Dynamic Authenticated Route for Risk Attacks in Ad Hoc Networks

[1.] C. Chandra Prabha, [2.] Dr. K. Karthikeyan
[1.] Research Scholar, Dr. SNS Rajalakshmi College of Arts and Science,Coimbatore, India.
[2.] Head, Department of Information Technology, Dr. SNS Rajalakshmi College of Arts and Science,Coimbatore, India.

***Abstract*— Ad-hoc networks are utilized to setup wireless communications in today's environment for more advanced infrastructure. It has become more essential for large places to centralize the main point to authorize and authenticate with the changing nature of network topology. The risk aware response needs risk estimation and prevention techniques which cause no negative impacts during the process of routing operations. A new dynamic approach for routing attacks with an intrusive node and the separate identification of the routing attacks. This gives active response for more assurance for risk identity responses. It prevents malicious nodes in the utilization within the network and detects nodes which act in different manner. There are number of attacks that can be used to manipulate the routing in an ad-hoc network. The protocol, named Dynamic Authenticated Routing (DAR) for Ad-hoc networks, uses encrypting mechanisms to defeat all identified attacks. This DAR mechanism detects and protects malicious actions by third parties and peers. It also introduces authentication, message integrity and non repudiation to routing in an ad-hoc environment a part of a minimal security policy.**

I. INTRODUCTION

The overall goal of the security solutions for ad-hoc networks is to provide security services including authentication, confidentiality, integrity, anonymity and availability to the mobile users. In order to achieve to this goal, the security solution should provide complete protection spanning the entire protocol stack. In ad-hoc networks, only focus on the network layer, which is related to security issues to protect the ad-hoc routing and forwarding protocols. From the security design perspective, the ad-hoc has no clear line of defense. Unlike wire networks that have dedicated routes. Each mobile node in ad hoc networks may function as a router and forward packets for other peer nodes. For mobile ad-hoc networks, the issue of routing packets between any pair of nodes becomes a challenging task because the nodes can move randomly within the network.

II. RELATED WORK

The Intrusion Detection System (IDS) gives an attack alert with a confidence value [15] and then Routing Table Change Detector (RTCD) runs to find out the number of changes on routing table are caused by the attack. Risk assessment gives an alert [6] from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Trust-based clustering algorithm was proposed [22] and it defines in-depth analysis of trust-based clustering schemes and illustrates the integration of reputations. They were compared with various trust metrics and finally conclude with open research issues. The Light-Weight Authentication Model was used [16] as a security model for low-value transactions in ad-hoc networks. They focused on authentication in core requirement for commercial transactions. They delivered a survey of various existing models and analyze them in terms of scope and applications.

The "BBCMS" clustering algorithm was proposed [24] and the algorithm defines overall network which is divided into clusters and cluster head is connected by virtual networks. The establishment of the "temporal order" events [11] which is used to structure (or order) the algorithm's reaction to topological changes. They referred to the protocol as the Temporally-Ordered Routing Algorithm (TORA).

The trust establishment methods and the defense mechanisms [20] were introduced for the effectiveness of the attacks and detecting malicious nodes in MANETs. They summarized the roles of trust and the core design issues of trust establishment mechanisms in a distributed network. The mechanism of Trust Enhanced Security Architecture for Manet (TEAM) was proposed [21] in which a trust model is overlaid on the security models such as key management mechanism, secure routing protocol, and cooperation model. They were presented the operation of the architecture, system operation of the novel trust and cooperation model, which is Secure MANET Routing with Trust Intrigue (SMRTI) for security purpose. Securing Ad-hoc routing protocols was proposed [2] and they were incorporated security mechanisms into routing protocols [23] for ad hoc networks. Using AODV [10] they developed a security mechanism to protect its routing information. The techniques would also be applicable to other similar routing protocols and the management of key could be used in conjunction with the solution.

III. PROPOSED WORK

A. Dynamic Authenticated Route Mechanism

Dynamic authentication route is a new scheme with cost efficient and reliable intrusion techniques. The protocol, named Dynamic Authenticated Routing (DAR) for Ad-hoc networks, uses encrypting mechanisms to defeat all identified attacks. This DAR mechanism detects and protects against malicious actions by third parties and peers. It also introduces authentication, message integrity, and non repudiation to

routing in an ad-hoc environment, a part of a minimal security policy.

