Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

PERFORMANCE OPTIMIZATION OF WIRELESS ADHOC NETWORKS WITH AUTHENTICATION

Dr. S. Smys
Professor, CSE, RVS Technical Campus,
Coimbatore, India
Email id: smys375@gmail.com

Dr. Jennifer S. Raj
Professor, ECE, Gnanamani college of Technology
Namakkal, India.
Email id: jennifer.raj@gmail.com

Abstract: Adhoc networks as the name suggests is framed for a specialized reason using the volunteering devices available near the source to destination, utilizing the devices in between the source and the destination as the relaying nodes. Several methods were framed to optimize the performance of the wireless adhoc network to retain the energy level of the devices in turn to extend the lifetime of the devices. The cluster based routing seemed to be very promising in terms of energy efficiency, throughput and delay. These cluster based adhoc networks are very much exposed to security breaches as they are not aided with sufficient security. The conveyance taking place between the head of the cluster to base station is often affected by the many attacks from different sources by altering the information or hacking the information. So the paper puts forward the verification code for every data transmitted from the head of the cluster to the base station. The proposed method is validated using the network simulator-2 in the terms of throughput, energy consumption and security in data conveyance and compared with the prevailing methods that bare authentication.

Keywords: Wireless Adhoc network, Authentication, Cluster based routing, Throughput, Energy Consumption and Security in Conveyance.

1. INTRODUCTION

Wireless adhoc networks that are framed for the specific purpose utilizing the devices nearby, have become very prominent as it allows an information transfers with the much reduced cost. These networks framed without any infrastructure are termed as decentralized network as they do not have any central body controlling them. The network formed either using the heterogeneous or a homogenous device is capable of self-organizing, self-healing and as well as reconfiguring on the entry or the exit of the any devices. The devices connected to the network are

ISSN: 2582-337X (online)

Ubiquitous Computing & Communication Technologies

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

free to move anywhere, anytime so they do not require any complex infrastructure set up and administration and allow the devices to join the network, frame it and leave it on the fly according to their convenience.

The network holds dynamic topology as the devices are unrestricted to move in any direction at any time, this often affected the life of the network and also the transmission process. As the conventional routing methods were not compatible for this kind of networks, proactive, reactive and the hybrid (combining both the proactive and reactive) methodologies of routing were developed to handle information conveyance through the network. Further, more modifications were also introduced in the routing methods in order to retain the battery of the devices in turn to extend the life of the network.

From many methods framed to optimize the performance of the adhoc-networks, such as reducing the energy consumption by bringing down the delay in the transmission enumerating the devices with the minimum distance to the destination for communication. The cluster based routing technique seemed to be very efficient and promising providing an optimized route with minimum energy consumption as more devices were not involved in relaying of the information's.

Despite its efficiency the information conveyed between the head of the clusters to the base station was often affected by multitudes of attacks either modifying the information conveyed or hacking them due to the security insufficiency in the cluster based routing.

To protect the information conveyed and as well as optimize the energy usage. The paper puts forth cluster based routing for energy optimization and includes a verification code for every packet transmitted from the head of the cluster to destination.

In the proposed method it is assumed that the base station is deployed with authenticated devices, the parameters such as the trust, energy, distance and the degree of the devices are evaluated to identify the optimal device and assign as the cluster head, nodes and the relaying nodes. The proposed method utilizes the hill climbing algorithm to identify the optimal devices and utilizes the fuzzy logic to enumerate the trusted path from the source to the head of the cluster. The verification code is added to each data packet transmitted from the head of the cluster to the destination to authenticate that the information has reached the authorized person.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

The paper is organized with the related works in section 2 the proposed authentication scheme in section 3, result evaluation in section 4 and conclusion in section 5.

2. RELATED WORKS

The wireless adhoc network also coined as the mobile adhoc networks are utilized in variety of applications such as the mobile networks, vehicular networks, wireless mesh networks, wireless sensor network, disaster rescue, data monitoring, and mining etc. As the energy consumption was the main reason behind the failures in these networks many researchers strived at improving the performance of the network to reduce the energy consumption and enhance the network life time the approaches such as the cross layer optimization was put forth by the author Raj, Jennifer S. et al [1] to enhance the performance of the mobile adhoc networks and achieve the energy optimization.

