ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 8, August 2016

TD-DEEDV: A Technique to prevent collaborative attacks using Clustering and Digital Signature in Multi Hop Hybrid Ad-hoc Networks

Ankita Joshi, Er. Aditi Agrawal, Prof A. K. Jaiswal, Dr. Rajeev Paulus

***Abstract*— Multihop Hybrid Ad hoc Networks are not the pure Ad hoc Networks instead a base station is deployed with the help of clustering approach. Ensuring security of such networks is a researchable task. In case of Wireless Communication, the attacks against the wireless networks are in large scale and it is very sturdy to tackle all the types of security attacks under single mechanism, therefore in this paper main focus is given to combination of black hole and grey hole attacks. We propose Three Dimensional-Distributed Energy Efficient Distance Vector (TD-DEEDV) which performs security checks on the basis of three parameters and enhances the performance of previously implemented EMAODV by 58%, 5% and 8% in terms of Number of Nodes Alive, Packet Delivery Ratio and Throughput, respectively.**

***Index Terms*— Black hole Attacks, DEEC, DSA, Grey Hole attacks.**

I. INTRODUCTION

Mobile Wireless Networks have been in demand from the last 20 years. Few years back the two most important applications of wireless networks were mobile telephony and messaging, but the most recent mobile networks can transfer virtually any kind of data. These data services are getting more and more in use [1].

So far infrastructure networks are most oftenly used. But due to need of decentralized network for accessing data regardless of geographical positions, the wireless ad hoc network and hybrid networks are evolved. Ad hoc networks are a self- reliant system in which each nodes are connected to each other through wireless links. When the mobile devices come closer to each other then they start detecting each other and start to organize themselves without any central authority, e.g. Bluetooth.

***Ankita Joshi**, Department of Electronics and Communication Engineering, SHIATS, Allahabad, India, +919917274157.*
***Er. Aditi Agrawal**, Department of Electronics and Communication Engineering, SHIATS, Allahabad, India, +919935733330.*
***Prof. A. K. Jaiswal**, Department of Electronics and Communication Engineering, SHIATS, Allahabad, India, +91983946365.*
***Dr. Rajeev Paulus**, Department of Electronics and Communication Engineering, SHIATS, Allahabad, India, +919415262430.*

The ad hoc networks and infrastructure networks are amalgamated so that the advantages of both the networks are used. The amalgamation of pure ad hoc networks with those of cellular networks is termed as Multi Hop Hybrid Ad hoc Networks. The advantage of using cellular network is to provide larger service area but since the nodes are capable of extending the service area by themselves, therefore clustering concept is used which is the process that divides the network into interconnected substructures, called clusters. Each cluster has a particular node elected as cluster head (CH) based on a specific metric or a combination of metrics such as identity, degree, mobility, weight, density, etc. The cluster head plays the role of coordinator within its substructure. Each CH acts as a temporary base station within its cluster and communicates with other CHs [2,3]. A cluster is therefore composed of a cluster head, gateways and members node.

- *Cluster Head (CH):* it is the coordinator of the cluster.
- *Gateway:* is a common node between two or more clusters.
- *Member Node (Ordinary nodes):* is a node that is neither a CH nor gateway node. Each node belongs exclusively to a cluster independently of its neighbours that might reside in a different cluster [4].

One of the main goals of Multi Hop Hybrid Ad hoc Networks is to ensure security from attacks such as Black hole attack, Worm hole attack, DoS attack, Sybil attack, Grey hole attack, etc. Working at the current status the most prominent of them are Black hole and Grey hole attacks. The proposed algorithm i.e. TD-DEEDV(Three Dimensional-Distributed Energy Efficient Distance Vector) is designed to detect and prevent the cooperative Black hole and collaborative attacks. The stated algorithm performs security checks based on (1) Distance (2) Residual Energy (3) Optimality and finally verifies the digital signature of the received data packets.

Our suggested technique works on firstly- Distance which is determined by the Euclidean Distance formula between the intermediate nodes, secondly- Residual Energy, calculated by Distributed Energy Efficient Protocol and lastly, the optimality of the route i.e. form the databases. This is novel and effective solution which overcomes the limitation of various approaches.

