the total nodes used in both scenarios, energy fixed per node in the network and other resultant values obtained from the application of the GK algorithm.

TABLE I. THE CITY-BASED NETWORK DETAILS

Total nodes	**40**
Energy per node	100J
Total Energy in network	4000J
Protocol	TCP
Generated Packets	3177
Received Packets	3062
Consumed Energy (%)	36.57%
Remaining Energy (%)	63.43%
Packet delivery Ratio (%)	96.39%
Average End-End delay	0.0513627

TABLE 2. THE NH-BASED NETWORK DETAILS

Total nodes	**20**
Energy per node	100J
Total Energy in network	2000J
Protocol	TCP
Generated Packets	4992
Received Packets	4943
Consumed Energy (%)	23.41%
Remaining Energy (%)	76.59%
Packet delivery Ratio (%)	99.02%
Average End-End delay	0.239705

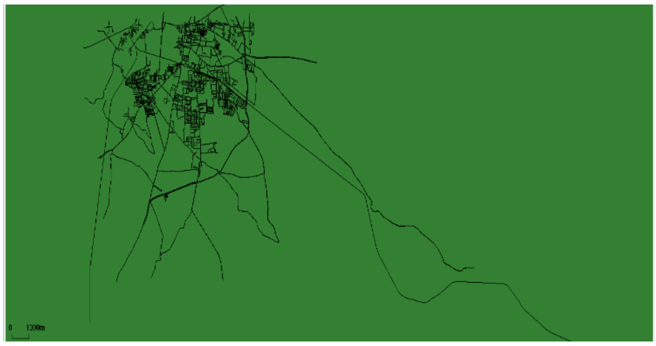

Figure 2. NH Based Area – SUMO

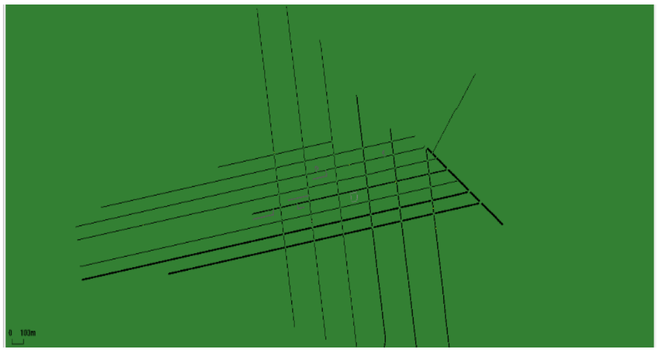

Figure 3. Urban Based Area – SUMO

Here the Figure 2 and Figure 3 shows the simulation result of the SUMO software for the National Highway-based network and Urban-based network respectively. The database for importing the network was Open Street Map (OSM). The mobile nodes can be set according to the scenarios and have their fixed Round trip Time (RTT).

The Figure 4 describes the data transmission in NH-based network between the source and destination nodes in a selected path where the fitness value was high. Here the source and destination are fixed for reliability checking where the node 2 act as a source and the node 11 act as a destination. The data transmission for the Urban-based network was described in the Figure 5. In the Urban scenario, the node 2 act as a source and the node 14 act as a destination and the data was transmitted in the reliable path.