B. Dynamic Authenticated Route Discovery

Dynamic routing uses a dynamic routing protocol to automatically select the best route to put into the routing table. So instead of manually entering static routes in the routing table, dynamic routing automatically receives routing updates, and dynamically decides which routes are best to go into the routing table. Dynamic authenticated routing (DAR) is reflected in the various administrative distances assigned to routes from dynamic routing. These variations take into account differences in reliability, speed of convergence and other similar factors.

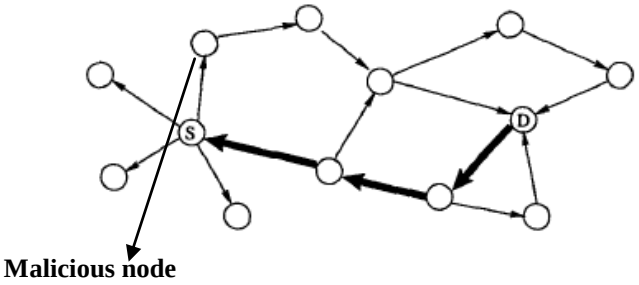

Figure 1. Identification of malicious node scenario

In the above figure, the malicious node is identified, which is neighbor to the source node S with the help of routing table updates from the source to destination. Finally the destination use reversed path to send acknowledgement to the source node.

C. Route Maintenance

A link break occurs when two nodes on a path are no longer in transmission range. If an intermediate node detects a link break when forwarding a packet to the next node in the route path, it sends back a message to the source notifying it of that link break. The source must try another path or do a route discovery if it does not have another path. There are few problems which DAR needs to detect and successfully overcome it. They are collision problems between the nodes. A malicious node sends incorrect route request again and again which causes interruption to the route path. In the previous techniques of routing attacks, it does not detect the misbehaving node but it only detects which node has threshold bandwidth while forwarding a packet.

In DAR, the misbehaving or malicious node is detected during route discovery and the authentication is verified with all the neighboring nodes for transmission of data. Even if DAR does not have the information of hops in route path, it prevents a malicious or broken node from broadcasting a packet to non- existent node. Each node maintains a rating for every other node it knows about in the network. Once a node detects a link failure for the next hop or receives a route request from a neighbor for one or more active routes, a route request message is generated and broadcasted to all upstream neighbors. Later, when a node detects a link failure, or receives a message from a neighbor for one or more active routes, it will send a route request for all unreachable destinations sharing the same next hop with the shared asymmetric key, corresponding source and destination sequence number list in the same route request message. The upstream nodes extract the information needed from the various lists to reconstruct the authenticated route path and to verify the authentication instantaneously.

D. Shortest route path discovery

Source node S and its neighbor node have got a route with quickest time and hence it has dynamic route path for the forwarding of data packets. S initiates a route discovery by broadcasting a route request packet to its neighbors that contains the destination address D. The neighbors in turn append their own addresses to the route request packet and rebroadcast it. This process continues until a route request packet reaches D. D must now send back a route reply packet to inform S of the shortest discovered route. Since the route request packet that reaches D contains a path from S to D, D may choose to use the reverse path to send back the reply or to initiate a new route discovery back to S. Since there can be many routes from a source to a destination, a source may receive multiple route replies from a destination.

E. Encryption technique for risk attacks

Between two nodes, a shared asymmetric key is given for encrypting two or more nodes in the route path for dynamic authentication. If an attacker gains access to the network, they can masquerade as a router on the network to either gain information about the network or disrupt network traffic. If a high quality firewall is configured, it will help the network security and stop many of this type of threat.

All nodes in the route path keeps track on the authentication and authorization whether the nodes are active. Even if there is no traffic occurs, the error message generated in the route path is signed and is forwarded along the path towards the source without any changes. Since error messages and route request messages are securely authenticated and signed, DAR prevents malicious node to create or generate error messages for other nodes. If a node generates more number of error messages, it is then avoided and the source node keeps way for another alternative route path for more security and integrity.

F. Certificate X.509

Risk attacks in Ad hoc routing are due to malicious nodes which cause network traffic. By giving certification to the nodes in the network which has routing optimizations and help in end- to- end authentication. The routing messages are authenticated end-to-end and only authorized nodes participate at each hop between source and destination. Each node will receive an authentication certificate where it avoids attacks from external or inside hackers.

