International Journal of Research in Advent Technology, Vol.7, No.2, February 2019
E-ISSN: 2321-9637
Available online at www.ijrat.org

Analyzing the Performance of an Optimized Secure Cross Layer Routing Protocol with Secure Cross Layer Routing Protocols for Mobile Adhoc Networks

Amit A. Bhusari[1*],P.M. Jawandhiya[2], V.M.Thakare[3]
[1*]*Applied Science,PLITMS Buldana,SGBAU Amravati,India*
[2] *CSE,PLITMS Buldana, SGBAU Amravati India*
[3] *PGDCS,SGBAU Amravati,India*
aabhusari@gmail.com,pmjawandhiya@rediffmail.com,vilthakare@yahoo.co.in

Abstract: Cross layer based approaches is an emerging technique that annexes the new dimensions to MANET (Mobile Adhoc Network) by relaxing fixed layer boundary constraints. These new paradigm makes it possible to restrict the challenges such as low battery, limited bandwidth, link breakage of MANET. Still cross layer based designs are trying to liberate such barriers and trying to make MANET more adaptive. Though cross layer based designs are flexible and reliable, securing the network from malicious attack and optimizing network performance with security is definitely arduous task. This paper is to analyze the performance of Optimized and secure cross layer routing protocol (OSCLPC) and Secure Cross layer routing protocol over the AODV. We have designed and simulated MCLPC (Malicious cross layer based Power control) protocol to analyze the impact of attack on CLPC (Cross layer approach for power control). We defend the DoS attacks and blackhole, wormhole attacks by designing and simulating SCLPC (Secure cross layer based power control), security is imposed using AASR (Authenticated anonymous secure routing), but the network metrics as end to end delay and routing overhead are found disturbed. To optimize the network performance here we proposed OSCLPC (Optimized secure cross layer based power control protocol). The proposed OSCLPC has been evaluated using SHORT (Self healing and optimizing route technique). In this paper we have examined our proposed protocols OSCLPC and SCLPC with CLPC.

Keywords*:* Cross layer designs, CLPC, AODV

1. INTRODUCTION

Mobile adhoc network is a dynamic, decentralized and infrastructure less network used in various application viz. academics, disaster management, commerce, adversarial environments, health. Mobile nodes can have high speed and varying density that cause the networking threats to MANET. We have seen that researchers are gearing up their interest towards the Cross Layered architecture than traditional architecture as cross layer architectures are more scalable, easily interfaced with layers and providing QoS [1]. Though Cross layer based routing are providing better results, security of various cross layer based designs is a matter of thought [2]. Transmission power related issues can directly affect the various network parameters. We have designed SCLPC (Secure cross layer based power control protocol). We implemented security techniques in CLPC which uses AODV as a underlying (Cross layer approach based power control) protocol [3]. CLPC is cross layer based protocol uses RSS (Received signal strength) parameter from Physical layer. Every node computes the Avg_RSS of their neighbor's and constructs the communication regions as Maximum communication region, average communication region and minimum communication region. CLPC uses PHY-MAC-NET layer interaction with dynamic transmission power control mechanism to predict the link breakage. This mechanism helps to maintain node connectivity intact. At routing layer routing decision are made by selecting a node belonging to maximum communication region and possessing the maximum RSS value. In this CLPC we implement AASR protocol which hides all the routing details from the intermediate nodes. Anonymous communication means identities of source and destination nodes cannot be revealed to other nodes (Unidentified ability) also the link or traffic between source and destination cannot be recognized by any other node (Unlink ability) [4]. Nodes are aliased with pseudonym and we try to hide the identity of route, packets, source and destination. To defend any type of attacks and to prevent the intermediate nodes from modifying the packets,

RREQ packets are authenticated by group signature and key encrypted onion routing with route secret verification message is designed to prevent the intermediate nodes from inferring as destination. This SCLPC incurs the network overhead and delay. Hence to optimize the network performance parameter we proposed SHORT (self healing and optimizing route technique) method to design the OSCLPC. The reminder of the paper is organized as follows. The cross layer design CLPC and SCLPC is presented in section 3. Proposed optimized routing method for secure cross layer power control routing is discussed in section 4. Simulation results in section 5. Section 6 concludes the paper.