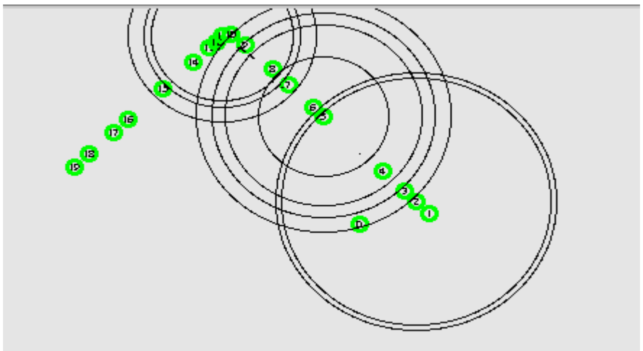

Figure 4. Data transmission in NH scenario

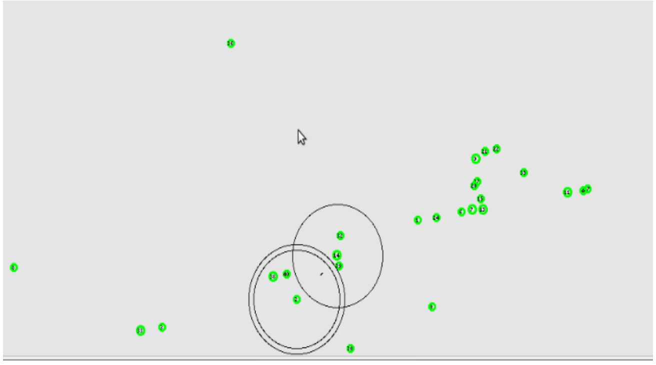

Figure 5. Data transmission in Urban scenario

By obtaining the results for the various prominence parameters, the graphs are generated for evaluating the performance of the algorithm in both NH-based network and the Urban-based network. The Power consumption, Delay, throughput and the Detection rate was showed in the Figure 6, Figure 7, Figure 8 and Figure 9 respectively. The energy conserved per node in both the NH and the Urban networks are compared as a residual graph as shown in Figure 10.

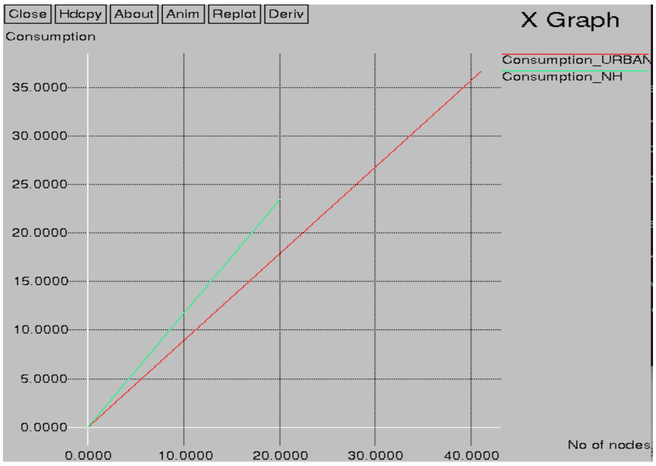

Figure 7. Power consumption in NH and Urban networks

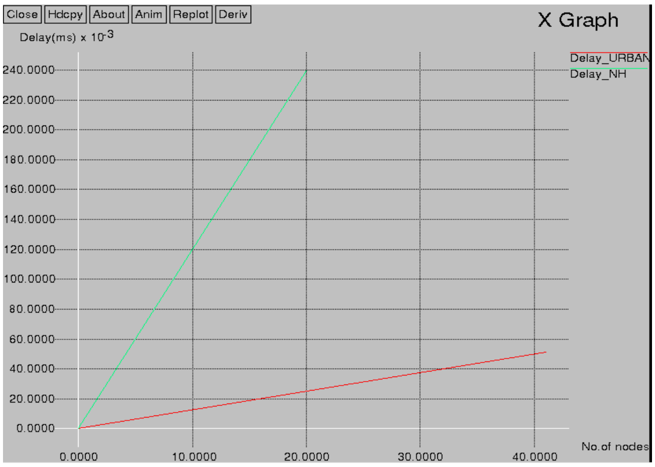

Figure 8. Delay of data transmission in Nh and Urban networks.