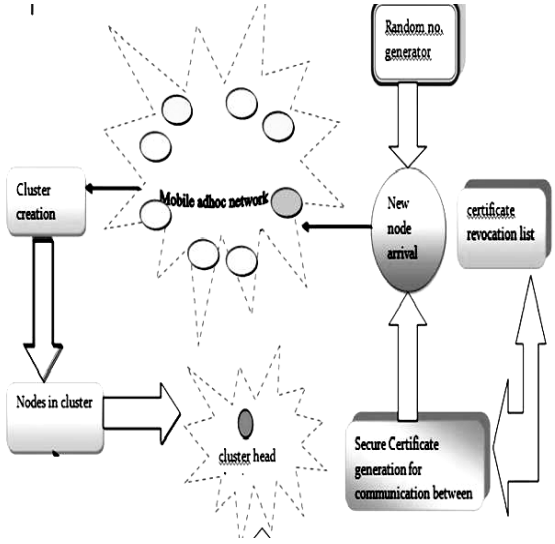

Figure 2. Certificate X.509 architecture

In the above figure, X.509 Certificate which is used for authentication of ad-hoc networks and the new arrival node. Every node gets the certificate from the Certificate Authority (CA). Only the certificate owners can forward data and allow only authorized participants to route in their path and verify until the message reaches the destination.

G. Dar Attack Model

DAR Attack model includes a major advantage of a simple method to protect data where a shared encrypted key can be used by two neighbor nodes. Attacks from the authorized neighbors in case of invalid or expired certificate can be tracked and prevented by attaching individual certificates for nodes within the route path and verify until the message reaches the destination. Also choosing shortest path for transmission can prevent tunneling attacks in between the route.

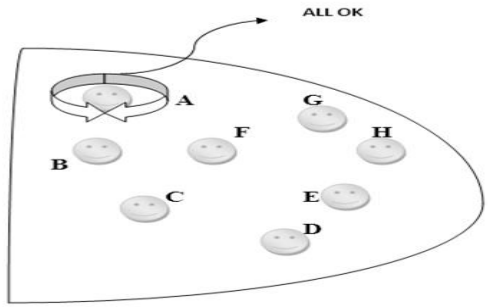

Figure 3. Dynamic authenticated route model

In the above figure, A, B, C, D, E, F, G, H are the nodes in a route path. When source node passes information with clear certificate and shared asymmetric key with B, it easily diagnoses, if B is a malicious node. Likewise node B easily diagnoses its neighbor C, C –D, E-F, F-G and finally G-H.

The valid certificates to each and every node in the route path process can prevent the effective attack of sending unnecessary route requests. If a node is found to be malicious, a route message is passed to the route nodes and the source node provides an alternate shortest route path and then transmits the data packet.

Attackers cannot decrease the hop count value, but they can still attempt to commit another type of fraud where they transmit or forward routing messages they receive directly, without incrementing the hop count value. In order to prevent such “same hop count fraud", the node identity should be encoded into the hash values to form an authenticator. Consequently, each node cannot forward routing messages with authenticators encoded with another node's identity, and they must increase the hop count. For small networks, each node can encode its identity directly, and no adversary can derive its value from neighbor’s values that correspond to the same hop count.

H. Optimized Clustering Algorithm (OCA)

This algorithm is a secured weight-based clustering algorithm allowing more effectiveness, protection and trust in the management of cluster size variation. It includes security requirements by using a trust value and each node is trusted by its neighborhood, and using the certificate as node’s identifier to avoid any possible attacks. OCA elects cluster-head according to its weight computed by combining a set of system parameters (Stability, Battery, Degree … etc). It is divided into number of modules like clustering, cluster head election criteria and the X.509 certificate which are being used for authentication of node in the present research work. A node id is assigned to each node by using Random number Generator. After this, overall ad hoc network is divided into cluster and each cluster have its own Cluster Head (CH). There are different number of parameters are used to elect the cluster head of cluster.