2. RELATED WORK

Optimization of routing protocols achieves the significant performance of protocol concerned with various network parameters. When we add security code to the protocol to prevent from intrinsic or extrinsic threats, security features increases the overhead and also enhances the end to end delay. Optimization tries to balance the network performance. More generally optimization technique enhances the performance of secure routing protocols or routing method. Chao Gui and Prasant Mohapatra designed a self healing and optimizing routing technique for adhoc network for both AODV and DSR protocol. They also evaluated the probability of existence of shorter path [5]. Gaurav Bhatia and vivek kumar proposed an adaptive retransmission algorithm for IEEE 802.11 MAC to reduce false link failures and predict node mobility [6]. Muhammed Asif Khan, Sahibzadaa Zakiuddin, Jalal Ahmad proposed optimization technique which uses EDCA parameter from MAC layer and decides routing path [7]. Zouhair El-Bazzal, Khaldoun El-Ahmadieh, Zaher Merhi, Michel Nahas and Amin Haj-Ali suggested cross layered routing protocol Turbo-AODV with PHY-MAC-NET layer interaction [8]. Sreedhar C, Dr. S. Madhusudana Verma, Dr. N. Kasiviswanatha proposed cross layer based secure routing protocol CSR-MAN which is again PHY-MAC-NET layer interaction[9]. Y.C. Hu and D.B. Johnson suggested route caching technique for on demand routing protocols for wireless adhoc networks [10].

3. SECURE CROSS LAYER BASED POWER CONTROL FRAMEWORK

Cross layer designs are emerging trends in wireless networks and various secure cross layer designs are available which have their own layering structure [11]**.** In CLPC nodes collects the RSS values from their neighbors using hello packets and using dynamic transmission power control mechanism every node calculates minimum RSS, Average RSS and Maximum RSS. Source generally selects the nodes with a min distance (1-hop) from it and having max RSS. Nodes with max RSS value are considered as more durable and reliable. These RSS from physical layer are interfaced to the network layer by MAC layer. And depending on RSS values the routing decision are made. The timely updated RSS value allows the node to modify the transmission power at the physical layer. In this each node calculates the Average of all its neighbors RSS as and define three threshold as

$$A\_RSS = \frac{\sum_{i=1}^{n} RSSi}{n}$$

$$A\_Min\_RSS = \frac{\sum_{i=1}^{Min\_node} RSSi}{Min\_node} \text{ where } RSSi < A\_RSS$$

$$A\_Max\_RSS = \frac{\sum_{i=1}^{Max\_node} RSSi}{Max\_node} \text{ where } RSSi > A\_RSS$$

Using these values every node determines the communication region and source nodes arrange the nodes regionwise based on node's RSS value. Source nodes broadcast the RREQ to nodes on Maximum communication region and intermediate nodes determines the RSS to decide weather or not to broadcast it to the next node. In the CLPC.CC we add the code for malicious behaviour and in tcl script. We simulate the normal CLPC against the CLPC with malicious code (MCLPC)

3.1 **MCLPC (CLPC WITH THE MALICIOUS BEHAVIOR*):*** In CLPC we add the code for malicious code and examined the network parameter using ns2.

```
CLPC::command(int argc, const char*const* argv) {
if(strcmp(argv[1], "attack") == 0)
{ malicious = true;
  return TCL_OK;
}}
/ /if I am malicious node
 if (malicious == true ) {
 drop(p, DROP_RTR_ROUTE_LOOP);
printf ("Malicious Attacker Active in current round....!\n" );
}
```

We proposed the anonimity based secure cross layer routing protocol (SCLPC). We have attemped to implement AASR (Authenicated Anonymous secure routing) with CLPC. We also used Onion routing

protocol concept to map RREQ to RREP as authenticated path for source and destination. Also AASR uses all the cryptographic concepts while securing the routes, packets and nodes in the MANETs.

