JCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

Performance Analysis of an Optimized and Secure Routing Protocol with impact of malicious behavior utilizing Cross Layer Design 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

Available online at: www.ijcseonline.org

Accepted: 10/Jun/2018, Published: 30/Jun/2018

Abstract: Cross layer based approaches has given new dimensions to MANET (Mobile Adhoc Network) by releasing fixed layer boundary constraints. These new paradigm makes it possible to limit the issues such as low battery, limited bandwidth, link breakage of MANET. Still cross layer based designs are trying to remove such barriers and trying to make Manet more scalable. Though cross layer based designs are flexible but securing the network from malicious attack is definitely challenging task. This paper is an attempt to discuss about technique to optimize the performance of secure cross layer routing protocol. We have designed SCLPC (Secure cross layer based Power control) protocol. But when security is imposed using AASR (Authenticated and anonymous secure routing), the network metrics as end to end delay and routing overhead is 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). We also examined the OSCLPC with malicious code. The OSCLPC and M-OSCLPC (malicious OSCLPC) is simulated in ns2 and we also compared it with reactive routing protocol AODV.

Keywords: Cross layer designs, CLPC, AODV

I 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 secure cross layer power control routing is discussed in section 4. Simulation results in section 5. Section 6 concludes the paper.

II 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].

III 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

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

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

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

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

A. PROTOCOL DESIGN: a) S store following entries in RREQ

TABLE 1

Dest.Nym.	***Dest.Str***	***Dest. Pub Key***	***Session Key***
N_D	Dest	K_{D+}	K_{SD}

Where N_D - Pseudonym of Destination,
Dest :Destination binary string,
K_{D+} : Destination Public key,
$K_{SD:}$Symmetric key for Source & Destination

b) Source then broadcast RREQ containing above information and signed by S with its group signature private key
$S \rightarrow * : [RREQ; Nsq; V_D; V_{SD}; Onion(S)]G_{S-}$
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.

c) $V_{SD} = (N_v)K_v$
Where N_v is one time nonce generated by S for Destination D for route verification,
K_v is symmetric key

d) The secret message V_D is defined as

$$V_D = \langle N_v; K_v; dest\rangle K_{SD}, \{K_{SD}\}K_{+}$$

e) Onion(S) can be defined as Onion(S) = $O_{K_v}(N_s)$,
Where N_S is on time generated nonce and encrypted by Symmetric key which will only be decrypted at destination. Source generates core of onion and every intermediate node go on encrypted layer with its symmetric key.

f) After sending the RREQ, S creates new entry in routing table as

TABLE 2

Req. Nym	***Dest.Nym.***	***Ver. Msg.***	***Next hop***	***Status***
N_{sq}	N_D	V_{SD}	N/A	Pending

g) Every intermediate node maintains neighborhood table. E.g. from fig. 1 we can see that node I is neighbor of node S and J. Then neigh borer table of I is

TABLE 3

Ngh_Nym	***Session key***
N_S	$K_{S,I}$
N_J	$K_{I,J}$

From neighborhood table I knows that RREQ packet is received from neighbor S. As RREQ is received by node I from node S, Node I decrypts RREQ by applying its group public key and determine sequence number N_{sq}. If sequence number is not updated in routing table than it is considered as fresh RREQ and hence it can be retransmitted to other node. Also we are using timestamp to check whether the RREQ with seq. no is already generated. If Seq. no. is exist in routing table but with old timestamp then it is already processed RREQ and will be ignored. If sequence no. exist but with fresh time stamp then it is considered as malicious [12]. It is to be noted that intermediate nodes cannot decrypt V_D and V_{SD} they only can encrypt onion(S) sent by source S and put their group private signature key.
Onion(I) = OK_{SI} (NI ;Onion(S)).
Intermediate nodes will broadcast the RREQ as
I → * : [RREQ; Nsq; V_D; V_{SD}; Onion(I)]GI-

h) At Destination, when RREQ is received, D decrypts it by using public group signature key. And validates V_D and using Symmetric key K_{SD} it decrypts V_{SD}.

i) Destination D creates RREP as

D → * : (RREP ; N_{rt}; ⟨K_v;Onion(J)⟩K_{JD})