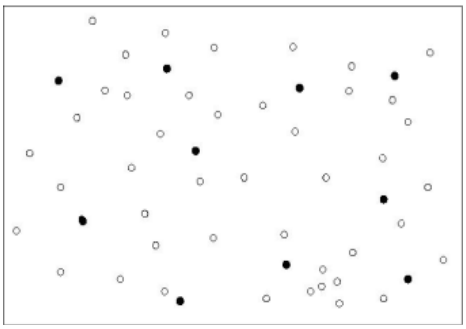

Figure 4. Cluster Heads Identification

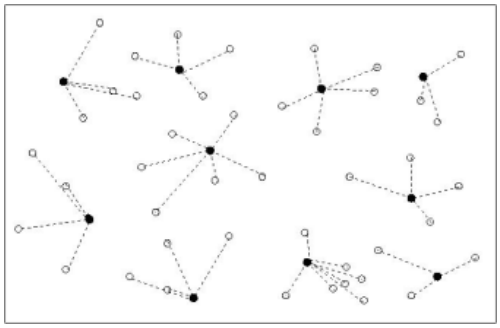

Figure 5. Clusters are formed

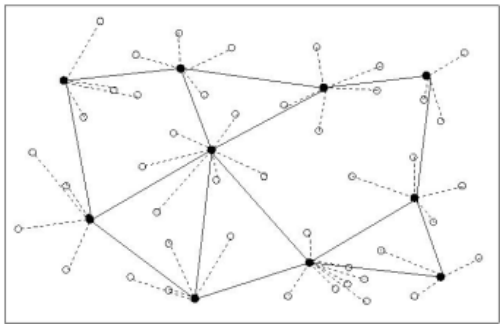

Figure 6. Clusters are connected

Cluster Head Election Criteria

Belief value (B): Based on previous history of nodes, each node should be trusted to its neighbor**.** It is defined as the average of belief values received from each neighboring node.

$$B = \frac{\sum_{i=1}^{N} B_i}{N}$$

Connectivity (C): It is the number of neighbors of a given node, within a 2D hop.

Battery power (b): Power play is an important role to decide the cluster head, because cluster head have many responsibilities, so it must be communicate long time.

Max Value (M): It defines a number of nodes that a cluster can handle within the cluster.

Stability (S): It is also a useful parameter to decide the cluster head. Most stable node elect as a cluster head of cluster. The following parameters are used to calculate the stability of node.

Distance: The distance between two nodes A, B is the number of hops between them.

$$D_{A,B} = = \sum \sqrt{((x_2 - x_1)^2 + (y_2 - y_1))^2}$$

Average distance**:** It is defined as the average of distances between node A and all its neighbors. *N* is the degree of A when *AD* = 2, which means that the majority of neighbors are within 2 hops.

$$AD = \frac{1}{N} \sum_{n=1}^{N} D_{A,n}$$

Mobility: It is calculated by using the difference between two values of average distance at t and t-1.

$$MTA = AD_t - AD_t - 1$$

Weight Factor**:** Weight factor also plays a very important role to decide the cluster head. Weights are assigned to nodes such that their summation is unity.

$$\sum_{i=1}^{N} W_i = 1$$

Global Weight: This is the main parameter to decide the cluster head, which is calculated by using all the above parameters. Node that has the minimum value will elect as a cluster head.

$$W_G[i] = (W_B[i] * F_B[i]) + (W_C[i] * F_C[i]) + (W_b[i] * F_b[i]) + (W_N[i] * F_N[i]) + (W_S[i] * F_S[i])$$

Working Operation

PHASE-1: Cluster and cluster Head Creation in Ad-hoc Network Step-I.

Assign Node Id for each node of Ad-hoc network
No of Node = N;
For (i=0; i<N; i++)
{
Node Id[i] =Random No Generator ( );
} /*Random No Generator generate different random Node id for each node in Ad-hoc network. By this way, higher security for secure communication can be provided.*/

STEP-II Cluster Creation ( )

{Total No of Node=N;
For (i=0; i<N; i++)
{
Each node sends a route request message to its Neighbor to notify its presence to neighbor;
} /*route request message contains the state of node, each node builds neighbor list based on Route request Message*/
}
Int Max Value, Min Value;
for (i=0; i<n; i++)
{
if (No of node in Cluster< Max_value)
{
join cluster( );
}
if(No of node in Cluster>=Max_value)
{
Create new cluster();
}
else
{
Cluster Assimilation () /*if no. of nodes in cluster <min. value*/
}
}