II. RELATED WORK

In present scenario, the security issues are the most prominent concerning issues in Wireless Networks. The security goals are- Availability, Confidentiality, Integrity, Authentication, Authorization, Resilience to attacks, and Freshness. In retrospect, the work in [10], presented EMAODV (Enhanced Modified Ad hoc On Demand Distance Vector). In this paper, the normal AODV is modified so that the individual black hole attack and Collaborative attacks can be detected and prevented. The results showed that the EMAODV gives better results than normal AODV when different parameters were taken into account i.e. throughput, routing overhead and packet delivery ratio but the drawback of EMAODV was that it cannot detect the cooperative black hole attack and a threshold value is set in which certain distance is defined upto which it can detect the attack.

In [11], the authors described a BAAP (Black hole Attack Avoidance Protocol) protocol for avoiding malicious nodes in the routing path by using legitimacy table which was maintained by each node in the network. The report presented in [1], investigated the problem of placing Base Stations in Multi Hop Hybrid Networks and proposed the Cluster Covering Algorithm, an algorithm which takes into account the percolation phenomenon, and compare it with several greedy algorithms. Author also measured the connectivity through different simulations on real population distribution data of Zurich (CH), the Surselva Valley (CH) and Finland. The simulation results showed that the Cluster Covering Algorithm outperforms the greedy algorithms.

The review conducted in [4], presented an analysis of some existing clustering approaches for MANETs that recently appeared in literature, which they classified as: Identifier Neighbor based clustering, Topology based clustering, Mobility based clustering, Energy based clustering, and Weight based clustering. Authors also included clustering definition, review existing clustering approaches, evaluated their performance and cost, discussed their advantages, disadvantages, features and suggested a best clustering approach. In [12], author proposed an on-demand routing protocol for ad hoc wireless networks that provides resilience to byzantine failures caused by individual or colluding nodes. The authors in [7] [8], presented the solutions to tackle the problem of grey hole attacks in MANETs. The work in [13], proposed and evaluate a new distributed energy-efficient clustering scheme for heterogeneous wireless sensor networks, which is called DEEC. In DEEC, the cluster-heads are elected by a probability based on the ratio between residual energy of each node and the average energy of the network. The epochs of being cluster heads for nodes are different according to their initial and residual energy. The nodes with high initial and residual energy will have more chances to be the cluster-heads than the nodes with low energy. The simulation results showed that DEEC achieves longer lifetime and more effective messages than current important clustering protocols in heterogeneous environments. In [6], authors tried to find the secure path for transmission through Digital Signature which is the verification technique.

III PRELIMINARIES

(A) Black Hole Attack

Black hole problem in MANETS [5] is a serious security problem to be solved. In this problem, a malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept.

1) Single Black Hole Attack

In AODV route discovery is done with the help of RREQ/RREP messages. As shown in fig 3.1, when source node S wants to send data packets then it first broadcast the RREQ message to the neighbour nodes, after receiving the route request messages then either destination node sends the RREP message to the source node or the intermediate nodes. If the RREP is given by the attacker node then it means that all the data packets are forwarded to the attacker node as it replies the source node with minimum hop count and minimum destination sequence number.