3.2 Sceure Cross layer based Power Control Protocol SCLPC:

Protocol Design: The routing process of AASR can be summarized as follows:

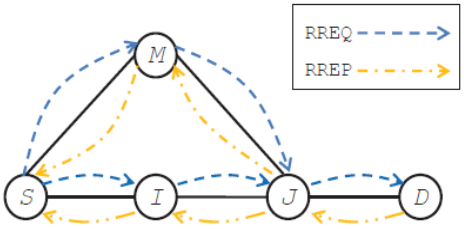


Figure1 AASR Network Architecture

During the route discovery, a source node broadcasts a RREQ packet in the format

$S \rightarrow * : [RREQ; Nsq; V_D; V_{SD}; Onion(S)]G_S$-Where Nsq- Sequence no. of RREQ,
V_D – Encrypted message for request validation at destination.
V_{SD}-Encrypted message for route validation at intermediate nodes.
Onion(s) - key encrypted onion created by S.
If an intermediate node receives an RREQ packet, it verifies the RREQ packet by using its group public key. And add one layer on top of the key encrypted onion as

Onion (I) = OK_{SI} (N_I ;Onion(S)). The process will continue till packet reached to the destination or expires.Once the RREQ packet is received and verified by the destination node, the destination node assembles the RREP packet in following format and broadcast it back to the source node.

$D \rightarrow * : (RREP ; Nrt; Kv; Onion(J)K_{JD})$

On the reverse path back to the source, each intermediate node validates the RREP packet and updates its routing and forwarding table, then it removes the one layer on the top of the key encrypted onion and continues broadcasting RREP in the form

$J \rightarrow * : (RREP ; Nrt; Kv; Onion(I)K_{IJ})$

When source node receives the RREP packet, it verifies the packet and updates its routing and forwarding table.

Lastly source node starts data transmission in the established route format,

$S \rightarrow D: (DATA; Nrt; (Pdata)K_{SD})$

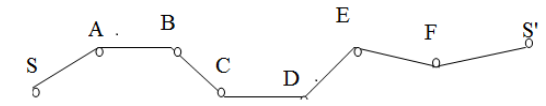
AASR protocol uses time stamps and sequenece numbers which can more precisely used to detect the network layer attacks like blackhole and wormhole.As the sequenec number determine the freshness and time stamps records the time when the RREQ was flooded in the network. These parameters can efficiently able to identify and mitigate the attacks on network layer and other DOS attacks.

3.3 **Onion Routing:** It is secured way of communication private services over public network. Onion core is developed and signed by the sender node for RREQ. During a RREQ phase, each forwarding node go on embedding encrypted layer to the route request message. It is not necessary for source and destination node to know the identities of intermediate forwarding node. The destination node receives the onion and delivers it along the route back to the source. The intermediate node can verify its role by decrypting and deleting the outer layer of the onion. Eventually an anonymous route can be established. AASR method adopts a key-encrypted onion to record a discovered route and design an encrypted secret message to verify the RREQ-RREP linkage. Group signature is used to authenticate the RREQ packet per hop, to prevent intermediate nodes from modifying the routing packet. Extensive simulations are used to compare the performance of AASR to that of ANODR, a representative on-demand anonymous routing protocol. The results show that, it provides more throughput than ANODR under the packet-dropping attacks, although AASR experiences more cryptographic operation delay. AASR suffering from the worst delay performance. Hence this is main research problem for this thesis work.

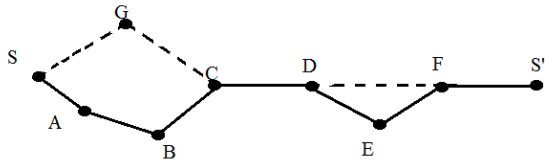
4.PROPOSED OPTIMIZED ROUTE METHOD TO SECURE CROSS LAYER BAESD POWER CONTROL ROUTING PRTOCOL MECHANISM USING ANONYMOUS ROUTING

Proposed SHORT (self healing and optimizing routing tecnique) is a packet delay aware AODV

based method and try to reduce the number of hops without any routing overhead [13]. It discovers the short and secure path with our approach. SHORT method can be summarised as follows. The basic scenario of the shortcut discovery process is shown in Figure 2. The hop-count (HC) field is initialized to zero at the source node and gets incremented by one at every hop the packet takes. This information is maintained as an array termed as the hop comparison array. Each of the elements of the array has an expiration time after which they are invalidated. Consider a routing path from a source node S to a destination node S' as shown in figure 2(a). This initial path is determined through the path discovery process, and the packet takes 7 hops while getting routed from S to S'. Due to the mobility of nodes consider the routing path as shown in fig. 2(b). With this, G is in the maximum communication region of S and C node. The current routing path is shown by the solid lines in the figure. Hence the new route is formed in which number of hops reduced from 7 to 5 as showing in figure 2(c)



