International Journal of Engineering & Technology, 7 (2.8) (2018) 134-138

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research Paper

Secure and effective random paths selection (SERPS) algorithm for security in MANETs

P. Suma [1] *, Mohammed Ali Hussain [2]

[1] Research Scholar, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India
[2] Professor, Department of ECM, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, India
**Corresponding author E-mail: sumapatra@gmail.com*

Abstract

Mobile Ad-hoc Networks (MANETs) are wireless and nodes of it are mobile in nature. These networks can be adopted where equipment like wires cannot be established and the nodes are moving. Due to the mobile nature of nodes, a fixed topology cannot be achieved. This leads to a dynamic or ever changing network structure. The paths between the communicating nodes also change frequently. Overall monitoring system is absent in it i.e. supervising node is not present for establishing routes in the network. Each node itself acts as a router. Due to the lack of fundamental management system and ever moving nodes, security becomes a challenge and detection of attackers also becomes tough. Dynamic source Routing (DSR) is used in route discovery. In this routing strategy, paths are established only on demand of sender and receiver nodes. And to reduce the cost many algorithms were proposed, but the concept of security is deficit in them. In this paper, Secure and Effective Random Paths Selection (SERPS) algorithm is proposed with the concepts of minimum cost and node disjointness to achieve security. All the node disjoint paths between sender and receiver are found. Among them a minimum of 4 minimum cost paths are selected. Then data packets are sent through them by randomly selecting the paths. Care is to be taken such that no consecutive packets go through the same path. By this, attacker at any node gets only the random packets but not the complete data. In this way security can be achieved. The simulation for the proposed SERPS algorithm is done to show the routing process.

Keywords: *Dynamic Routing; Node Disjoint Paths; Minimum Cost; Secure and Effective Random Paths Selection (SERPS) Algorithm.*

1. Introduction

Mobile networks are preferred these days due to its advantages. These networks are suitable where huge equipment or wires cannot be used for connecting nodes. [1] MANETs are preferred in military communication, rescue operations in disaster management, outdoor gaming, communication in transport like, air, water and land etc. Routers are not necessary for communication. Failures in physical connection are least possible with such Ad hoc networks. Different protocols can adopted for efficient data transfer and routing. Compared to wired networks, MANETs need no heavy infrastructure. So MANETs are cost effective [2].

Bandwidth is a basic constraint of MANETs. Fixed bandwidth has to be shared by the nodes of the network. Another crucial restriction is power in the battery of a node. As the nodes are not stable, power charging is definitely a problem. And because of the mobile nature of nodes, topology of the network becomes unstable. Due to this fixed paths between the sender and receiver cannot be maintained [3]. Nodes in a MANET have to move within the boundary. New nodes which enter the boundary can be added and nodes which move out will be discarded from the network. Due to addition and removal of nodes, mobile nature, unstable topology, MANETs are very highly prone to attacks.

Detecting the attacker is also very tough. Different types of attacks as well as solutions for few of them are still evolving.

Basically MANET attacks are classified into Active and Passive attacks. Where in active attacks, the data packets while in transit may be changed, deleted, dropped or routed to different destinations. In Passive attacks the network activities are uninterrupted and unauthorized persons listen to the data messages [4].

1.1. Drawbacks and challenges

Deficiency of Central Monitoring System: To manage and mangle with communication system of MANETs, there will be no central management [5].

Detection of Malicious Node: Many devices join and many moves away from the network scope while in transit. So the detection of suspicious node is difficult.

Adjustability: The network must be able to accept the attachment of new nodes.

Cooperation between Nodes: The nodes in MANET need be more cooperative with all the other nodes in the network.

Ever Changing Topology: Due to the position change of nodes, reliance between the nodes gets reduced.

Scarcity of Resources: Resources like bandwidth, battery constraints, and virus tolerance levels, will not be up to the mark.