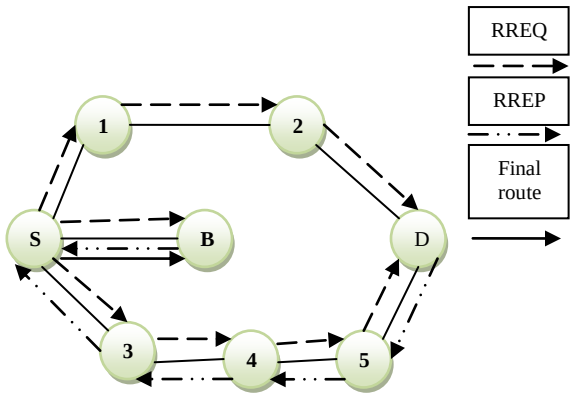
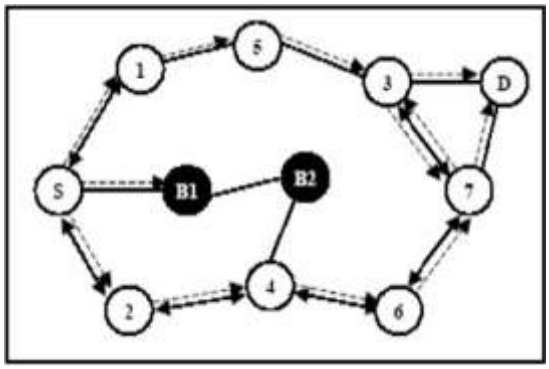


Fig 3.1: Black hole Attack

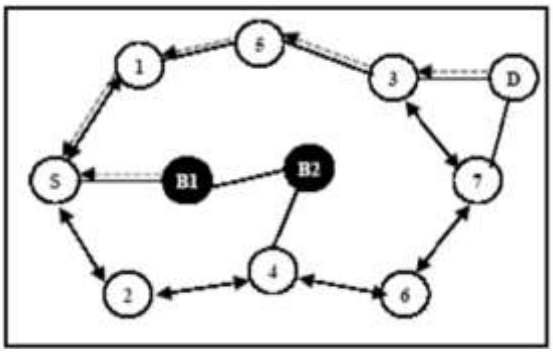
B denotes the black hole node through which data packets are not able to reach to the destination node.

2) Cooperative Black hole Attack

In cooperative black hole attack there is more than one attacker node in the network.



(a)



(b)

Fig 3.2(a) & (b): Cooperative Black hole Attack

In above fig 3.2(a), when multiple black hole nodes are acting in coordination with each other, the first black hole node B1 refers to one of its teammates B2 as the next hop. According to [6], the source node S sends a "Further Request (FRq)" to B2 through a different route (S-2-4-B2) other than via B1. Node S asks B2 if it has a route to node B1 and a route to destination node D. Because B2 is cooperating with B1, its "Further Reply (FRp)" will be "yes" to both the questions, then all the packets are consumed by node B1 and the security of the network is compromised.

B) Grey Hole Attack

A grey-hole attack is extension of black-hole attack used to bluff the source and monitoring system by partial forwarding. Here, attackers uses selective data packet dropping method to behave as genuine node and try to participate into full communication. Grey-hole malicious node participate into route discovery process and update the source route cache/ routing table as shortest path. Afterwards, source always consider malicious node as next hop node and forward packet to same. Malicious node captures all the incoming packets but drop on random basis. The complete phenomena create toughness against detection and prevention mechanism because harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature [7].

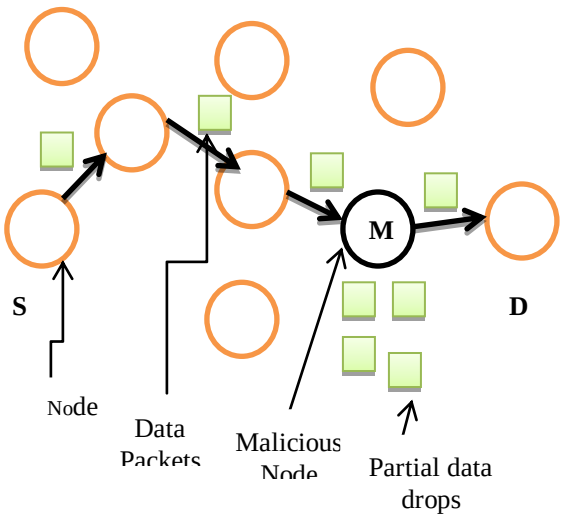


Fig 3.3: Grey hole Attack

C) EMAODV

- Normal AODV doesn't have any secure method to detect or prevent Black hole and Grey hole attacks.
- EMAODV (Enhanced Modified AODV) [10] was used for preventing and detecting malicious nodes in MANETs during conditions of single individual attacks or collaborative Black hole and Grey hole attacks.
- Collaborative Attacks are combinational synchronized attacks by two or more attacker on MANETs which are also compatible to each other.