STEP-III Cluster Head Election criteria

Cluster Head Assignment ( )
{
Total No of Node=n;

```
for(i=0; i<n; i++)
{
/*Assign Weight for each node in such a way summation of all weight is unity*/ W_B [i]={}; /*Partial Weight factor for belief value*/
W_C[i]={};/*Partial Weight factor for node connectivity*/
W_b[i]={}; /*Partial Weight factor for Battery */
W_M[i]={}; /*Partial Weight factor for Max value*/
W_S[i]={}; /*Partial Weight factor for Stability*/
/*Take all value from table which is created on the bases of Route request Message by each node*/
F_B[i]= {}; /* Belief value*/
F_C[i]={}; /* Connectivity*/
F_b[i]={}; /* Battery power*/
F_M[i]={}; /* Max value*/
F_S[i]={}; /* Stability*/
*/calculate Global Weight for each Node*/
} Find out minimum Global Weight in Cluster and assign as Cluster Head (CH);
}
```

STEP-IV Newly Arriving Node in Ad-hoc network

a. New node U broadcast route request signal to its neighbor in their transmission Range

b. Calculate following factor for Newly arriving node $F_{B,}$ F_C, F_b, F_M, F_S,W_B, W_C, W_b, W_M and W_S calculate WG (Global weight) for newly arrive node.

c. If (Newly arrive node global Weight <Cluster Head of Cluster)

```
{
Assign New node as a Cluster head;
}
else
{
Join Cluster();
}
```

STEP-V Threshold of battery Power

Check the battery power of Cluster Head
If (CH_battery Power< Threshold)
CH sends Battery power low Signal to Its Neighbor and recalculate the Global weight for each node and Minimum global weight node assign as Cluster Head else

```
{
No requirement;
}
```

IV. DAR PERFORMANCE RESULTS

DAR introduced very limited overhead, which needs the route information collected by route discovery, which has to be done anyway in multi-path routing. DAR works well under different network topologies and node transmission range.

Both AODV (Ad hoc On-Demand Distance Vector Routing) and DAR requires the originator to sign and authorize each packet it sends, and intermediate nodes to verify the signature for each routing packet it processes. DAR is mainly based on asymmetric encryption. It only requires the originator and intermediate nodes to apply a computationally generate and verify authenticators.

It is also observed that the amount of bytes needed for routing overhead was roughly twice larger for AODV than DAR. For DAR, the average packet delivery delay is slightly increased due to the increased communication overhead, while the increase in delay for AODV is roughly three times with cache which means mechanism for the temporary storage of data (packets) is enabled and five times without cache support.

Comparison of DAR with AODV & ARAN:

AODV – Ad hoc On-Demand Distance Vector Routing

ARAN - Authenticated Routing for Ad hoc Networks

DAR mechanism is more efficient for preventing routing attacks when compared to AODV protocols.

AODV only prevents the decrease of the hop count, while attackers can still transmit routing messages with the same hop count as the messages they receive. DAR encrypts node identity into sequence numbers and hop counts; hence attacks would have to increase the hop count as they forward the messages. In DAR, malicious nodes cannot forward the routing packets by replacing the authentication or signature or key of another node.

ATTACK	AODV	ARAN	DAR
Remote redirection modification of sequence numbers	Yes	No	Yes
Modification of hop counts	Yes	No	Yes
Modification of source routes	No	No	Yes
Tunneling	Yes	Yes, but only to lengthen path	Yes, for both short &long paths

Table. 1

V. CONCLUSION

A new mechanism called Dynamic Authenticated Route and Optimized Clustering Algorithm for reducing routing attacks and detecting malicious nodes with low communication and processing overheads was proposed in this paper. In order to measure the risk of both attacks and countermeasures, DAR was compared with a notion of AODV importance factors. Based on several metrics, the performance and practicality of the approach was also investigated. The experimental results clearly demonstrated the effectiveness and scalability of DAR approach. Based on the promising results obtained through these experiments, further more systematic way could be seeked to accommodate securing

nodes and prevent risk attacks frequency in ad hoc networks with a new adaptive decision model.

Thus to conclude, work may be done in this problem by using different clustering algorithms that may be better suitable for the MANET in future.

REFERENCES

[1] Hu, Y., Johnson, D. and Perrig, A. (2003), "SEAD: Secure efficient distance vector routing for mobile wireless Ad-hoc networks", 1:175 - 192.

[2] Zapata, M.G. and Asokan, N. (2002) , "Securing Ad-hoc routing protocols". In Proceedings of ACM Workshop on Wireless Security (WiSe), pages 1 – 10.

[3] Li, J., Blake, C., Couto, D., Lee, H. and Morris, R. "Capacity of Ad-hoc wireless networks," in Proc. ACM Mobicom'01, pp. 61 - 69.