Insecure Environment: Malicious nodes may enter the network as new nodes get added. This leads to data theft or stopping the services to nodes.

Varying Protocols: Each node in the network may have different protocols and all these nodes must be compatible with each other.

Inappropriate Boundary: The border of the network in all dimensions cannot be set accurately. Nodes can be added or deleted from the network.

1.2. Routing protocols

Different protocols are present to establish a route between source and destination. Intermediate nodes are necessary for communication, when the source and destination nodes are far apart. Basically there are three routing protocols like proactive, reactive and hybrid routing protocols [6].

Proactive: In proactive routing protocols, each node in a network maintains a routing table. This routing table contains the information of active nodes, neighbouring nodes, and routes to reach other nodes in the network. This table keeps on updating with the latest information in short and regular intervals of time. Using this information, routing of data is done. Periodic updation of routing table even when not required, leads to overhead and consumption of power and bandwidth. Destination Sequenced Distance Vector (DSDV) is an example of proactive routing.

Reactive: In reactive routing protocols, routes are found only when required i.e. only on demand. In this protocol, routing information is not assessed in regular intervals. But when a sender wants to send data to a node, the protocol starts searching for the routes to the destination. Then communication is done. This type of protocol is better suited for MANETs as routes are established only on demand. Thus bandwidth and power are less consumed. This is less suitable for large networks. Dynamic Source Routing (DSR) protocol is an example of reactive routing protocol. In DSR protocol when communication is needed, neighbouring nodes are found by sending route request packets. And based on the fast replies, path is established between source and destination [7].

Hybrid: Hybrid routing protocols support both proactive and reactive routing protocols. This protocol is best suited for large networks because the network is segmented as zones and communication within the zone follows proactive routing and outside the zone routing is reactive. By hybrid routing protocol, the pitfalls of reactive and proactive protocols can be overcome. Zone Routing Protocol (ZRP) is an example of hybrid routing.

1.3. Security

Static networks have fixed number of nodes. Paths between all the nodes are also fixed. If someone within the network creates any attack, they can be detected by using many methods. But in mobile networks, topology is unstable, routes are ever changing, nodes may be added or discarded from the network within the boundary. [5] So creation of attacks is easy and detection of attacker is not possible that easily. Many solutions for few attacks were proposed already and there is a need to optimize them and create solutions for remaining attacks. There are two ways to come out of the attacks. One is to get the solution after getting attacked and the other is to prevent them.

Shortest path algorithms are used to make the communication cost affordable. Many algorithms were proposed for finding the shortest (min-hop) paths. Data transmission through minimum cost paths improves the Quality of Service (QoS) in a network. But sending data through a fixed path may lead to many attacks like eaves dropping. In some cases security is important rather than cost, overhead and many other parameters.

The concept of node disjoint paths provides solution to load balancing, connection disruption, traffic balancing and finding optimal paths. But the concept of node disjoint routes doesn't deal with security much.

This paper combines the concept minimum hop paths and node disjoint paths to provide security and QoS of the network.

2. Literature review

In this section we provide the research survey of MANET security which has lead to the development of SERPS algorithm [8].

Shuchita et al. [9] proposed a method of finding node and link disjoint paths to attain few positive qualities. A Node Disjoint Multipath Routing Considering Link and Node Stability (NDMLNR) protocol was proposed to reduce energy loss of few nodes and to work well in link breakages.

Node-Disjoint Multipath Routing Protocol (NDMR) was proposed [10] to mitigate the overhead while routing data. This protocol proposed an agent based Service Level Agreement (SLA) management system to pick a node disjoint path. This is also used to balance the traffic and to cope with node failures.

A multipath routing technique was proposed [11] to handle the link failures in MANETs. Node disjoint paths are identified between the sender and receiver to reduce delay and to attain good throughput levels.

A protocol with multipath routing using node disjoint paths was proposed to work well in link failures. This technique of routing was meant to reduce packet dropping, delay and efficient delivery of data to the destination [12].