Drawbacks of EMAODV-

- EMAODV cannot detect the cooperative black hole attack i.e. more than one black hole attack.
- In this technique the threshold value is set in which certain distance is defined up to which it can detect the attack.

D) DEEC (Distributed Energy Efficient Clustering)

The DEEC protocol is a distributed based energy efficient protocol for heterogeneous Wireless Sensor Networks. It is the successor of LEACH protocol but the cluster head selection is different in DEEC. The cluster head selection is done with the probability based ratio between the residual energy of each node and average energy of the system. The DEEC upholds the distributed property as it can be implemented on the Multi-Level heterogeneous WSN [9].

DEEC uses the initial and residual energy level of the nodes to select the cluster-heads. To avoid that each node needs to know the global knowledge of the networks, DEEC estimates the ideal value of network life-time, which is use to compute the reference energy that each node should expend during a round [10].

E) DIGITAL SIGNATURE

Digital Signature is a mathematical technique used to validate the authenticity and integrity of data. Digital Signatures depends on public key cryptography which is also called as Asymmetric cryptography. With the help of RSA (Rivest Shamir Adleman) two keys are generated i.e. public key and private key. To create a digital signature, the electronic data which is to be signed is converted to the hash value by the help of signing software. Then this hash value is then encrypted by the private key. Digital Signature is the encrypted hash with other algorithm such as Hashing Algorithm. If the data is changed even a single character then the hash value is different for the changed data since hash value is unique for hashed data. This concept is used for validation of the data. The public key is then used to decrypt the hash. This decrypted hash is then matched to the second computed hash of the same data, if the two hash does not match then it means the data has been tempered.

IV. PROPOSED APPROACH

The proposed protocol TD-DEEDV enhances the security level of data by three level checking. For this, there are 100 nodes placed in an area of 100mx100m. These nodes have random mobility. The performance at 10m/sec average speed of all nodes with pause time 100 sec. has been observed in this dissertation. The simulation time is 1000 seconds.

A) Modules for Attack Detection and Prevention Technique

Phase 1: Create a network of 100 nodes.
Phase 2: Broadcast the member nodes of one BS (Base station) according to given range.
Phase 3: Select the neighbor member of nodes which is neighbor to the base station.
Phase 4: Send the packets from one node to another node.
Phase 5: Analyze the parameter such as packet sent and received.
Phase 6: Apply Attack detection and Prevention Technique to detect the network under collaborative attack or not.
Phase 7: Remove the attack.

It is considered that if the residual energy of a node is greater than the average residual energy of the network, then this node has sufficient energy and has a high probability of transmitting more data packets before being exhausted.

B) Steps of proposed algorithm

Step 1: when node wants to send data
Step 2: node sense channel. If it is free then check all coverage distance of node to send data.
Step 3: if (ACK == yes) then packet received successfully (repeat process 1)
Step 4: if (ACK == no) means acknowledgment not received then new digital signature back-off which optimize by using residual energy of individual node is called to calculate the waiting slot time.
Step 5: if (n=number of attack detect< no of transmission) then discard packet and find all grid position of back-off node in network.
Else
WT = Digital signature (n)
End if
Step 6: wait till WT = 0 and then send packet again
If (intrusion) then check optimality of node.
Go to step 5
Else
Go to step 1
Step 7: end

