CBDAT: Cross Layer Based Detection and Authentication Technique for MANET

K.Suresh Babu
Research Scholar
School of IT
JNT University Hyderabad, India.

K.Chandra Sekharaiah
Professor in CSE
School of IT
JNT University Hyderabad, India

Abstract
Mobile adhoc networks (MANETs) are prone to many security attacks and risks due to its characteristics such as mobility, lack of infrastructure and dynamic topology changes. In this paper, we propose CBDAT, a cross layer based detection and authentication technique for MANET. Our technique defines the observer node to monitor the neighbor transmissions and to compute the trust values. The observer node is elected considering residual energy, node degree and stability information. The trust value is protected using message authentication code (MAC). The estimated trust value is used for selecting the best path among the multiple paths between the source and the destination pairs. The selected path information is forwarded to Media Access Control (MAC) layer to allocate access time. The MAC layer distinguishes each node in the path by their trust value. While transmitting data in the selected path, the MAC grants more access time for the nodes with high trust value. Our technique proficiency is proved by the simulation results. It precludes more security attacks and improves system performance.

Keywords:
mobility, trust values, MAC, access time

1. Introduction

1.1 Mobile Adhoc Network(M ANET)

An impermanent and infrastructure less network which contains group of wireless mobile nodes is termed as wireless adhoc network[1]. Mobile Ad Hoc Networks (MANETs) are autonomous network and it offers multihop connectivity among mobile nodes. It is a kind of wireless adhoc network and is a self-configuring network of mobile routers connected by wireless links – the union of which forms an arbitrary topology[20].Dynamic topology changes, lack of central controller and limited resources in terms of power and bandwidth are the features of the ad hoc networks. [2] The mobile nodes are well found with a wireless radio, a processor, memory and a power source. [3] MANET has its own merits and demerits for its unique characteristics. [4] MANET has wide range of applications from military network to home network. It is also utilized in conference meetings, office networks and crisis response, etc [5] .

1.2 Security Threats and Attacks in MANET

The characteristics of MANET such as infrastructureless network, mobility of nodes, closure communication medium, lack of centralized control and frequent topology changes brings more security risks in the network. The use of wireless links makes MANETs susceptible to attack[9]. Similarly, the nature of MANET complicates the user authentication process, which disallows the unauthorized users from accessing the network. [7] Since, MANET is a wireless network; security is entirely different from many fixed hardwired networks. Attacks can be occurred at any node from any direction. Therefore, every mobile node in the network must be equipped with security mechanisms.
Mobile nodes in the network can be attacked by malicious nodes both from inside and outside of the network. Isolating individual malicious node in adhoc network is a daunting task. A secure mechanism is needed, which prepares each node that it should not trust any node without authentication. To cope with this, a distributed architecture can be utilized to attain high availability. This prevents serious attack caused by compromised central entity, which introduce dangerous attack overall network. [8] When nodes in the network compromised or attacked from malicious nodes, it requires alternative path selection or retransmission of packets. This recovery process could cause delays in the network. [6].

1.3 Cross Layer Approach

Traditionally all the networks follow the layering architectures like ISO-OSI Model, TCP/IP Model, etc. In which each layer provide its own functions and gives services to the upper or below layers. These are strictly layered architectures. Each layer implements a specific service: the architecture forbids direct communication between non-adjacent layers, while the communication between adjacent layers works by using standard interfaces. Cross-layer design breaks away from traditional network design, where each layer of the protocol stack operates independently and exchanges

Manuscript received July 5, 2013
Manuscript revised July 20, 2013

information with adjacent layers only through a narrow interface[21]. In the cross-layer approach information is exchanged between non-adjacent layers of the protocol stack, and end-to-end performance is optimized by adapting each layer against this information Cross-layering is not the simple replacement of a layered architecture, nor is it the simple combination of layered functionality: instead it breaks the boundaries between information abstractions to improve end-to-end transportation. The Cross Layering has the following features.