A protocol based on AODV protocol was stated to find three node disjoint paths between sender and receiver. This was done to reduce load on fixed nodes by distributing load on to many nodes [13].

In Node-Disjoint Multipath routing protocol [14] for routing of packets is done by making the nodes disjoint in the network. This type of multipath routing is done to have reliable data transfer in time.

An Efficient Dynamic Route Optimization Algorithm for Mobile Ad hoc Networks [15], is an algorithm to find optimal route. This algorithm can be shortly called DROA. To optimize the route number of hops, delay in traffic, power of nodes were considered.

S.Sharon et al. [16] proposed an efficient routing protocol to provide security in data transmission. In this geographical or position based routing is done. Time is a constraint in routing, i.e when time limit is reached, other next hop is chosen for transmission.

Another type of routing technique which is based on Alpha numeric [17] was proposed. Nodes in a network are classified as leader nodes and active nodes, where leaders are used to monitor the active nodes. Data transmission is done only through the nodes which are authorized. This algorithm is specially used to prevent worm hole attack. In worm hole attack a tunnel is established between two attacker nodes and data is transmitted in through this tunnel only.

Back up routing protocol was proposed by S.J Lee et al., [18]. This is based on AODV protocol. When a link failure occurs, alternative path is selected for transmission dynamically.

Node disjoint paths are used in On-demand Multipath Distance Vector Routing for Ad Hoc Networks [marina]. In this routing method, many paths are involved for data transmission. Stale path usage can be reduced by the concept of node disjointness.

Hamdy H El-Sayed [19] came out with the literature survey on shortest paths routing in Ad hoc networks proposed by many researchers and their solutions.

2.1. Problem statement

MANETs are the wireless networks with mobile nodes. As the nodes are mobile, structure of the network keeps on changing. Each node acts as a router, due to the absence of central monitoring system. These nodes can communicate with the other nodes of the network within the boundary limit. These mobile nodes may move out of the boundary and few may come into the network. On the whole the network topology is very unstable. So there is a possibility of many attacks. Cause of the attack cannot be found that easily. These networks are mostly used in rescue operations when calamities occur and also in military communications. The information obviously will be highly confidential. So the data is prone to have high insecurity while in transit. This paper tries to provide secure data transmission in MANETs which are unstable and high attack prone.

3. Proposed methodology

We propose a solution for preventing secret listening of data called eavesdropping and also in reducing the level of damage through different attacks like worm hole, grey hole attacks and many others. And the main advantage is the achievement of security with least cost and minimum time for transmission. This is achieved using Secure and Effective Random Paths Selection (SERPS) Algorithm to provide security in MANETs. The basic theme behind this algorithm is calculating node disjoint paths and then the minimum cost paths [22] among them. Then the routing is done through all the selected paths in random.

Usually for communication between nodes, a specific path has to be finalized for data transmission. This path has many intermediate nodes (say N). The complete data is divided into packets and these packets have to pass through all intermediate nodes (N1, N2....Nm). Suppose an attacker is present at N5, he can read all the data passing through. So security is lost for the confidential data.

In order to handle such disaster, SERPS algorithm works well. This algorithm works using the following three steps

1) Find the node disjoint paths between the source and destination.
2) Find the cost of each node disjoint paths and select few among them (a minimum of 4 paths). This selection is based on the minimum cost (number of hops between the sender and receiver). This can be done by applying Loop less k-shortest path algorithm to all the node disjoint paths. Using this algorithm, we can find not only the minimum cost path, but also the cost of all the paths in increasing order.
3) Route the packets by selecting the routes (node disjoint and minimum cost) in random.

Detailed process:

Suppose there are 4 least cost and node disjoint paths. Send packet1 from any of the 4 routes in random (suppose path 3). Store the path number in any data structure like array with size 4. i.e. the no. of paths chosen.