INITIAL PATH 2*a*



PATH EVALUATED BY SHORT 2*b*

NEW PATH *2 c*

4.1 Algorithm for Short Process:

Step 1: When node i receive or overhear a packet P, IF the node i is the final destination address, consume the packet. GOTO END;

Step 2: (Assume P belongs to $<SA_k,DA_k>$ flow.) Compare $<SA_k,DA_k>$ (Pseudonyms) to all the valid entries in the hop comparison array;

Step 3: IF there is no match with the entries, store $<SA_k,DA_k,HC_k,NA_k>$ in the hop comparison array;

Step 4: IF the packet is destined to i as the next-hop node,process the packet for forwarding further.

Step 5: (Assume that it matched with an entry $<SA_k,DA_k,HCj,NAj>$)

IF ($HCk - HCj > 2$), a short-cut is found, node i do the following:

Step 5.1: Send a message to NAj to update the routing table such that the next hop address for destination node DAk is modified to the address of node i;

Step 5.2: Modify its routing table by making the next-hop address for destination DAk as NAk;

Step 5.3: Modify its hop comparison array, delete the entry corresponding to $<SA_k,DA_k>$;

Step 6: Return the delay efficient path.

Step 7: Stop

Hence using SHORT process we can ensure optimized and secure routes for data transmission between nodes. We refer this routing as OSCLPC (optimized and secure cross layer based power control) routing. It provides secure route because

a. It selects the nodes to broadcasts the route messages to nodes from maximum communication region having max RSS (CLPC).

b. In this cross layer based protocol we implemented security by using anonymous routing [14-15] and named it as SCLPC (Secure cross layer based power control).

c. lastly we implement SHORT process to minimize the end delay and to lower down the routing overhead for on demand cross layer based routing protocol. [16].

5. SIMULATION RESULT

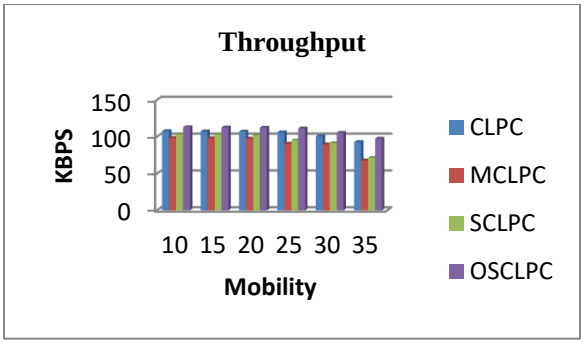
We simulate our OSCLPC and SCLPC in ns-2 [21], with following network configuration.

TABLE 1

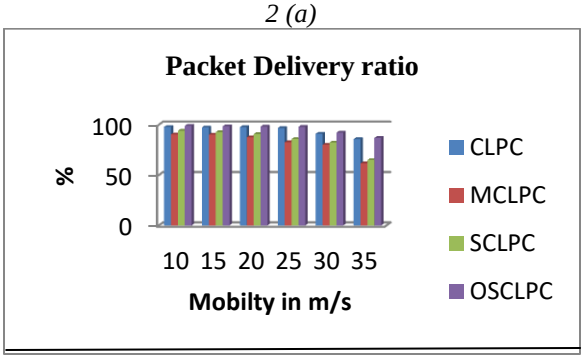
Network parameters	Range
Speed	10–35 m/s
Load	20% network size
Packet rate	4 Packets/s
Topography	1000 * 1000
Max propagation range	250 m
Receiver sensitivity (Min RSS)	90 dBm (Milli watts in decibel)
Mac protocol	IEEE 802.11
Routing protocol	AODV,OSCLPC
Packet size	512 bytes
Transport layer protocol	UDP
Application	CBR (constant bit rate)
Simulation time	80 s
Node density	100–200

We have simulated the network metrics as packet delivery ratio, throughput, end to end delay and