Where Nrt is route pseudonym generated by D
K_{JD} is symmetric key stored in neighborhood table of node J , J Decrypts onion and from neighborhood table it forwards the RREP to next node I.
J will verify the linkage of the received RREP with its stored RREQ. It tries to use the obtained *Kv* to decrypt the verification message V_{SD} stored in its routing table. Once *J* finds the matched V_{SD}, it will update the corresponding routing entry as follows:

TABLE 4

Req. Nym	***Dest.Nym.***	***Ver. Msg.***	***Next hop***	***Status***
N_{sq}	N/A	V_{SD}	N_D	Active

j) When RREP reached at source, it validates the route as

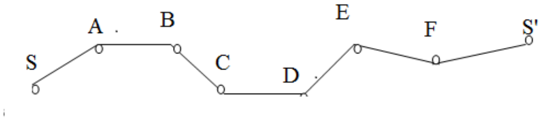
TABLE 5

Req. Nym	***Dest.Nym.***	***Ver. Msg.***	***Next hop***	***Status***
N_{sq}	N_D	V_{SD}	N_I	Active

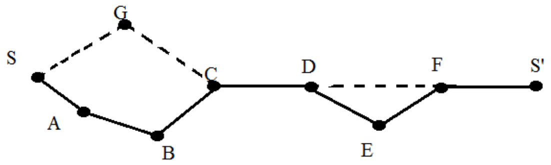
Now *S* can transmit the data to *D*. The format of the data packet is defined as follows:
S → D: (DATA; N_{rt}; ⟨P_{data}⟩K_{SD}) where Nrt is the route pseudonym. When we compared SCLPC with CLPC we evaluated it better but end to end delay and rouitng overhead parameter were with extended values. To reduce the delay and overhead we then proposed OSCLPC which uses SHORT process to find the secure and optimal path between source and destination.

IV.PROPOSED OPTIMIZED AND SECURE CROSS LAYER BAESD POWER CONTROL ROUTING PRTOCOL MECHANISM USING ANONYMOUS ROUTING

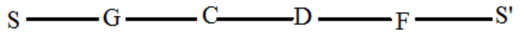
Proposed SHORT (self healing and optimizing routing tecnique) is a packet delay aware AODV based method and try to reduce the number of hops without any routing overhead [13]. It discovers the short and secure path with our approach. SHORT method can be summarised as follows. The basic scenario of the shortcut discovery process is shown in Figure 1. 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 1. (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. 1(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 1 (c). The example is analyzed in steps as follows



INITIAL PATH *1a*



PATH EVALUATED BY SHORT *1b*



NEW PATH *1 c*

A. ALGORITHM FOR SHORT PROCESS:

Step 1: When node i receives or overhears a packet P, IF the node i is the final destination address, consume the packet. GOTO END;
Step 2: (Assume P belongs to <SAk,DAk> flow.) Compare <SAk,DAk> (Pseudonyms) to all the valid entries in the hop comparison array;
Step 3: IF there is no match with the entries, store <SAk,DAk,HCk,NAk> 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 <SAk,DAk,HCj,NAj>)
IF (HCk − HCj > 2), a short-cut is found, node i does 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 <SAk,DAk>;
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].

B. M-OSCLPC (OSCLPC WITH THE MALICIOUS BEHAVIOR): In OSCLPC we add the code for malicious code and examined the network parameter using ns2.

```
OSCLPC::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" );
}
```

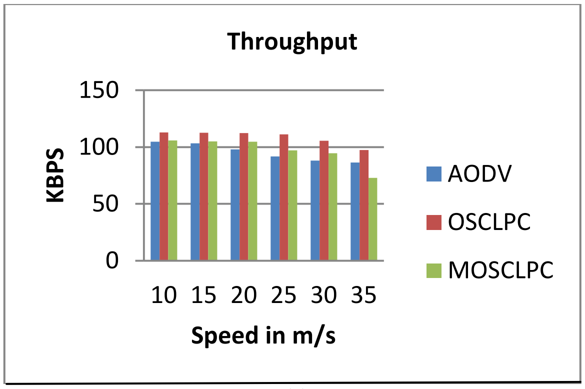
V. SIMULATION RESULT

We simulate our OSCLPC and also m-OSCLPC in ns-2 [17], with following network configuration.