Later the author Harikumar, R., et al [2] in his paper analyzed the “connectivity methods in the adhocnetwork to improve the throughput and reduce the delay in the process of the conveyance”. Ramesh, S et al [3] in his paper proposed the “heuristic clustered architectures for the WSN” the performance analysis showed much improvement in the energy consumption compared to the other routing methodologies.

Smys, S. et al [4] proposed “Energy-Aware Security Routing Protocol for Wsn in Big-Data Applications." just enumerating the distance of the nodes, and encrypting the information’s conveyed, but the information through this process were through the untrusted nodes in the network. The author Anto Prem Kumar et al [5] put forth an "Energy Efficient Localization and Routing Strategy for Cluster Based Sensor Networks." though the method was promising this lacked the security in the network.

Smys, S et al [6] has put forth the machine learning to detect the attacks in the telecommunication networks and Duraipandian, M et al [7] put forth the performance analysis of the MANET routing method that were based on the machine learning techniques. Rahimunnisa, K et al [8] put forward the “hybridized evolutionary algorithms to improve the performance of the adhoc networks by enumerating the optimal devices. Shakya, Subarna et al [9] presents the “An Efficient Security Framework for Data Migration in a Cloud Computing Environment."

The author Bashar, Abul et al [10] put forth the "Secure and Cost Efficient Implementation of the Mobile Computing Using Offloading Technique." G. Josemin Bala et al [11] in her paper details the “Self organized,

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

topology control ability of the backbone node in wireless networks." by introducing the novel method called the Stab-WIN.

Praveena, A et al [12] explains the cryptographic methods available to secure the conveyance in the wireless sensor networks. Sridhar, S., et al [13] in his paper proposes the "A hybrid multilevel authentication scheme in the private cloud environment." to enhance its security. Dordaie, et al [14] utilizes the PSO in combination with the HCA to schedule the tasks in the cloud computing. Joseph, S. Iwin Thanakumar et al [15] presents the comprehensive survey on the intelligent computing system that operate utilizing the data mining algorithm's. Most of the methods found above concentrated on the improving one parameter at the cost of the other and the cluster based routing concentrated on the performance improvement and lacked security so the paper is to address the security needs of the adhoc networks and as well as optimize the performance of the same.

3. METHODOLOGIES USED

The proposed method utilizes the hill climbing algorithm to determine the parameters of the device engaged in framing the network and separates the devices as the head of the cluster, member and the relaying nodes. Further the fuzzy logic is put forth in handling the information transmission from the member- devices to the cluster head (CH) – device and from the CH-device to the Destination-device by including a verification code by applying the symmetric cryptographic method. The fig .1 below shows the block diagram of the proposed method.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