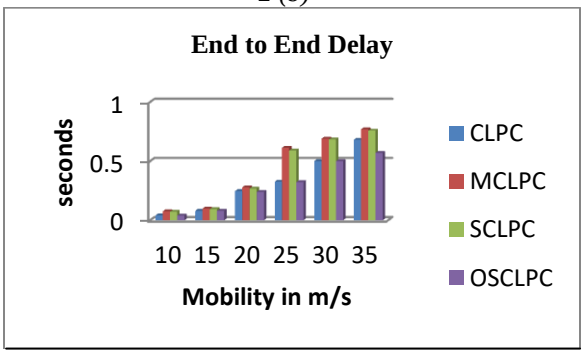
routing overhead metrics for measuring the performance of OSCLPC against SCLPC for varying mobility and density. We have shown the comparative analysis of CLPC (Cross layer based power control protocol) ,MCLPC (Malicious CLPC) , SCLPC (Secure the cross layer power control routing protocol) and OSCLPC (Optimized and secure cross layer routing Protocol)



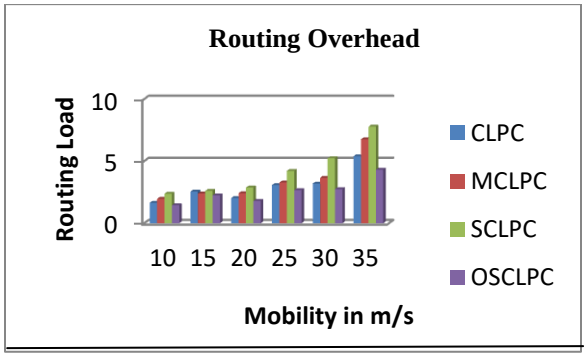
2 (a)



2 (b)

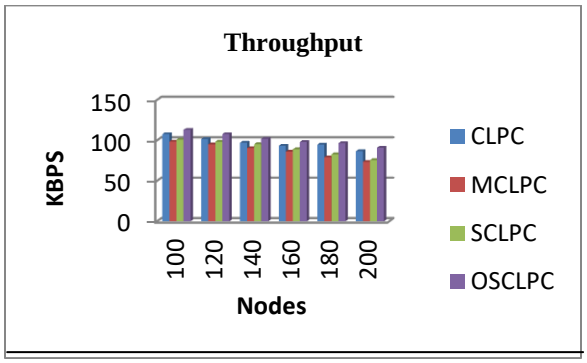


2 (c)

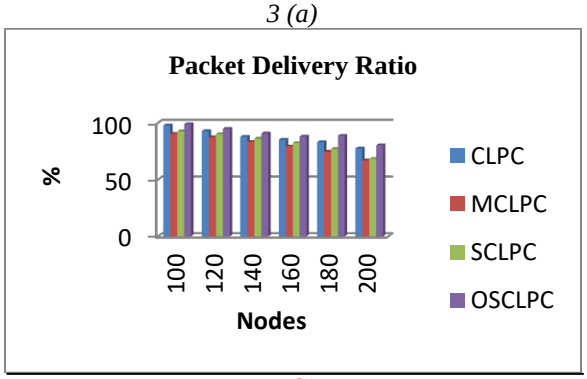


2 (d)

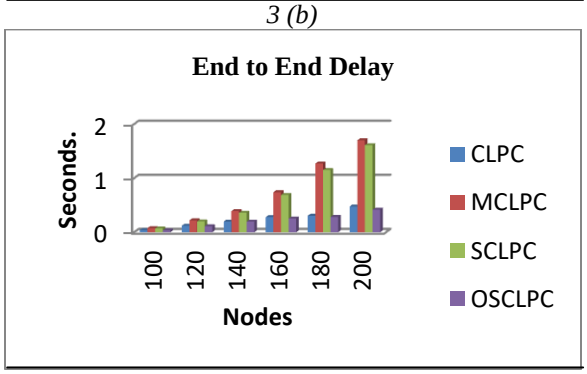
Similarly the metrics comparison for AODV, OSCLPC and MOSCLPC is as follows. Here we assume the mobility as 10m/s.