- *By giving out and distributing information on multiple layers, cross layer approach becomes an efficient mechanism to deal with traffic in the network. Further, the information gathered in a layer can be used in other layers to regulate the performance of the protocol. [10]*
- *Using cross layer architecture, protocols are aware of their network current state from the point of local node. Further, Quality of Service (QoS) of applications can be enhanced by cross layer approach. [11]*
- *The overall performance of adhoc networks like wireless sensor network (WSN), mobile adhoc network (MANET) and wireless mesh networks (WMN) are enriched using cross layer architecture. [12]*
- *It resolves many open issues in MANET by sharing network information in multiple layers while still maintaining separate layers. [13]*

1.4 Organization of the Paper

In this paper we propose a novel cross layer techninue CBDAT, a cross layer based detection and authentication technique for MANET, that detects the malicious nodes in the network and also provides the authentication by using the various metrics form physical layer, data link layer and network layer. We investigate the mechanism by implementing the required changes on the existing routing protocol AODV. The simulation is performed using the NS-2 simulator. The rest of the paper is structured as follows. In section 2, the need of cross layer and problem is identified. In section 3, the cross layer based detection and authentication for manet is proposed. In section 4, the results of the simulation are discussed. In section 5, the conclusion and scope for future work are presented.

2. Problem Identification

A cross layer based adaptive real-time routing attack detection system for MANETS (CARRADS) is proposed in [14]. It used support vector machine (SVM) algorithm for detecting routing misbehaviors. This method is not feasible in resource-constrained ad hoc network nodes. It has maintain all the routing patterns and maintain the routing behaviours.It has not considered the dynamic abnormalities found in the process of routing.Moreover, it does not provide any authentication mechanism for validating the reports.In [15], Arjun P. Athreya et al. have presented cross layer based routing mechanism and it is used only for establishing multiple paths rather than security. Abderrezak Rachedi et al. [16] have introduced a cross layer monitoring process. However, it does not provide any authentication mechanism for validating the nodes. In addition, no suitable mechanism for selecting the monitoring nodes is discussed. To alleviate all above-mentioned problems and to introduce a new technique for security in this paper, we propose to design a CBDAT: cross layer based detection and authentication technique for MANET.

3. CBDAT: Cross Layer Based Detection and Authentication Technique for MANET

3.1 Overview

CBDAT is a cross layer based mechanism to detect the malicious nodes and to provide the authentication in MANETs. It gathers various features from the bottom three layers of the OSI model, by providing cooperation between the layers. Based on this features, the CBDAT tries to provide the security to the mobile adhoc network. In this technique, after deploying nodes in the network, using the physical layer, each node measures its residual energy, link stability and node degree. Based on these measurements, the observer node is selected. The observer node is responsible for estimating trust value for its neighbors by monitoring the transmissions. Each individual node also maintains its trust value. It periodically broadcasts the computed trust values to all its neighbors. By receiving this broadcasted information, each node updates its trust value. At network layer, using AODV protocol, during route discovery process, the trust value is appended in the RREQ packet. In order to protect the trust value from attacks, each intermediate node computes message authentication code (MAC) using its shared key with destination node. While receiving RREQ packet, the destination updates the trust value considering success and failure of authentication. This updated trust values are sent back to the source using RREP packets. The source obtains multiple paths to the destination and selects the path with high trust value. Then, the source forwards the selected path information to the MAC layer for access time allocation. The MAC layer differentiates each node by their trust value and allocates more access time for the nodes with high trust value.

3.2 Estimation of Metrics

3.2.1 Calculation of Residual Energy of a Node

Initially every node has got some initial energy to operate in the network. Most of the times it is charged to its maximum capacity. To perform the communication and control operations, every node consumes energy. The residual energy of a node at an instance of time is the total energy left out with the node after certain amount of time, i.e., the difference between the initial energy of the node and the consumed energy by the node.