The data (path number) in the array will be like

3			

Then for sending packet2, choose any path apart from path3 which is stored in the array (suppose packet 2 is sent through path4). Update the array with the newly used path. Then the array is

3	4		

Send packet3 through any path apart from path3, 4 by checking the data in array(suppose packet 3 is sent through path1). The array now is

3	4	1	

Send packet4 through any path apart from the paths in array (suppose path2). The array now is

3	4	1	2

At any point of time, if the data packets are over, terminate the process and the data structure if full, clear its content and repeat the process for the packets5, 6 and so on till the complete data is sent.

From the whole process, we can observe that each packet follow different routes among the selected ones. Assume that the paths selected are four and the number of data packets is 12. From each node disjoint path, only 3 unordered packets are transmitted. 4 paths multiplied by 3 packets passing through them is equal to 12 packets. So the nodes in each path know only 3 disordered packets. So the attacker at any node cannot read the complete data. If the security is highly needed, the packet size can be reduced. By this little data from here and there can only be retrieved. Thus security is achieved with less cost. As less cost means the less number of hops, transmission time also is reduced.

Representative Notations:

- Source: S
- Destination: D
- Paths which are node disjoint between source and destination are X.Where X = {X1, X2.....Xn | n is the number of node disjoin paths}
- Minimum cost paths selected among X are Q={Q1, Q2....Qm | m= atleast 4 provides good security}
- Array is R and its size is equal to 'm' i.e. the number of least cost among node disjoint paths.

To execute this algorithm, all the node disjoints paths between the source S and destination D have to be found i.e. X = {X1, X2.....Xn}. Then among X find atleast 4 least cost paths Q={Q1, Q2....Qm }.

Secure and Effective Random Paths Selection (SERPS) Algorithm:

Steps:

1) Set up a network.
2) Decide the source node and the receiver node.
3) Compute the different node disjoint paths X = {X1, X2.....Xn} between the two communicating nodes.
4) Also find the least cost paths Q among X i.e. Q={Q1, Q2....Qm }.
5) Declare an array R which can store 'm' path numbers to hold the information of paths used in sending data packets.
6) Transfer the data packet from any of the path from Q. (Assume as Qx) and store the path number x (suppose 4) as the data element of array.

Select a path from Q (Assume Qy) to send the next packet. But before transmitting check the elements of the array and choose the path which is not present in the array.

7) Store that path number 'y' as the next element.
8) Repeat Step 6 until the array is filled completely or until all the data packets are transmitted.

If the array is full, clear the elements of the array and start again from Step 6.

If the complete data is sent, TERMINATE the process of communication.

As we use different routes to transmit the consecutive packets, no attacker in a single path can get the complete data. Using SERPS algorithm solution can be provided to many MANET attacks. Not only the security, link failures can be handled, load on the nodes can be balanced, and Power consumption [20] among the nodes also can be even.

Many attacks can be handled using the proposed algorithm. Few of them along with the solution is stated below[5].

a) Black hole attack [21]: An attacker node may suggest that a particular node is the shortest path among all paths. Using this false information, the sender uses the particular shortest path for transmitting the complete data. The attacker who is somewhere in that path reads the confidential data.

Solution: using SERPS algorithm, data is sent through many paths. Even if the attacker sends the false information that a particular route is the shortest, data is sent through multiple paths. So the attacker at a node of a single path cannot get complete data. He can read only few random parts of data. It is not possible that all the paths have attackers and they collude with each other.

b) Data Packet Dropping attack: A Malicious person at a node drops the data packets and thus prevent to reach the destination.

Solution: By the algorithm proposed, only few packets that pass through the attacker path are dropped by the attacker and other packets reach the destination node through different routes. The dropped packets can be resent.

c) Eaves Dropping & Man in the middle attack: A malicious person at a node can secretly take the confidential data. This secret hearing of data is called eavesdropping.