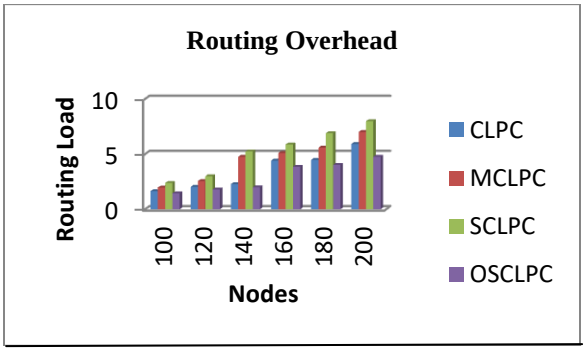
3 (a)



3 (b)



3 (c)



3 (d)

As we discussed in earlier section OSCLPC is an optimized secure routing protocol for power control mechanism using cross layer design [17]. In this paper we compare all the cases for cross layer based routing protocol, with and without security. As shown in the diagram we consider CLPC protocol as an existing protocol. CLPC protocol has better simulation results over AODV for the network metrics packet delivery ratio, end to end delay and routing overhead because of its dynamic transmission power control mechanism. RSS has been used as cross layering parameter from physical to network layer as reliable routing technique. Then we simulate MCLPC by adding malicious attacking script in CLPC. Simulation results for various network metric shown performance of network seriously affected due to packet dropping attack and it clears the necessity to secure the cross layer approaches [18]. We proposed SCLPC which implements AODV based AASR protocol and provides the security to network. But on applying the security the network appears with increased delay and routing overhead. To optimize the network metrics we further proposed the SHORT algorithm which is delay aware AODV based and provides the security along with balanced performance. Clearly it can be noticed that fig. 2(a) to 2(d) and 3(a) to 3(d) our approach OSCLPC is certainly simulating the results better than AODV, CLPC, MCLPC and SCLPC. MCLPC, SCLPC and OSCLPC are our proposed protocols which we have simulated on base protocol CLPC to analyze the need for securing the cross layer designs against any threats for both mobility and density scenario. In MOSCLPC we have added malicious code in OSCLPC to check how OSCLPC performs for any intrinsic or extrinsic threat. Our simulated protocols are performing and enabling the secure transmission of data without disclosing any identity. The comparative performance analysis clearly justifies that OSCLPC performs better than AODV for all network parameter under malicious attack. Thus our proposed approach not only mitigates the attack but also do not allow degrading the network performance. The interesting feature of OSCLPC is at first stage it uses nodes to forward the RREQ from maximum communication region. The nodes with maximum RSS is considered as most reliable to forward the data. At second stage we imposed the security to packets, routes, source and destination using anonymous routing. We named it as SCLPC and in our previous work we compared our SCLPC (Secure cross layer based power control protocol) with Malicious CLPC i.e. MCLPC. At third stage we know that added security lower down the delay and routing overhead parameter and thus we implemented optimize technique using self healing which dynamically reduces the number of hops to the destination. Whole process of route discovery and data transmission is totally secure and incurs no extra routing overload [20].

6. CONCLUSION

CLPC is dynamic transmission power control protocol and can perform route estimation with possible route failure. Its cross layer approach makes it more flexible than AODV. But CLPC lower down its performance under threat. Hence here we first proposed the security scheme using AASR routing and onion routing that makes CLPC strong against attacks but this added security imbalance the network metrics like end to end delay and routing overhead. To balance such metrics we further implemented SHORT method which is delay awareness and AODV based. OSCLPC is an optimized secure cross layer based power control protocol which has been designed to provide QoS for MANET base application. The simulation results show that our proposed approach SCLPC and OSCLPC are doing well and providing the security as well as optimized behavior over CLPC. Hence our designed approach OSCLPC is optimized and can defend the attacks strongly for mobility and density oriented networks.

REFERENCES

[1] Vineet Srivastava, Mehul Motani “Cross-layer design: A survey and the road ahead” communication Magazine, IEEE, Vol:43, Issue:12, Issue Date:Dec, 2005.
[2] Amit A. Bhusari,P.M Jawandhiya, V.M. Thakare “Anonymity based secure cross layer routing protocol for Mobile Adhoc Networks” IEEE Xplore, October 2018
[3] A. Sarfaraz Ahmed, T. Senthil Kumaran, S. Syed Abdul Syed, S. Subburam “Cross layer Design

Approach for Power control in Mobile Adhoc Networks" Egyptian Informatics Jouran 2015.