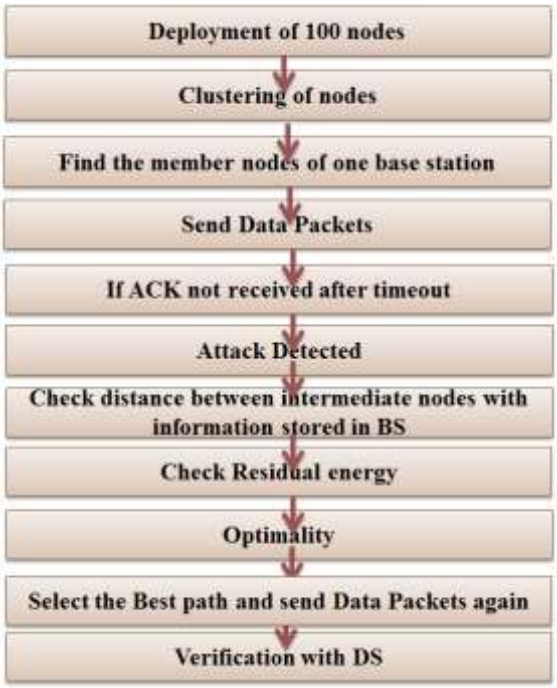


Fig4.1 Steps of proposed approach in blocks

V. PERFORMANCE AND EVALUATION

A) Environment Of Simulation

Proposed scheme evaluation done by MATLAB 2014a for 100 nodes and shows that TD-DEEDV gives better performance than EMAODV.

Table I Simulation Parameters

Examined protocols	AODV and DEEC with DSA
Simulation time	1000 seconds
Simulation area (m x m)	100 x 100
Number of Nodes	100
Traffic Type	TCP
Performance Parameter	Packet sent and receive
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Time (s)	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

B) Result and discussion

Our goal is to determine the protocol which shows less vulnerability in case of black hole attack and grey hole attack (Collaborative attack).

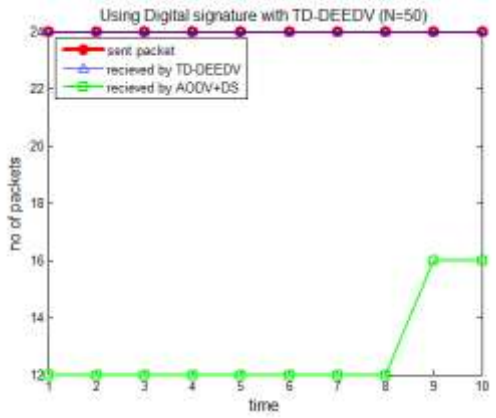


Fig 5.1: Performance Of Total No Of Packets w.r.t Sent Packet-Received Packet By TD-DEEDV And AODV+DS Using Digital Signature With TD-DEEDV

If network is distributed with grid positioning, then packet sent using TD-DEEDV factorize the packet on the basis of node energy, distances(depend on routing table) and optimality and at the time of packet receiving it verify it by grid digital .

Fig 5.1 shows that, if 30 packets are sent then acknowledgement receive for 24 nodes i.e. only 24 packets are effectively sent. By using TD-DEEDV it is clear that 24 packets are received wrt 24 sent packets. In case of AODV with DS, the packet received for 12 nodes i.e.12 packets are received till the execution time is 8 nsec. After that it gets improved for 9nsec to 10nsec i.e. 16 packets are received.

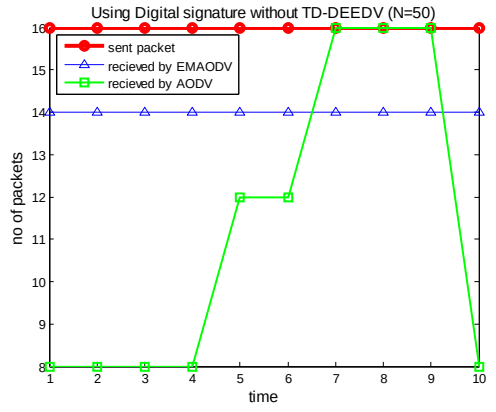


Fig 5.2: Performance Of Total No Of Packets w.r.t Sent Packet - Received Packet By EMAODV And AODV Using Digital Signature

Similarly in fig 5.2, the total number of sent packets are 16 w.r.t. 30 packets. In EMAODV the received packets are 16 while in case of AODV, 8 packets are received till execution time is 4nsec and after that at 5nsec, packets received are 12 then it becomes constant upto 6nsec, at 7nsec total number of packet received are 16 upto 9nsec and at 10nsec only 8 packets are received. Therefore after comparative study of above two graphs, it shows that total number of received packets are more with the help of TD-DEEDV and hence it is better.