Solution: only few unordered packets can be retrieved but the complete data is not disclosed to the attacker. If the packet size is less, security increases.

d) Fabrication attack: In this, the data is sent through the route in which the attacker is present. This is done by sending the false information that the neighbouring node chosen is inactive.

Solution: The data packets are sent through multiple routes. So, attacker at a node cannot get the whole data.

e) Grey-hole attack: In this attack, insecure route is projected as the efficient route and the packets moving through this route are dropped by the attacker.

Solution: As data is sent through different paths, only the packets passing through the attacker path are dropped and the remaining packets are transmitted safe.

f) Rushing attack: In this kind of attack, route requests (RREQ) are trapped by an attacker. Then he rushes to send the route reply (RREP) packet faster than other neighbouring nodes. So that the attacker path is chosen for transmission. By this the data can be stolen.

Solution: As multiple paths participate in SERPS algorithm, data passing through the attacker path is only stolen and this stolen data is not complete.

g) Selective Forwarding attack: This is also an attack related to packet dropping. Only few unimportant packets are forwarded to the destination.

Solution: same as solution proposed to rushing attack

h) Wormhole attack: Two attacker nodes at a distance collude and make a tunnel between them to send data. Then confidential data can be tapped.

Solution: Though a tunnel is established for a single route, data passes through multiple routes. Only the data through tunnel is attacked. The receiver then requests the sender to resend the missing packets.

4. Results and discussion

This section illustrates how each data packet takes different routes in a network of 10 nodes with names from 1 to 10. Usually MANETs have many nodes but for simple understanding less number of nodes is taken. The source and the destination nodes are 5 and 3 respectively. Many disjoint routes are possible between them. Like 5-3, 5-1-3, 5-2-3, 5-1-2-3, 5-1-4-3, 5-1-4-6-3 etc. Among them the least cost paths are Path1→5-3, Path2→ 5-1-3, Path3→5-2-3 and so on. The following are few screen shots showing the routes taken.

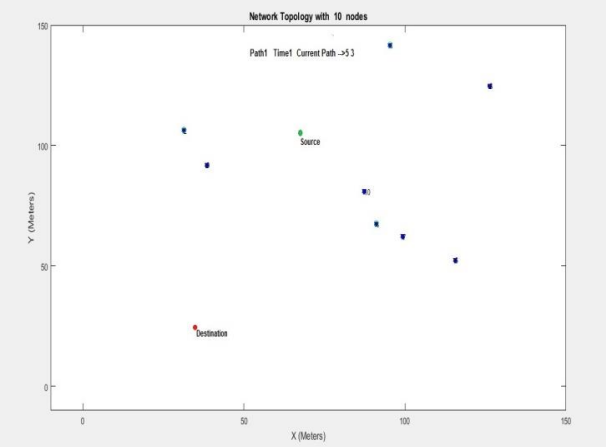

Fig. 1: This Is the Path with Minimum Cost. I.E. Only One Hop From 5 to 3 Directly.

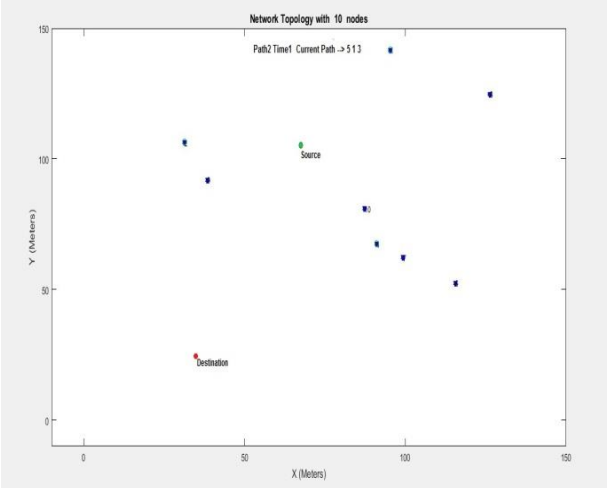

Fig. 2: This Is the Next Minimum Cost Path with Two Hop from 5 to 1 and To 3.