Let the number nodes deployed on the network is n. After time(t) is elapsed, the total energy consumed by node i (where i = 1,2,3,….n) is given by

$$C_E(i) = T_p * \varpi + R_p * \vartheta \quad \textbf{(1)}$$

Consider that initial energy of node i is IE (i), then the residual energy (R) of node (i) at time t is,

$$R(i) = I_E(i) - C_E(i) \quad \textbf{(2)}$$

If residual energy of a node becomes zero, then the mobility and the operations of the node become null.

Notations	Description
C_E (i)	Total energy consumed by node i
T_P	Total number of packets forwarded by node i after time t
R_P	Total number of packets received by node i
ϖ	$0 \leq \varpi \geq 1$
ϑ	$0 \leq \vartheta \geq 1$
I_E (i)	Initial enery of the node i

Table 1: Description of the notations

3.2.2 Computation of Link Stability

The consistency of the link between two communicating nodes is called as Link Stability. It is an important metrics in analyzing the MANETs. As the MANETs are more prone to change its topology/network dynamically, the link stability between two nodes also changes more dynamically. The stability of the link is given as,

$$S_L = \frac{R}{d} \quad \textbf{(3)}$$

Notations	Description
S_L	Stability of the link
R	Transmission range of the nearest Access point
D	Distance between two nodes

Table 2: Description of the notations

3.2.3 Measurement of Node Degree

Every node in the network is surrounded by different nodes. Hence every node has to have information about their neighboring nodes based on which it can judge whether the node is genuine or malicious. Number of neighboring nodes that surrounds a node is known as node degree and it is represented as DN.

D_N → No. of neighboring nodes (4)

Notations	Description
D_N	Node degree

Table 3: Description of the notations

3.3 Selection of Observer Node

To select the observer node from the deployed n nodes in the network, each node broadcasts Nw_Dis (Network Discovery) message to all its neighbors. On receiving the Nw_Dis message, each node computes its residual energy, stability of the link and node degree that connects its neighbor using the Equations – 2, 3, 4 respectively. After calculating the metrics and updation, it then forwards back to the node. The Nw_Dis message takes the following format:

Sending Node ID	Neighboring Node ID	Sequence Number	Residual Energy (R)	Link Stability (S_L)	Node degree (D_N)

Table 4: Nw_Dis, Network Discovery Message Format

Each node waits for time t to receive all possible Nw_Dis messages from all the other nodes. After the expiration of time t, using the Nw_Dis messages each node constructs neighborhood table.

Neighboring Node	Neighboring Node ID	Residual Energy (R)	Link Stability (S_L)	Node Degree (D_N)
B				
C				
D				
…				
…				

Table 5: Neighborhood Table for node A

It computes the cumulative value for residual energy, link stability and node degree, called Absolute Value of a node A [Abs(A)]. It is computed as

$$\textbf{Abs(A)} = \sigma R + \upsilon S_L + \tau D_N \quad \textbf{(5)}$$

Notations	Description
S_L	Stability of the link
R	Transmission range of the nearest Access point

D_N	Node degree
Abs(A)	Absolute Value of a node A
Σ	Normalizing constant
Y	Normalizing constant
T	Normalizing constant

Table 6: Description of the notations

The absolute values calculated at each node is transmitted to all other neighboring nodes. The node that has high absolute value (Abs) is chosen as Observer Node (O).

Observer Node(O) ⟹ ***MAX{Abs(A), Abs(B), Abs(C)…….}*** **(6)**

For example, in the Figure-1, consider the nodes A, B, C and D in the network. The transmission range of nodes is represented in the form of circles. By estimating the absolute value of nodes, node B is selected as the observer node (O). We can observe that node B has more stability in terms of transmission range, node degree and distance between their neighbors.