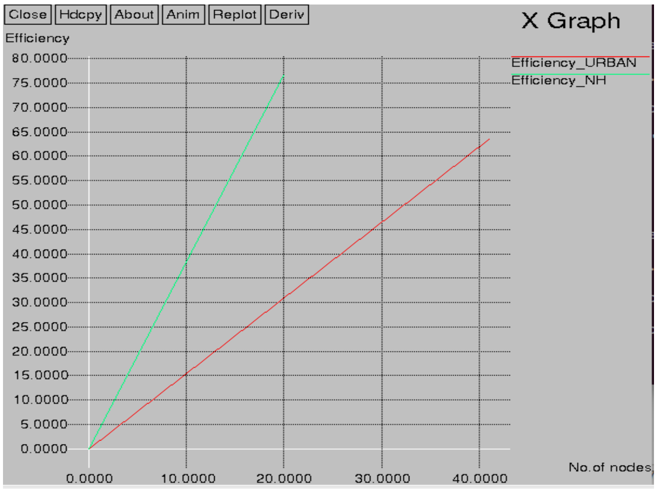

Figure 8. Throughput result for NH and Urban based networks

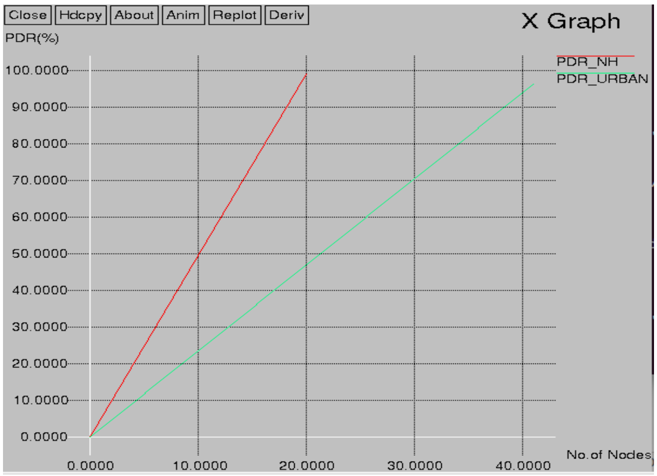

Figure 9. Packet delivery ratio for NH and Urban based networks

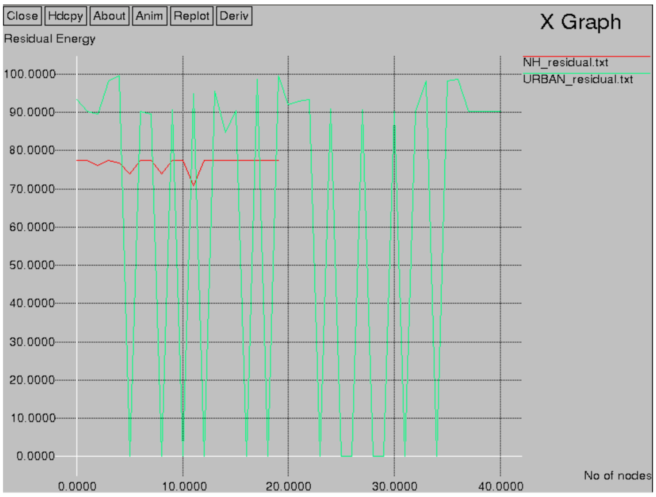

Figure 10. Energy conservation of each node per 100J.

V. CONCLUSION

In this paper, a secured algorithm named GK has proposed to enhance a protocol for finding a reliable data transmission between two nodes by finding an optimal path. Here the combination of KH and GOA is done to select an optimized path between the source and the destination using various parameters like power, delay, distance, and prominent factors. Finally, the scenario where the delay and distance had reduced, and throughput was high was compared. Here the prominence is a parameter used to provide a secured routing protocol between the nodes for data transmission. The prominent factors include the mobility of the nodes, history of the node movements, capability of the node, and the prominence among the neighboring nodes. The result has analyzed in the Ns2 simulator.

ACKNOWLEDGMENTS

THE CAPES-Coordination for the Improvement of Higher Education Personnel and www.normatizaoficial.com

REFERENCES

[1] Zhang, M., Yang, M., Wu, Q., Zheng, R. and Zhu, J., “Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs,” Future Generation Computer Systems, 2017

[2] ChrispenMafirabadza and Pallavi Khatri, “Efficient Power Aware AODV Routing Protocol for MANET,” Wireless Personal Communications, vol. 97, no. 4, pp. 5707-5717, 2017.

[3] Md. Mahbubur Rahman and Md. Akhtaruzzaman, “An Efficient Position based Power Aware Routing Algorithm in Mobile Ad-hoc Networks,” International Journal of Computer Network and Information Security, vol. 7, pp. 43-49, 2016.

[4] Vanitha, K. and Rahaman, A.Z., “Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol,” Cluster Computing, pp.1-9, vol.12, March 2018.

[5] Almazyad, A.S., “Reputation-based mechanisms to avoid misbehaving nodes in ad hoc and wireless sensor networks,” Neural Computing and Applications, vol.29, pp.597-607, May 2018.

[6] Menaka, R., V. Ranganathan, and B. Sowmya, “Improving Performance Through Reputation Based Routing Protocol for Manet,” Wireless Personal Communications, Vol. 94, No. 4, pp. 2275–2290, 2017.

[7] Ravi, G., and K. R. Kashwan, “A new routing protocol for energy efficient mobile applications for ad hoc networks,” Computers & Electrical Engineering, Vol.48, pp. 77-85, 2015.

[8] Navin Mani Upadhyay, KumariSoni, and Arvind Kumar, "Power Aware Routing in Mobile Ad Hoc Networks by using Power Aware Matrices," International Journal of Computer Applications, vol. 166, no. 11, pp. 24-29, 2017.