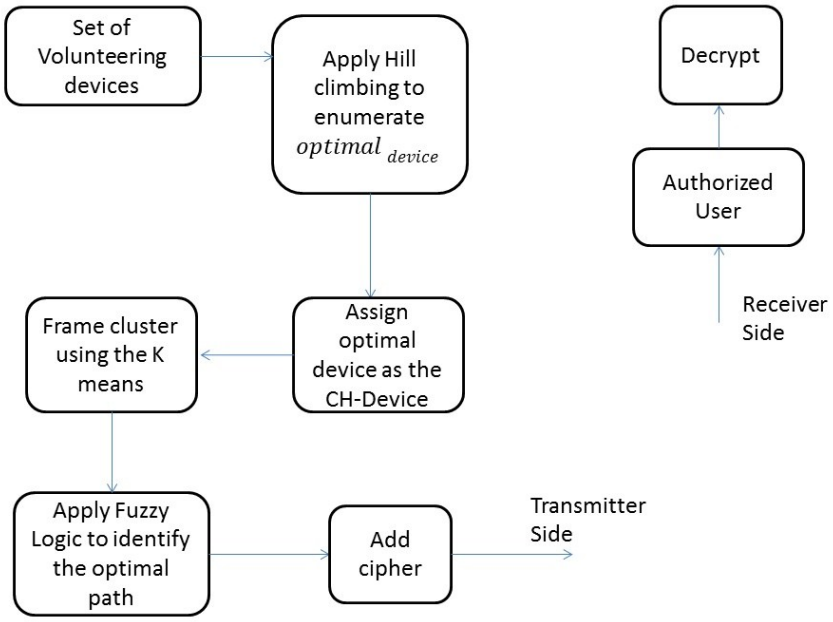

Fig .1 Proposed Block Diagram

3.1. DEVICES IDENTIFICATION USING THE HILL CLIMBING ALGORITHM [14]

The devices that are volunteering to participate in the network are gathered and their particulars regarding their distance ($device_{dist}$), the trust ($device_{trust}$), energy level ($device_{energy}$) and the degree of the devices ($device_{degree}$) are collected. These parameters are enumerated to identify the capable device to assign as the cluster head applying he hill climbing algorithm, that continuously travels forward in the increasing elevation to identify the best solution and stops on reaching the optimal solution, where no other neighbor has a higher value The figure.2 below shows the flowchart of the hill climbing algorithm in identifying the cluster head.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

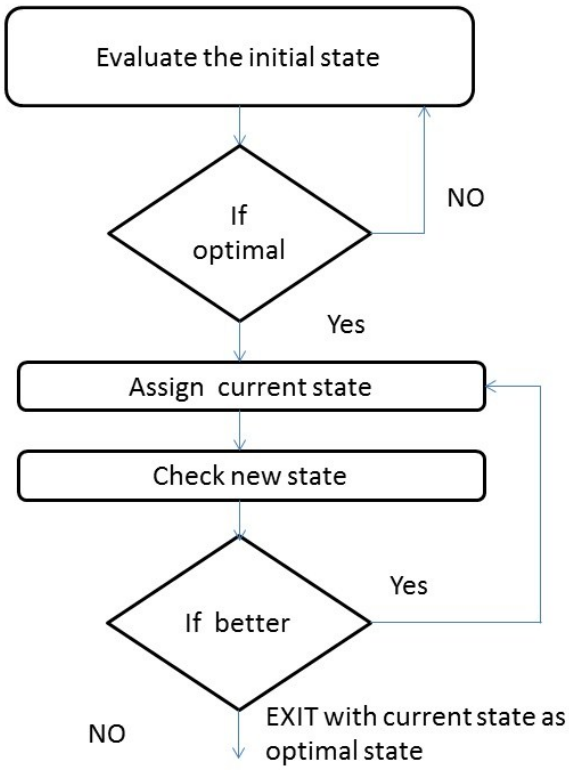

Fig.2 Hill Climbing Algorithm

The other devices in network are either assigned as the members to CH-devices until the degree is satisfied and the left over members are assigned as the relaying devices. This process continues periodically to ensure that network is assigned with the more efficient device as the head of the cluster.

3.2. FUZZY LOGIC IN FINDING THE TRUSTED PATH

The parameters of the member–devices and the relaying-devices are enumerated to identify the path between the source to the CH-device and the CH-device to the Destination, by generating a greeting message from the destination in order to find out trusted path with minimum distance from the source to the destination. The fuzzy logic[15] applied gathers the details of the parameters and coverts it into the fuzzified values using the membership

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

function based on the triangular and the trapezoidal and applies the fuzzy rule and identifies the best path to transmit the information. The table.1 below provides the fuzzy rules in identifying the trusted path with minimum distance.

Max	Max	Max	Max	Normal
Min	Max	Max	Max	Best
Min	Min	Min	Max	Worst
Min	Min	Max	Max	Normal
Min	Max	Min	Min	Worst
Min	Min	Max	Min	Worst
Max	Min	Min	Max	Worst

Table.1 Fuzzy Rules

As the devices in the adhoc network are mobile in nature, they are free to move on the fly, such high mobility of the devices still remain as the threat to the information conveyance, so to further improve the security in transmission the proposed method introduces the cryptography ciphers [4], where each device in the network is provided with the key and the every data packet that is transmitted is aided with a key. The CH-device encrypts the data along with the data packets and transmits the information, such that the information can be decrypted only by the authorized devices for which the information is destined for the fig. 3 below shows the method of encryption and decryption followed in the proposed process.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