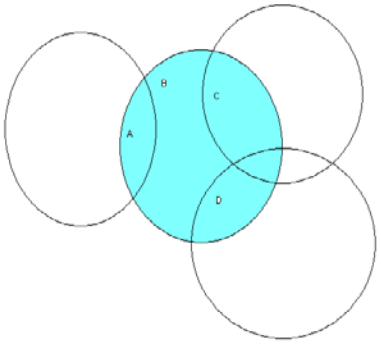

Figure-1 Observer Node Selection

3.4 Computation of Trust values of Nodes

The node O i.e., node B observes the neighbors transmission and computes trust value for its neighboring nodes. The observer (O) estimates the trust value as a ratio of amount of packets observed by the observer to the amount of successful transmission between the observer and the observed node. The trust value is symbolized as,

$$Tr = nOP / nSP \quad (7)$$

Notations	Description
Tr	Trust value of a node
nOP	Number of packets observed by the observer
nSP	Number of successful transmission between the observer and observing node

Table 7: Description of the notations

Node ID	Sequence Number	Hop Count	Trust value (Tr)

Table 8 : Header T-table

The observer node O keeps track of the neighbors trust value in a table, called Trust Table (T). The T- Table Header is shown in table-8.

We assume that, in addition to the T- table, the observer node periodically broadcasts the trust value of nodes to all its neighbors. Each node updates its trust table according to the broadcasted information of observer.

3.4 Authentication Scheme

The trust value present at each node is used in deciding whether the node is malicious or not. As the RREQ and RREP packets are appended with trust value, it must be protected and authenticated by intermediate nodes between the source and the destination. For the authentication the modified secure AODV algorithm proposed by us [22] is used. In this technique, during deployment, each node shares a key with other nodes called mutual key (Mkey.). This key is used by the nodes to secure control packets and to authenticate trust value of nodes.

Let S be the source node and D be the destination node
Let I_1 I_2, I_3... I_n be the set of intermediate nodes between source and destination
Let T_1, T_2, T_3 …T_n be the trust values of nodes I_1 I_2, I_3 ... I_n respectively

$$S \xrightarrow{RREQ[S,D,H,Tvalue]} I_1$$

$$I_1 \xrightarrow{RREQ[S,D,H,MAC(T1)SignI1]} I_2$$

$$I_2 \xrightarrow{RREQ[S,D,H,MAC(T1),MAC(T2),SignI1,SignI2]} I_3$$

$$I_n \xrightarrow{RREQ[S,D,H,MAC(T1),MAC(T2),MAC(T3)...MAC(Tn),SignI1,SignI2,SignI3...SignIn]} D$$

Figure-2 Sequence of steps of RREQ Authentication Process

On receiving all possible RREQ packets, the destination authenticates trust value of nodes by verifying its signatures. To perform this authentication and verification, the destination uses Mkey of corresponding nodes. While authenticating trust values, if any intermediate node fails authentication, then its trust value is decremented by 1. For successful authentication, the destination increments the trust value by 1.

Let D be the destination and T_i is the trust value of node n_i
1. D authenticates n_i
2. If authentication is successful
Then
  2.1 $T_i = T_i + 1$
3. Else if authentication is failed
Then
  3.1 $T_i = T_i - 1$
End if

Figure-3 Algorithm for Trust value Updating at Destination

By completing the authentication process, the destination node computes MAC for updated trust values. (i.e) MAC (T1, T2, T3, … Tn) using its Mkey with the source node. This updated trust value is appended in the RREP packet and it is digitally signed by the destination. Finally, the RREP packet is sent back to the source node through the reverse path of RREQ packet. While the RREP packet traversed in the reverse path, each intermediate node looks for its id in the route table. Then it validates the destination by verifying the digital signature. If the destination is not a valid node, then it drops that RREP packet. Otherwise, it signs the RREP packet and forwards to its neighbor.