The next paths will be 5-2-3, 5-4-3, 5-6-3 and so on. If all the routes are once used, routing starts from beginning i.e from 5-3, 5-1-3... This process continues till the data packets are over. Suppose the number of packets is 6, and the attacker is at node 2. Only one packet passes through the intermediate node 2 and he can get only that data which is just a small part of the complete data.

5. Conclusion

MANETS are preferred as it needs no wired connections and the nodes are movable. Establishment of the network is also easy due to less infrastructural equipment and the central monitoring system. The advantages of these networks lead to several security issues. MANETs are prone to several attacks. The proposed Secure and Effective Random Paths Selection algorithm provides solution for most of the attacks. This paper explains the process of providing security. The node disjoint and minimum hop paths are chosen for routing. Reducing the packet size provides more security. And the same algorithm when implemented with cryptographic algorithms fails the attempt of the attacker. Not only for mobile ad hoc networks, SERPS algorithm when applied to other wired or wireless networks provide security.

References

[1] Adnan Nadeem., Michael P. Howarth, " A survey of manet intrusion detection & prevention approaches for network layer attacks," IEEE COMMUNICATIONS SURVEYS & TUTORIALS, Vol. 15, Issue 4, pp. 2027-2045, 2013. https://doi.org/10.1109/SURV.2013.030713.00201.

[2] J. Godwin Ponsam and R.Srinivasan, "A survey on MANET security challenges, attacks and its countermeasures," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3, Issue 1, 2014.

[3] Shiva Shankar, Golla Varaprasad and Hosahalli Narayan [1]agowda Suresh, "Importance of on-demand modified power aware dynamic source routing protocol in mobile ad-hoc networks," IET Microwaves, Antennas & Propagation, Vol. 8, Issue 7, pp. 459-464, 2014. https://doi.org/10.1049/iet-map.2013.0230.

[4] Zaiba Ishrat, "Security issues, challenges & solution in MANET", IJCST Vol. 2, Issue 4, 2011.

[5] P.Suma, "Overview of Terminology Related to the Security Issues in MANETS", IJAER, Vol. 10, Issue 11, 2015, pp.29457-29466.

[6] Yuxin Mao and Ping Zhu, "A Game Theoretical Model for Energy-Aware DTN Routing in MANETs with Node's Selfishness", Mobile Networks and Applications, Vol. 20, no. 5, pp. 593-603, 2015. https://doi.org/10.1007/s11036-015-0610-7.

[7] Shubhajeet Chatterjee and Swagatam Das, "Ant colony optimization based enhanced dynamic source routing algorithm for mobile Ad-hoc network," Information Sciences, Vol. 295, pp. 67–90, 2015. https://doi.org/10.1016/j.ins.2014.09.039.

[8] P Suma, O Nagaraju, MA Hussain, “Node Disjoint Random and Optimal Path Selection (NDROPS) Algorithm for Security in MANETS”, International Journal of Electrical and Computer Engineering (IJECE), Vol. 7 Issue. 3, pp. 1197-1203, 2017. https://doi.org/10.11591/ijece.v7i3.pp1197-1203.

[9] Dr. Shuchita Upadhayaya and Charu Gandhi., "Node Disjoint Multipath Routing Considering Link and Node Stability protocol: A characteristic Evaluation". International Journal of Computer Science Issues (IJCSI), Vol. 7, Issue 1, No. 2. 2010.

[10] Luo LIU1, Laurie CUTHBERT2. "QoS in Node-Disjoint Routing for Ad Hoc Networks", I. J. Communications, Network and System Sciences. vol , no. 1-103, 2008.

[11] A.Monisha, K.Vijayalakshmi, "A Reliable Node-Disjoint Multipath Routing Protocol For MANET", International Journal of Computational Engineering Research, Vol. 03, Issue. 4, pp. 6, 2013.