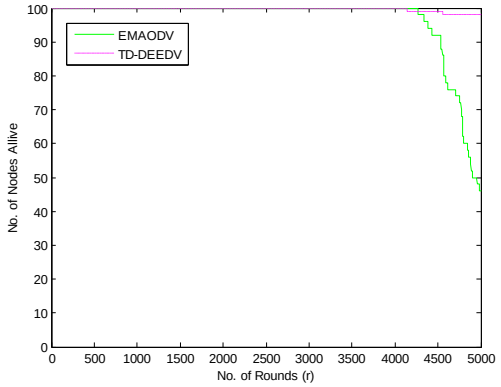


Fig 5.3: Performance comparison between EMAODV and TD-DEEDV for no of alive nodes

Alive Nodes per round: These are the nodes which exists till the last round. So higher would be the alive nodes better will network perform. Expected that the node energy is used to evaluate the probability based on the ratio between residual energy of each node and the average energy of the network. Fig 5.3 shows that the number of alive nodes per round for TD-DEEDV gives best result as compare to the EMAODV which is approximately 58% more improved.

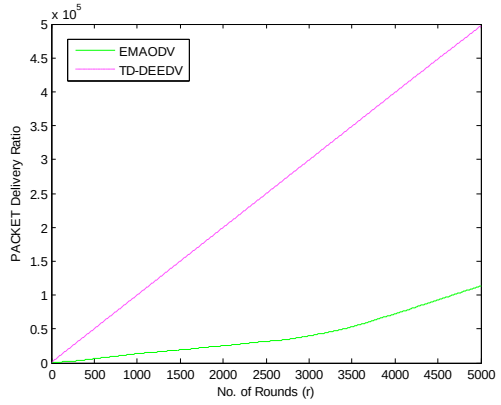


Fig 5.4: Performance comparison between EAOMDV and TD-DEEDV for no of packet delivery ratio

Packet Delivery Ratio is the percentage of the amount of the important inwards packets to the number of all packets conveyed by source. The larger value indicates that the more data packets are positively delivered to destination.

The normal rate at which the entire number of statistics packet is transported positively from one node to another node finished a communiqué network. Experimentally it is declared that TD-DEEDV has higher packet delivery ratio than EMAODV. This saves bandwidth and later increases performance.

Hence as compared to the existing technique we improve 5% more packet deliver ratio using collaborative black hole and grey hole detection and prevention technique.

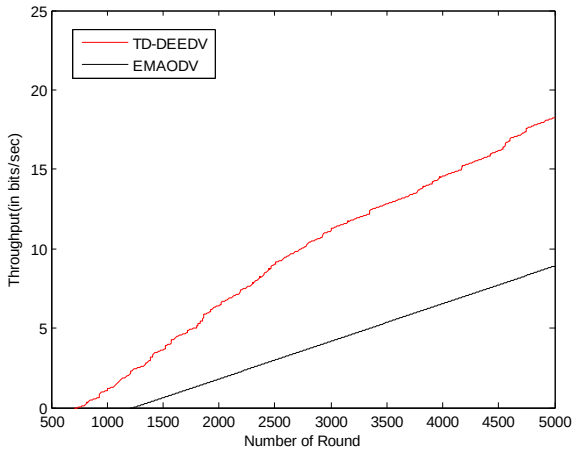


Fig 5.5: Performance comparison between EMAODV and TD-DEEDV for no of Throughput

Throughput is the total number of packets delivered over the total simulation time. Above figure 5.5, shows the Throughput of EMAODV and TD-DEEDV over number of rounds and an improvement of 8% is achieved as compared to existing work.