1. If destination is valid
Then
(1.1)The intermediate node sign the RREP packet
(1.2)The intermediate node forwards RREP packet to the next node
2. Else if destination is invalid
Then
(2.1)The intermediate node drops the RREP packet
End if

Figure-4 Algorithm for RREP Packet Traversing

$$D \xrightarrow{S,D,MAC(T1,T2...Tn)(I1,I2,...In)SignD} I_n$$

$$I_n \xrightarrow{S,D,MAC(T1,T2...Tn)(I1,I2...In)SignD,SignIn} I_{n-1}$$

$$I_{n-1} \xrightarrow{S,D,MAC(T1,T2...Tn)(I1,I2..In)SignD,SignIn,Signn-1} I_1$$

$$I_1 \xrightarrow{S,D,MAC(T1,T2...Tn)(I1,I2...In)SignD,SignIn,Signn-1...SignI1} S$$

Figure-5 Sequence of steps of RREQ Authentication Process

On receiving the RREP packet, the source authenticates the digital signatures of all intermediate nodes and the destination. It then recomputes MAC using destination Mkey and derives trust values of nodes. .

3.5 Path Selection

From the derived trust values for all nodes, the source calculates aggregate trust value for each path. It is estimated as,

$$TP_i = T_S + T_i + T_{i+1} + \ldots + T_D \qquad (4)$$

Here, TPi symbolize the trust value of path Pi, TS and TD denotes trust values of source and destination respectively. Ti, Ti+1 are the trust values of intermediate nodes. When multiple paths are available for the same destination, the routing layer selects a path with high trust value. The trust values of the nodes along the selected path are forwarded to the media access control (MAC) layer by the source node. The MAC distinguishes each node by their trust value. While transmitting data in the selected path, the MAC grants more access time for the nodes with high trust value.

4. Simulation Results

The proposed mechanism is simulated using NS-2 simulation tool. The performance analysis of CBDAT mechanism is done and is compared with the CARRADS technique.in the simulation we have varied the number of nodes as 10,50,100 and 200. In our experiment we vary the number of attackers as 1,2,3,4 and 5. The metrics considered for analysis are end-to-end delay, packet delivery ratio, packet drop and resilience. The simulation results are presented in the graphs.

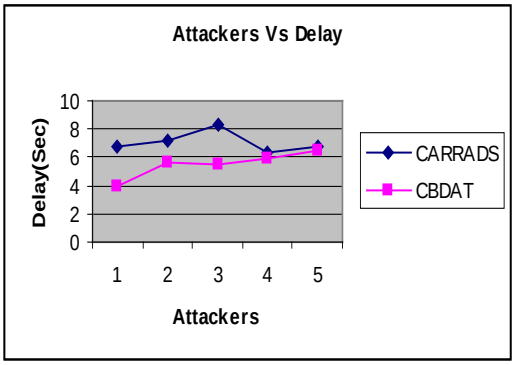

Figure-6 Attackers Vs Delay

From Figure-6, we can see that the end-to-end delay of our proposed CBDAT is less than the existing CARRADS protocol.

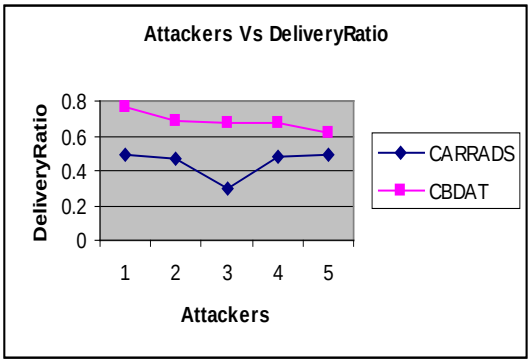

Figure-7 Attackers Vs Delivery Ratio

From Figure-7, we can see that the delivery ratio of our proposed CBDAT is higher than the existing CARRADS protocol.

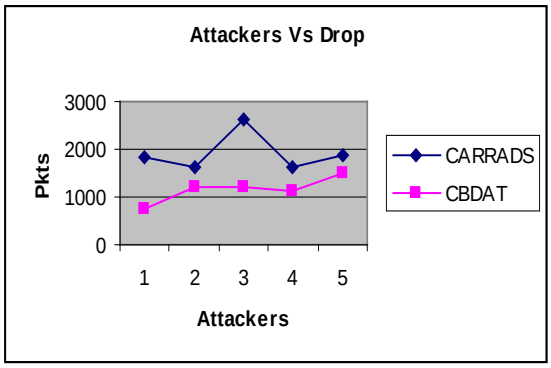

Figure-8 Attackers Vs Drop

From Figure-8, we can see that the packet drop of our proposed CBDAT is less than the existing CARRADS protocol.