[9] Kumari, S.V. and Paramasivan, B., “Defense against Sybil attacks and authentication for anonymous location-based routing in MANET,” Wireless Networks, vol. 23, no. 3, pp.715-726, 2017.

[10] Basurra, Shadi S., Marina De Vos, Julian Padget, YushengJi, Tim Lewis, and Simon Armour, “Energy efficient zone-based routing protocol for MANETs,” Ad Hoc Networks, Vol. 25, pp.16-37, 2015.

[11] S. Sharma, “A secure reputation-based architecture for MANET routing,” in proceedings of 4th International Conference on Electronics and Communication Systems (ICECS), Coimbatore, vol. 13, pp. 106-110, 2017.

[12] 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.

[13] Sathish, S., Ayyasamy, A. and Archana, M., “An Intelligent Beta Reputation and Dynamic Trust Model for Secure Communication in Wireless Networks,” In Industry Interactive Innovations in Science, Engineering and Technology, Springer, vol.11, pp. 395-402, July 2018.

[14] Safa, Haidar, Marcel Karam, and BassamMoussa, “PHAODV: Power aware heterogeneous routing protocol for MANETs,” Journal of Network and Computer Applications, Vol. 46, pp. 60-71, 2014.

[15] Smail, Omar, Bernard Cousin, RachidaMekki, and ZoulikhaMekkakia, “A multipath energy-conserving routing protocol for wireless ad hoc networks lifetime improvement,” EURASIP Journal on Wireless Communications and Networking, Vol. 139, No.1, pp. 1-12, 2014.

[16] Shiny, XS Asha, and R. Jagadeesh Kannan, “Energy Efficient Clustering Protocol using Self Organizing Map in MANET,” Indian Journal of Science and Technology,

Vol. 8, No. 28, pp. 1-8, 2015.

[17] Xie, Ling Fu, Peter Han Joo Chong, and Yong Liang Guan, “Routing strategy in disconnected mobile ad hoc networks with group mobility,” EURASIP Journal on Wireless Communications and Networking, Vol. 105, pp. 1024-1032, 2013.

[18] Raju, R, Amudhavel, J, Pavithra, M, Anuja, S, Abinaya, B, “A heuristic fault tolerant MapReduce framework for minimizing makespan in Hybrid Cloud Environment”, International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE), vol. 14, no. 43, pp.1,4, 6-8 March 2014

[19] Raju, R, Amudhavel, J, Kannan, N, Monisha, M, “A bio inspired Energy-Aware Multi objective Chiropteran Algorithm (EAMOCA) for hybrid cloud computing environment”, International Conference on Green Computing Communication and Electrical Engineering (ICGCCEE),vol.11,no.54,pp.1,5,doi:10.1109/ICGCCEE.2014.692246, 2014.

[20] S. Venkatesan, P. Dhavachelvan, C. Chellapan “Performance analysis of mobile agent failure recovery in e-service applications”, International Conference on Circuit, Power and Computing Technologies [ICCPCT] International Journal of Computer Standards and Interfaces, Elsevier, Vol-32, No.1-2, pp. 38 43. ISSN:0920-5489, 2015.

[21] Gandomi, A.H. and Alavi, A.H., "Krill herd: a new bio-inspired optimization algorithm," Communications in Nonlinear Science and Numerical Simulation, vol.17, no.12, pp.4831-4845, 2012.

[22] Saremi, S., Mirjalili, S. and Lewis, A., "Grasshopper optimisation algorithm: theory and application," Advances in Engineering Software, vol.105, pp.3047, 2017.

[23] Gouda, Bhabani Sankar, Ashish Kumar Dass, and K. Lakshmi Narayana. "A comprehensive performance analysis of energy efficient routing protocols in different traffic based mobile ad-hoc networks." Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), 2013 International Multi-Conference on. IEEE, 2013

[24] Suresh, HosahalliNarayanagowda, GollaVaraprasad, and Guruswamy Jayanthi. "Designing Energy Routing Protocol with Power Consumption Optimization in MANET." Emerging Topics in Computing, IEEE Transactions on 2.2 (2014): 192-197.

[25] Menaka, R., V. Ranganathan, and B. Sowmya, "Improving Performance Through Reputation Based Routing Protocol for Manet," Wireless Personal Communications, Vol. 94, No. 4, pp. 2275–2290, 2017.