[4] Wei liu and Ming Yu "Authenticated Anonymous secure routing for Manets in adversarial environments" IEEE transactions on vehicular network, March 2014

[5] Chao Gui and Prasant Mohapatra " A self healing and optimizing routing technique for adhoc networks", Dept of Computer science, Davis, CA 95616.

[6] Gaurav Bhatia and Vivek Kumar" Adapting MAC 802.11 for performance optimization of MANET using cross layer interaction" International Journal of Wireless & Mobile Networks (IJWMN) Vol.2, No.4, November 2010

[7] Muhammed Asif Khan, Sahibzadaa Zakiuddin, Jalal Ahmad "Cross layer optimization of Dynamic source routing protocol using IEEE 802.11e based medium awareness" 978-1-4673-5885-9/13 IEEE 2013.

[8] Zouhair El-Bazzal, Khaldoun El-Ahmadieh, Zaher Merhi, Michel Nahas and Amin Haj-Ali " A Cross layered protocol for Ad hoc networks" 2012 international conference on Information technology and e-services 978-1-4673-1166-3/12

[9] Sreedhar C, Dr. S. Madhusudana Verma, Dr. N. Kasiviswanatha "Cross layer based secure routing in Manet" International Journal of Engineering Research and Applications, ISSN : 2248-9622, Vol. 3, Issue 5, Sep-Oct 2013, pp.725-731

[10] Y.-C. Hu and D. B. Johnson, "Caching Strategies in On- Demand Routing Protocols for Wireless Ad Hoc Networks", Proc. ACM International Conference on Mobile Computing and Network (MOBICOM), 2000

[11] S Bose and A.Kannan "Detecting Denial of Service Attacks using Cross Layer based Intrusion Detection System in Wireless Ad Hoc Networks" IEEE-International Conference on Signal processing, Communications and Networking Madras Institute of Technology, Anna University Chennai India, Jan 4-6, 2008. Pp]82-188

[12] Pradip M. Jawandhiya, Mangesh m.Ghonge, DR. M.S Ali and Prof.J.S Deshpande "A Survey of Mobile adhoc network attacks" IJEST,Vol.2, No.9, Sep 2010

[13] C. Perkins, E. Belding-Royer, S. Das, *et al.*, "RFC 3561 - Ad hoc On Demand Distance Vector (AODV) Routing," Internet RFCs, 2003.

[14] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila,"Towards a taxonomy of wired and wireless anonymous Networks," in *Proc.IEEE WCNC'09*, Apr. 2009.

[15] J. Kong, X. Hong, and M. Gerla, "ANODR: An identity-free and ondemand routing scheme against anonymity threats in mobile adhoc networks," *IEEE Trans. on Mobile Computing*, vol. 6, no. 8, pp.888–902, Aug. 2007.

[16] Ju-Lan Hsu and Izhak Rubin, "Cross Layer On-Demand Routing Algorithms For Multi-Hop Wireless CSMA/CA Networks," 978-1-4244-2677-5/08 IEEE 2008.

[17] R. Madhan Mohan, K. Selvakumar, "Power controlled routing in wireless ad hoc networks using cross layer approach", Egyptian Informatic Journal, Vol.13,Issue:2,July 2012,Pages:95-101.

[18] Azza Maohammed, Boukli Hacene Sofiane and Faraoun Kamel Mohamed "A Cross layer for detection and ignoring blackhole attack in Manet" IJCNIS, 2015,10,42-49 5,Sep-2015

[19] M. B. Pursley, H. B. Russell and S. Wysocarski, "Energy efficient transmission and routing protocols for wireless multiple hop networks and spread spectrum radios", Proceedings of EUROCOMM Conference, pp. 1−5, 2000

[20] Amit A. Bhusari, Dr.P.M Jawandhiya, Dr.V.M. Thakare "Performance analysis of an optimized and secure routing protocol with impact of malicious behavior utilizing cross layer designs for Mobile Adhoc Networks" published in International journal of computer sciences and engineering (IJCSE), Volume 6, Issue 6 June 2018. eISSN:2347-2693.

[21]NS2NetworkSimulator.http://www.isi.edu/nsnam/ns/