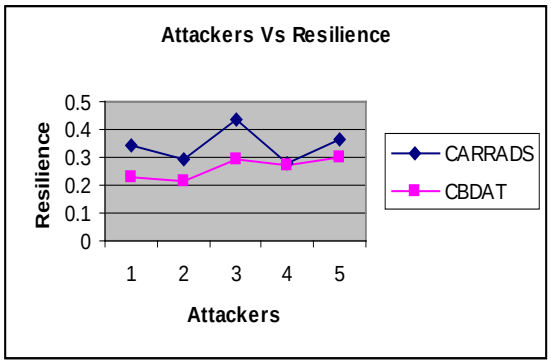

Figure-9 Attackers Vs Resilience

From Figure-9, we can see that the resilience ratio of our proposed CBDAT is less than the CARRADS protocol.

5. Conclusion and Future Scope

In this paper, we have proposed a cross layer based detection and authentication technique in MANET. Our technique defines the observer node to monitor the neighbor transmissions and to compute the trust values. During route discovery process, the trust value is appended in the RREQ packet. In order to protect the trust value, each intermediate node computes message authentication code (MAC) using its shared key with destination node. The estimated trust value is used for selecting multiple paths between the source and the destination pairs. The selected path information is forwarded to Media Access Control (MAC) layer to allocate access time. The MAC layer distinguishes each node by their trust value. While transmitting data in the selected path, the MAC grants more access time for the nodes with high trust value. From the simulation results it is proved that it has got better metrics. This technique proficiency is proved by the simulation results. It precludes more security attacks and improves system performance.

References

[1] Wei Wei and Avideh Zakhor, "Interference Aware Multi-Path Selection for Video Streaming in Wireless Ad Hoc Networks" IEEE Transactions on Circuits and Systems for Video Technology, Volume-19, Issue-2, Digital Object Identifier- 10.1109/TCSVT.2008.2009242, pp- 165-178, 2009

[2] Hwee Xian TAN and Winston K. G. SEAH, "Dynamic Topology Control to Reduce Interference in MANETs" In proceedings of 2nd International Conference on Mobile Computing and Ubiquitous Networking, Osaka University Convention Centre, Osaka, Japan, 2005.

[3] Pascal von Rickenbach, Stefan Schmid, Roger Wattenhofer, Aaron Zollinger, "A Robust Interference Model for Wireless Ad-Hoc Networks" 19th IEEE International Symposium on Parallel and Distributed Processing, Digital Object Identifier: 10.1109/IPDPS.2005.65, Publication Year: 2005

[4] Kousha Moaveni-Nejad, Xiang-Yang Li, "Low-Interference Topology Control for Wireless Ad Hoc Networks" Ad Hoc & Sensor Wireless Networks, 2005 – Citeseer

[5] R. P. Ramos, M. Geandre R.ego, Tarciana Lopes, R. Baldini Filho and C. de Almeida, "Interference Evaluation in CDMA Ad Hoc Networks" IEEE International Conference on Telecommunications Symposium, Digital Object Identifier: 10.1109/ITS.2006.4433411, pp-967 – 970, Publication Year: 2006

[6] Tanu Preet Singh, Manmeet Kaur and Vishal Sharma, "Automated Recovery Based Power Awareness (ARPA) Algorithm for MANETs" International Conference on Circuits, System and Simulation (IPCSIT) vol.7, 2011

[7] K.K.Lakshmi Narayanan and A.Fidal Castro, "High Security for Manet Using Authentication and Intrusion Detection with Data Fusion", International Journal of Scientific & Engineering Research Volume 3, Issue 3, March -2012 1 ISSN 2229-5518