VI. CONCLUSION

The main aim of this paper is to evaluate black hole and grey hole attack and to see the performance of network after excluding these attack from network. After having studied DEEC, Digital Signature, Hash Key and EMAODV we devised TD-DEEDV which works on three level of security checking, i.e. 1) Distance between the nodes 2) Residual Energy of the nodes 3) Optimality and finally the digital signature of data packets are verified. It is being concluded that the new proposed technique TD-DEEDV is more efficient than the previously suggested work in terms of parameters like number of packets sent and received, number of nodes alive, packet delivery ratio, and throughput. It has been analyzed that when the adversaries collude then the Black hole attack and Grey hole attack affects the network security severely.

The rendition of our work showed, via simulation results in MATLAB, is very convincing since the security of the network is raised to a great level.

VII. FUTURE SCOPE

In future work, the simulations can be developed for other attacks that are compatible to each other having their own specification to target the Multi-Hop Hybrid Ad hoc Network. For this, the different compatible collaborative attacks having own expertise that targets these networks should be examined.

VIII. REFERENCES

[1] T. Lochmatter, "Base Stations in Mobile Ad hoc Networks",EX032/2004,thomas.lochmatter@epfl.ch, July 4, 2004.

[2] M. Anupama and B. Sathyanarayana "Survey of Cluster Based Routing Protocols in Mobile Ad hoc Networks," *International Journal of Computer Theory and Engineering*, Vol. 3, No. 6, 2011.

[3] N. Gupta, M. Shrivastava, A. Singh, "Cluster Based on Demand Routing Protocol for Mobile Ad Hoc Network," *IJERT*, Vol. 1, No. 3, 2012.

[4] B. Abdelhak, A. Boubetra, H Saad, "Survey of Clustering Schemes in Mobile Ad hoc Networks", *Communications and Network*, Vol. 5, No. 8-14, 2013.

[5] L. Tamilselvan, V. Sankaranarayanan "Prevention of Co-operative Black Hole Attack in MANET", *Journal Of Networks*, VOL. 3, NO. 5, MAY 2008.

[6] R. Kaur, J. Kalra, "Detection and Prevention of Black Hole Attack with Digital Signature", *International Journal of Advanced Research in Computer Science and Software Engineering*, 4(8), pp. 843-847, 2014.

[7] R. Sharma, "Gray-hole Attack in Mobile Ad-hoc Networks: A Survey", *IJCSIT*, Vol. 7 (3) ,1457-1460, 2016.

[8] A. Kanthe, D. Simunic, R. Prasad, "A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks", *International Journal of Computer Applications*, Volume 53– No.16, September 2012.

[9] T. Jinpa, B. Reddy, "The Study of the Energy Efficient Protocols (MODLEACH, SEP and DEEC)", *International Journal of Computer Science & Communication Networks*, Vol 5(1),32-38.

[10] A. Rana, V. Rana and S. Gupta, "EMAODV: Technique to Prevent Collaborative Attacks in MANETs", *4th International Conference on Eco-friendly Computing and Communication Systems, ICECCS*, 2015.

[11] S. Gupta, S. Kar, S. Dharmaraja, "BAAP: Black hole Attack Avoidance Protocol for Wireless Network", *IEEE proceedings of the International Conference on Computer & Communication Technology (ICCCT)*,2011.

[12] B. Awerbuch,, D. Holmer, C. Nita-Rotaru, and H. Rubens,"An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," *Proceedings of the 3rd ACM Workshop on Wireless Security*, 2002.

[13] Li. Qing, Q. Zhu, M. Wang, "Design of a distributed energy-efficient clustering algorithm for heterogeneous wireless sensor networks", *Computer Communications*, 2230–2237, 2006.

BIOGRAPHY

Ankita Joshi, received her B.Tech Degree in Electronics and Communication Engineering. from UTU, Dehradun in 2014. She is pursuing her M.Tech in ECE (Communication System Engineering) from SHIATS, Allahabad. Her area of interest includes Wireless Communication and Networking.

Er. Aditi Agrawal is working as an Assistant Professor in the Department of ECE at SHIATS. She received the degree of M.Tech (Wireless Communication) from SHIATS , Allahabad. She is pursuing Ph.D from the same institute . Her area of interest includes Wireless Communication and Digital Communication.