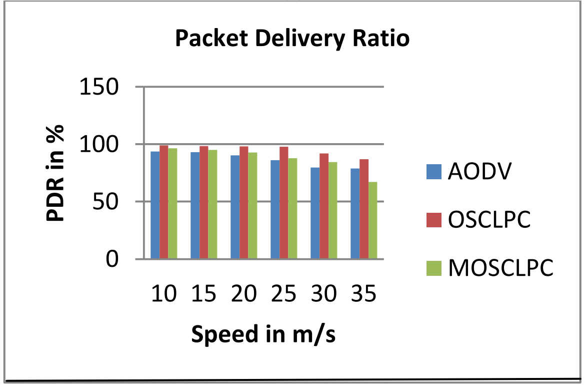
TABLE 6

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

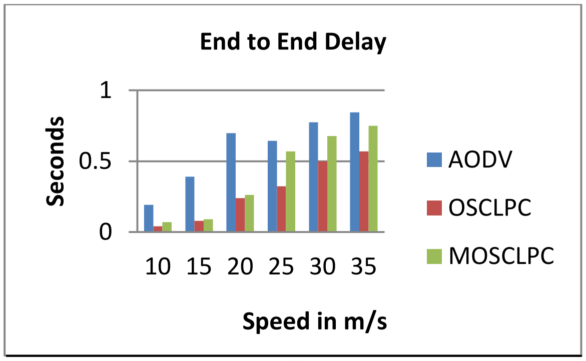
We have evaluated PDR, throughput, delay and overhead metrics for measuring the performance of OSCLPC and M-OSCLPC for varying mobility and density. We compared these results with reactive routing protocol AODV. Following are the graphs for four different metrics with varying mobility in m/s with 100 numbers of nodes.



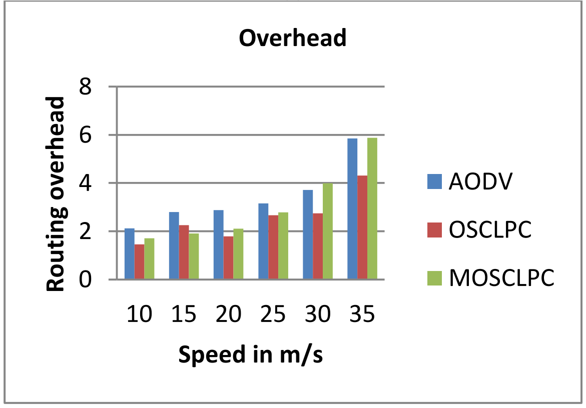
2 (a)



2 (b)

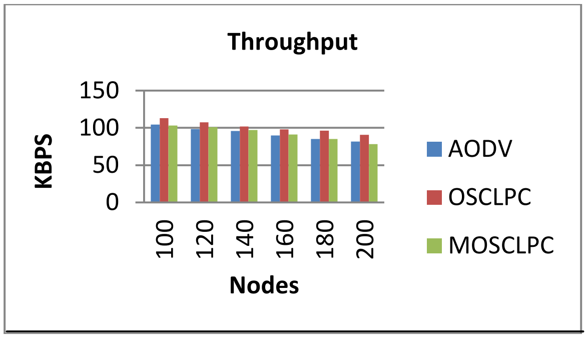


2 (c)

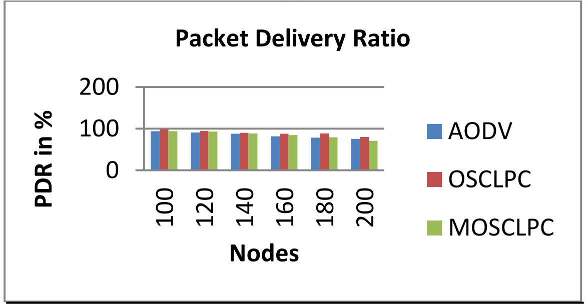


2 (d)

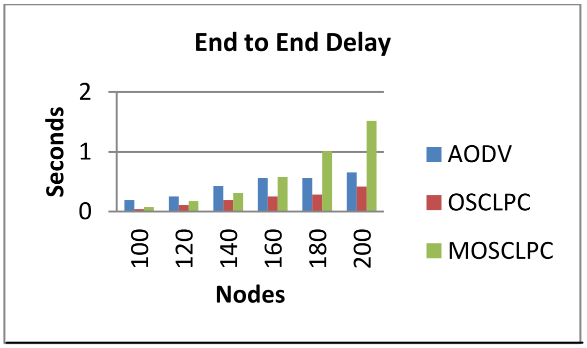
Similarly the metrics comparison for AODV, OSCLPC and MOSCLPC is as follows. Here we assume the mobility as 10m/s.