[4] Berger-Sabbatel, G., Duda, A., Heusse, M. and Rousseau, F.(2004), "Short-term fairness of 802.11 networks with several hosts," in Proc. 6th IFIP/IEEE Intl. Conf. Mob. Wireless Commun. Net., pp. 263 - 274.

[5] Broch, J., Maltz, D., Jonthon, D., Hu, Y. and Jetcheva, J."A performance comparison of multi-hop wireless ad-hoc network routing protocols," in Proc. ACM/IEEE Mobicom'98, pp. 85 - 97.

[6] Mu, C., Li, X., Huang, H. and S. Tian, (2008), "Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory," *Proc. 13th European Symp. Research in Computer Security (ESORICS '08)*, pp. 35-48.

[7] Basagni, S., Chlamtac, I., Syrotiuk, V. and Woodward, B. (1998), "A distance routing effect algorithm for mobility (DREAM)", in Proc. ACM Mobicom'98, pp. 76 - 84.

[8] Wu, D. and Negi, R. (2006), "Effective capacity-based quality of service measures for wireless networks," ACM Mob. Nets. App. (MONET), vol. 11, pp. 91 – 99

[9] Marti, S. (2000), "Mitigating Routing Misbehavior in Mobile Ad-hoc Networks," 6th MobiCom, Boston, MA.

[10] Kurosawa, S. (2006), "Detecting Black hole Attack on AODV-Based Mobile Ad-hoc Networks by Dynamic Learning Method," Proc. Int'l. J. Network Sec.

[11] Park, V.D. and Corson, M.S. (1997), "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks," Proc. lNFOCOM '97.

[12] Johnson, D. and Maltz, D. (1996), "Dynamic Source Routing in Ad hoc Wireless Networks," Mobile Computing, Imielinski, T. and Korth, H. Ed., pp. 153 - 81. Kluwer.

[13] Murthy, C.S.R and Manoj, B.S. (2008), "*Ad Hoc Wireless Networks"*, Pearson Education.

[14] George Aggelou, (2004), "*Mobile Ad Hoc Networks"*, McGraw-Hill.

[15] Ahmed, E., Samad, K. and Mahmood, W. (2006), "Cluster-based Intrusion Detection (CBID) Architecture for Mobile Ad Hoc Networks".

[16] Weimerskirch, A. and Thonet, G. (2001), "Distributed Light-Weight Authentication Model for Ad-hoc Networks", Vol. 2288, pp. 341, 354.

[17] Chlamtac, I., Conti, M. and Liu, J. (2003), "Mobile Ad Hoc Networking: Imperatives and Challenges," *Ad Hoc Networks*, vol. 1, no. 1, pp. 13 – 64.

[18] Hubaux, J.P., Buttyan, L. and Capkun, S. (2001), "The Quest for Security in Mobile Ad Hoc Networks".

[19] Gorlatova, M.A., Mason, P.C., Wang, M., Lamont, L. and Liscano, R.(2006), "Detecting Wormhole Attacks in Mobile Ad Hoc Networks through Protocol Breaking and Packet Timing Analysis," pp. 1-7.

[20] Sun, Y., Han, Z. and Liu, K.J.R. (2008), "Defense of trust management vulnerabilities in distributed networks," vol. 46, issue 2, pp.112-119.

[21] Balakrishnan, V.,Varadharajan, V., Tupakula, U.K. and Lucs, P.(2007), "TEAM: Trust Enhanced Security Architecture for Mobile Ad-hoc Networks," *2007*, pp. 182-187.

[22] Moazam Bidaki and Mohammad Masdar, (2013), "Reputation based Clustering Algorithms in MANET", IJAST, Vol-54.

[23] Levine, B., Shields, C. and Belding-Royer, E. (2002) "A Secure Routing Protocol for Ad Hoc Networks," *Proc. 10th IEEE Int'l Conf. Network Protocols (ICNP '02)*, pp. 78 – 88.

[24] Heenavarshney and Pradeep kumar, (2013), "Secure Communication architecture on "BBCMS" clustering algorithm for MANET", IJITEE, Vol-3.

[25] Balakrishnan, V.,Varadharajan, V., Tupakula, U.K. and Lucs, P.(2007), "Trust Integrated Cooperation Architecture for Mobile Ad-hoc Networks," *ISWCS 2007*, pp. 592-596.