[12] Jayshree Tajne, Veena Gulhane, "Multipath Node-Disjoint Routing Protocol to Minimize End To End Delay and Routing Overhead for MANETs", International Journal of Engineering Research and Applications (IJERA), Vol. 3, no. 4, pp.1691-1698, 2013.

[13] Priyanka Goyal, Sahil Batra, Ajit Singh, “A Literature Review of Security Attack in Mobile Ad-hoc Networks”, International Journal of Computer Applications. Vol. 9, No.12, 2013.

[14] Xu Yi, Cui Mei, Yang Wei, Xan Yin, “A Node disjoint Multipath Routing in Mobile Ad hoc Networks”, IEEE,2011.

[15] Liang Huang ,Fubao Wang, Guoqiang Yan, Weijun Duan, “An Efficient Dynamic Route Optimization Algorithm for Mobile Ad hoc Networks”, 2nd International Conference on Challenges in Environmental Science and Computer Engineering (CESCE 2011), Volume 11, Part A, PP.518–524, 2011. https://doi.org/10.1016/j.proenv.2011.12.082.

[16] S.Sharon Ranjini, G.Shine Let , “Security-Efficient Routing For Highly Dynamic MANETS “, International Journal of Engineering and Advanced Technology (IJEAT),vol 2, no. 4, 2013.

[17] Rajinder Singh, Parvinder Singh and Manoj Duhan ,"An effective implementation of security based algorithmic approach in mobile adhoc networks”, Human-centric Computing and Information Sciences, 2014.

[18] S.-J. Lee and M. Gerla, "AODV-BR: Backup Routing in Ad hoc Networks", In Proceedings of IEEE WCNC 2000, Chicago, IL, Sep. 2000. https://doi.org/10.1109/WCNC.2000.904822.

[19] Hamdy H El-Sayed., “Shortest paths routing problem”, Applied Mathematics & Information Sciences, Vol. 10, Issue. 5, pp. 1885-1891, 2016.

[20] Dr.Mohammed Ali Hussain, et al, “Energy Conservation Techniques in Ad hoc Networks”, International Journal of Computer Science and Information Technologies, Vol. 2, no. 3, pp. 1182-1186, 2013.

[21] S.J. Sultanuddin, et al, “An Efficient Approach For Countering Black Hole Attack In Manets “,International Journal of Computer and Electronics Research Vol. 2, no. 2, 2013.

[22] P. Suma, O. Nagaraju and Md. Ali Hussain, “Cost Optimal Random Path Selection Algorithm for Security in MANETS”, www.ijird.com, International Journal of Innovative Research and Development, ISSN 2278 – 0211 (Online), January, 2016, Vol 5 Issue 2.

[23] Dr. Seetaiah Kilaru, Hari Kishore K, Sravani T, Anvesh Chowdary L, Balaji T “Review and Analysis of Promising Technologies with Respect to fifth Generation Networks”, 2014 First International Conference on Networks & Soft Computing, ISSN: 978-1-4799-3486-7/14, pp. 270-273, August 2014.

[24] T. Padmapriya and V.Saminadan, “Improving Performance of Downlink LTE-Advanced Networks Using Advanced Networks Using Advanced feedback Mechanisms and SINR Model”, International Conference on Emerging Technology (ICET), vol.7, no.1, pp: 93, March 2014.

[25] S.V.Manikanthan and V.Rama“Optimal Performance Of Key Predistribution Protocol In Wireless Sensor Networks” International Innovative Research Journal of Engineering and Technology ,ISSN NO: 2456-1983,Vol-2,Issue –Special –March 2017.

[26] K.Srikar, M.Akhil, V.Krishna reddy “Execution of Cloud Scheduling Algorithms”, International Innovative Research Journal of Engineering and Technology ISSN NO: 2456-1983.Volume 2, Issue 4 June 2017. 108 -111.