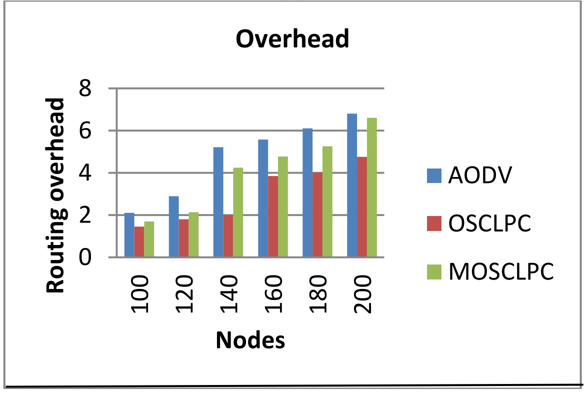
3 (a)



3 (b)



3 (c)



3 (d)

As we discussed in earlier section OSCLPC is an optimized and secure routing protocol for power control mechanism using cross layer design. MOSCLPC is malicious OSCLPC, attacking behavior on OSCLPC protocol. As shown in the diagram we simulate and compared the OSCLPC and MOSCLPC with AODV. 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 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 and when we simulate and compared it with AODV, we found it is giving the optimum performance. Our simulated protocols are performing and enabling the secure transmission of data without revealing 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.

VI. CONCLUSION

OSCLPC is an optimized and secure cross layer based power control protocol which has been designed to defend the problems such as power transmission and link breakage of MANET. Again we aimed to keep whole process secure and for this we added security using anonymous routing. The simulation results show that our approach is naturally doing better than AODV. More interestingly we again allowed our OSCLPC with malicious attack and as we can see in the graphs that MOSCLPC also on an average performing well to that of AODV. Hence our designed approach OSCLPC is optimized and can defend the attacks strongly for mobility and density oriented networks.

VII. REFERENCES

[1] Vineet Srivastava, MehulMotani "Cross-layer design: A survey and the road ahead" communication Magazine, IEEE, Vol:43, Issue:12, IssueDate:Dec, 2005.

[2] Amit A. Bhusari,Dr. P.M Jawandhiya "Review and classification of Cross layer Routing protocol for Manet" IEEE sponsored 3rd ICECS 2016,Coimbatore,pp 600-607

[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 Aliand 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 OnDemand Distance Vector (AODV) Routing," Internet RFCs, 2003.

[14] D. Kelly, R. Raines, R. Baldwin, B. Mullins, and M. Grimaila,"Towardsa 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]NS2NetworkSimulator.http://www.isi.edu/nsnam/ns/

Author Profiles

Amit A. Bhusari is working as an Asst. Professor at PLITMS Buldana. He is M.C.A. and M.Sc. (Maths) graduate and is pursuing his PH.D. in computer science & Engg. He has 10 years of teaching experience. He has published his papers in national and international journals. His area of research is wireless network and security.

Dr.Pradip M. Jawandhiya is Principal at Pankaj Laddhad Institute of technology and management studies buldana since 5 years. He is B.E., M.E. Ph.D. qualified. He has more than 23 years of teaching experience. He has presented and published many papers in national and international journals. He is life member of I.S.T.E.;C.S.I. and Fellow of I.E.T.E., Member IEEE, Member IACSIT. His research interest is computer networking and security, image processing and big data.

Dr. V.M. Thakare is working as Professor & Head in Computer Science, Faculty of Engineering & Technology, Post Graduate Department of Computer Science, SGB Amravati University, Amravati. He has published more than 100 papers in various National & International Conferences & 30 papers in various International journals. He is working on various bodies of Universities as a chairman & members. He has guided around 300 more students at M.E / MTech, MCA M.S & M.Phil level. He is a research guide for Ph.D. at S.G.B. Amravati University, Amravati. His interest of research is in Computer Architecture, Artificial Intelligence and Robotics,Database.