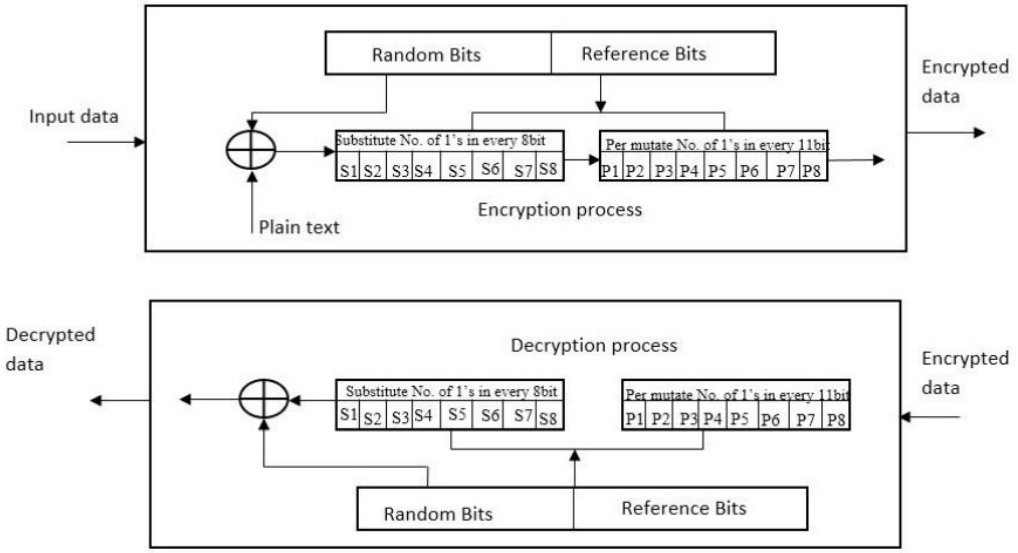

Fig .3 Encryption/Decryption Process [4]

3.3. PROPOSED ALGORITHM OF CLUSTER BASED ROUTING WITH AUTHENTICATION.

The proposed algorithm below provides the steps in the process cluster based authenticated routing

Step.1: Broadcast a REQST message from the destination and gather the REPLY of the volunteering nodes.

Step.2: Collect the particulars of the devices$device_{dist}$, $device_{trust}$, $device_{energy}$ and the$device_{degree}$.

Step.3: Enumerate the particulars applying the hill climbing algorithm.

Step 4: identify the Devices with the $max\ \{device_{trust}, device_{energy}\ and\ thedevice_{degree}\} \cup min\ \{device_{dist}\} = optimal_{\ device}$

Step.5: Assign the $optimal_{\ device}$ as the CH-Device and the remaining as the member –device and the relaying-device using the K-means algorithm

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

Step.6: Identifying the path enriched with the $max\{device_{trust}, device_{energy}\} \cup min\{device_{dist}\}$ applying fuzzy logic.

Step.7: Encrypt the data packets and transmit the information to the destination.

Step.8: Decrypt the data packets applying the reverse process of encryption and extract the information.

The Adhoc network framed with the authentication would be more suitable for the applications such as hospital monitoring, home security etc.

4. RESULTS AND DISCUSSION

The cluster based authenticated routing (CBAR) is evaluated using the network simulator-2 in terms of Throughput, energy consumption and the security for varying number of devices ranging from 100 to 500, for a simulation time 100seconds and initial power of 100 joules, the packet size ranged within the 1024 bits. The results obtained were compared with the prevailing cluster based routing without security (LEACH).