[8] A.Rajaram, Dr.S.Palaniswami, "A Trust-Based Cross-Layer Security Protocol for Mobile Ad hoc Networks" International Journal of Computer Science and Information Security, (IJCSIS) Vol. 6, No. 1, 2009

[9] K.Suresh Babu, K.Chandra Sekhariah, "Mobile Ad-Hoc Networks: A Novel Survey", *International Conference On Advanced Computing And Communication Technologies For High Performance Applications, FISAT, COCHIN, September 24-26' 2008, Vol. 1, Page.262-269.*

[10] Jyoti Jain, Mehajabeen Fatima, Dr. Roopam Gupta and Dr. .K.Bandhopadhyay," An Overview and challenges of routing protocol and MAC layer in Mobile Ad hoc network" Journal of Theoretical and Applied Information Technology© 2005 - 2009 JATIT.

[11] Eleonora Borgia, Marco Conti, and Franca Delmastro, "MobileMAN: Design, Integration, and Experimentation of Cross-Layer Mobile Multihop Ad Hoc Networks" IEEE Communications Magazine, Volume: 44 , Issue: 7 Digital Object Identifier: 10.1109/MCOM.2006.1668386, pp- 80-85, 2006

[12] Amardeep Singh and Gurjeet Singh, "Security in Multi-hop Wireless Networks" International Journal of Computer Science and Technology (IJCST) ISSN: 0976 – 8491, 2011
[13] Noureddine Kettaf, Hafid Abouaissa, Thang Vuduong† and Pascal Lorenz, "A Cross layer Admission Control On-demand Routing Protocol for QoS Applications" International Journal of Computer Science and Network Security, (IJCSNS) VOL.6 No.9B, September 2006
[14] John Felix Charles Joseph , Amitabha Das b, Bu-Sung Lee and Boon-Chong Seet , "CARRADS: Cross layer based adaptive real-time routing attack detection system for MANETS", Elsevier Computer Networks, 2010
[15] Arjun P. Athreya and Patrick Tague," Towards Secure Multi-path Routing for Wireless Mobile Ad-Hoc Networks: A Cross-layer Strategy" 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Digital Object Identifier: 10.1109/SAHCN.2011.5984886 , pp- 146 – 148, 2011
[16] Abderrezak Rachedi and Abderrahim Benslimane, "Toward a cross-layer monitoring process for mobile ad hoc networks", Wiley Inter Science, security and communication networks Security Comm. Networks, Published online in (www.interscience.wiley.com), 2008
[17] M. Shao, S. Zhu, G. Cao, T. La Porta and P. Mohapatra "A Cross-layer Dropping Attack in Video Streaming over Ad Hoc Networks," International Conference on Security and Privacy in Communication Networks (Securecomm), 2008
[18] Vinay Rishiwal, S. Verma and S. K. Bajpai, "QoS Based Power Aware Routing in MANETs", International Journal of Computer Theory and Engineering, Vol. 1, No. 1, April 2009
[19] S.Muthuramalingam and R.Rajaram, "A Transmission Range Based Clustering Algorithm for Topology Control MANET", International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.3, September 2010
[20] K.Suresh Babu, K.Chandra Sekhariah, B.Sasidhar, "Issues Related to Routing and Security in Mobile Adhoc Networks", CI-4.7, *International Conference Systemics, Cybernetics and Informatics ICSCI-2009, January 07-10 2009*
[21] K.Suresh Babu, K.Chandra Sekhariah, "Cross Layer Based Security in Manets", *International Journal of Advanced Research in Computer Science(IJARCS), INDIA*, page 57-60, Vol. 4, No.4, May 2013.
[22] K.Suresh Babu, K.Chandra Sekhariah, "*Securing AODV With Authentication Mechanism Using Cryptographic Pair Of Keys", International Journal of Computer Science and Information Security (IJCSIS)*, USA, Vol 11 No. 2, pp 42-45, February 2013.