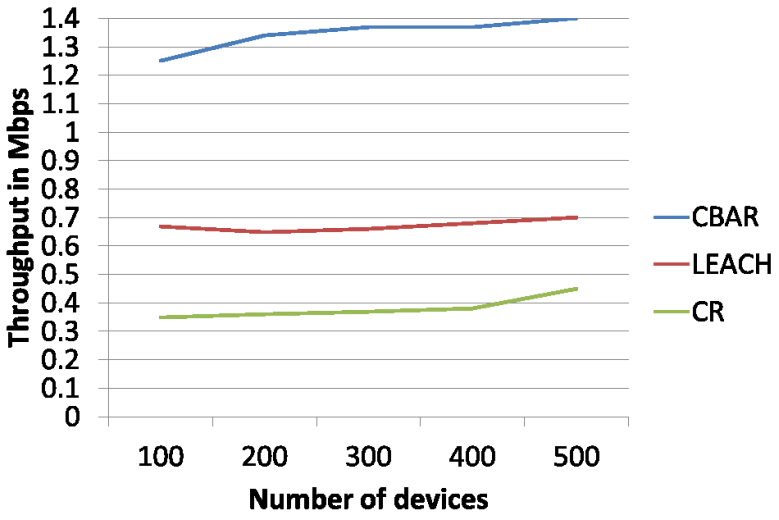

Fig.4 Throughput

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

The fig.4 shows the throughput achieved by the CBAR and the LEACH, the result obtained shows that the CBAR shows a 30 % higher throughput that he leach and 55% higher throughput than the conventional routing (CR) methods.

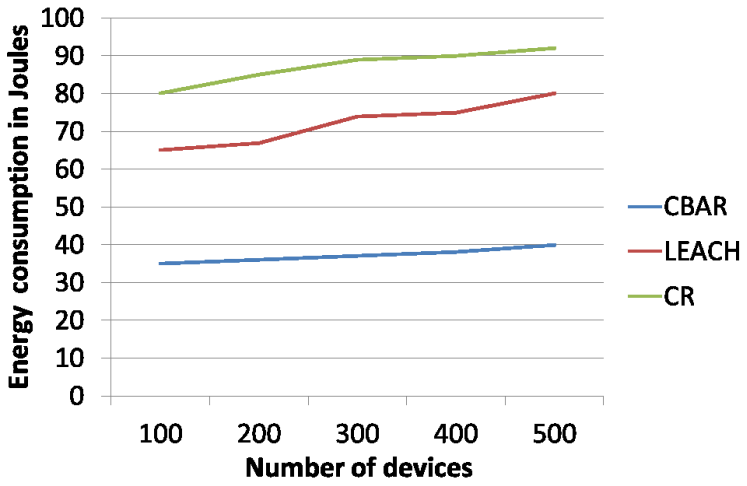

Fig.5 Energy Consumed

The fig.5 above gives the total energy consumed by the CBAR, LEACH and the conventional methods; the results acquired shows that the proposed has 20% less energy consumption than the LEACH and 45% lesser energy consumption than CR. The fig.6 below provides the security percentage of the achieved by the CBAR for varying number of nodes.

ISSN: 2582-337X (online)

Journal of Ubiquitous Computing and Communication Technologies (UCCT) (2019)
Vol.01/ No. 02
Pages: 64-75
https://www.irojournals.com/jucct/
DOI: https://doi.org/10.36548/jucct.2019.2.001

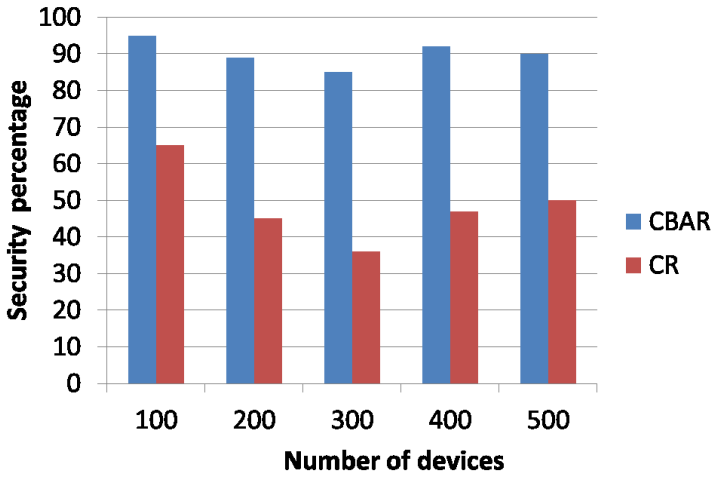

Fig.6 Security Percentage

5. CONCLUSION

The proposed method introduces authentication in the cluster based routing to avoid the unwanted security breaches in the communication between the head of the clusters to destination. The performance optimization in terms of throughput and energy consumption is achieved in the paper using the hill climbing algorithm that identifies the optimal devices and the fuzzy logic to identify the optimal routes. Further the verification code is included along with the data packets to secure the information transfer in the network. The result obtained shows the capability of the proposed method on the grounds of the security, throughput and the energy consumption. In future the secure adhoc network with the mobility management is to be addressed in the paper.

References

[1] Raj, Jennifer S., S. Smys, and G. Josemin Bala. "Performance improvement in manets: a cross layer approach via TCP." *International Journal of Recent Trends in Engineering* 2, no. 1 (2009).

[2] Harikumar, R., and Jennifer S. Raj. "Ad hoc node connectivity improvement analysis–Why not through mesh clients?." *Computers & Electrical Engineering* 40, no. 2 (2014): 473-483.

ISSN: 2582-337X (online)

[3] Ramesh, S., and S. Smys. "Performance analysis of heuristic clustered (HC) architecture in wireless networks." In *2017 International Conference on Inventive Systems and Control (ICISC)*, pp. 1-4. IEEE, 2017.

[4] Smys, S. "ENERGY-AWARE SECURITY ROUTING PROTOCOL FOR WSN IN BIG-DATA APPLICATIONS." *Journal of ISMAC* 1, no. 01 (2019): 38-55.

[5] Raj, Jennifer S., and A. Anto Prem Kumar. "ENERGY EFFICIENT LOCALIZATION AND ROUTING STRATEGY FOR CLUSTER BASED SENSOR NETWORKS."

[6] Smys, S. "DDOS ATTACK DETECTION IN TELECOMMUNICATION NETWORK USING MACHINE LEARNING." *Journal of Ubiquitous Computing and Communication Technologies (UCCT)* 1, no. 01 (2019): 33-44.

[7] Duraipandian, M. "PERFORMANCE EVALUATION OF ROUTING ALGORITHM FOR MANET BASED ON THE MACHINE LEARNING TECHNIQUES." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 25-38.

[8] Rahimunnisa, K. "HYBRIDIZED GENETIC-SIMULATED ANNEALING ALGORITHM FOR PERFORMANCE OPTIMIZATION IN WIRELESS ADHOC NETWORK." *Journal of Soft Computing Paradigm (JSCP)* 1, no. 01 (2019): 1-13.

[9] Shakya, Subarna. "AN EFFICIENT SECURITY FRAMEWORK FOR DATA MIGRATION IN A CLOUD COMPUTING ENVIRONMENT." *Journal of Artificial Intelligence* 1, no. 01 (2019): 45-53.

[10] Bashar, Abul. "SECURE AND COST EFFICIENT IMPLEMENTATION OF THE MOBILE COMPUTING USING OFFLOADING TECHNIQUE." *Journal of Information Technology* 1, no. 01 (2019): 48-57.

[11] Smys, S., and G. Josemin Bala. "Stab-WIN: Self organized, topology control ability backbone node in wireless networks." *Wireless Personal Communications* 63, no. 3 (2012): 529-548.

[12] Praveena, A., and S. Smys. "Efficient cryptographic approach for data security in wireless sensor networks using MES VU." In *2016 10th international conference on intelligent systems and control (ISCO)*, pp. 1-6. IEEE, 2016.

[13] Sridhar, S., and S. Smys. "A hybrid multilevel authentication scheme for private cloud environment." In *2016 10th International Conference on Intelligent Systems and Control (ISCO)*, pp. 1-5. IEEE, 2016.

[14] Dordaie, Negar, and Nima Jafari Navimipour. "A hybrid particle swarm optimization and hill climbing algorithm for task scheduling in the cloud environments." *ICT Express* 4, no. 4 (2018): 199-202.

[15] Joseph, S. Iwin Thanakumar. "SURVEY OF DATA MINING ALGORITHM'S FOR INTELLIGENT COMPUTING SYSTEM." *Journal of trends in Computer Science and Smart technology (TCSST)* 1, no. 01 (2019): 14-24.

ISSN: 2582-337X (online)