Middle-East Journal of Scientific Research 24 (S2): 340-346, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.24.S2.243

A Secured Defense Scheme against Collaborative Blackhole Attacks in MANET

[1]R. Hemalatha and [2]S.A. Arunmozhi

[1]PG scholar, Department of ECE Saranathan College of Engineering, Trichy, India
[2]Associate professor, Department Of ECE Saranathan College of EngineeringTrichy, India

Abstract: A mobile ad hoc network (MANET) is a collection of self-configuring infrastructure less network of mobile devices connected together by wireless links. Mobile ad hoc network is prone to many security issues in which black hole attack causes the serious problems. In the proposed method this blackhole attack is detected by means of Secured Bait Detection Scheme (SBDS). In this source node randomly selects the one hop neighborhood node as the bait node in which the address of the bait node is used to detect the malicious node in the network. After the blackhole node is detected it will be reverse traced and this node will be put in to the blackhole list which will be informed to all the other nodes. Even after the detection of blackhole nodes because of the lack of fixed infrastructure there are many difficulties in maintaining the secure communication. So the data is encrypted before transmission using the Elliptic curve-ElGamal cryptosystem.

Key words: Secured bait detection scheme · Collaborative blackhole attack · Bait node · Dynamic source routing · Mobile ad hoc network · Elliptic Curve-ElGamal cryptosystem

INTRODUCTION

A mobile ad hoc network (MANET) is a collection of self-configured and infrastructure less network of mobile devices connected together by wireless links. It has a dynamically changing topology (i.e.,) each device in a MANET can move randomly in any direction. It will therefore frequently change its links to other devices. They contain one or multiple and different transceivers between nodes. Each device can acts as router. Therefore each device forward the traffic unrelated to its own use. The major challenge in building a MANET is to make each device to monitor and maintain the information required to properly route traffic.

The types of MANET includes the following,

- Vehicular Ad hoc Networks (VANETs)
- Smart Phone Ad hoc Networks (SPANs)
- Internet based MANET link mobile nodes and fixed internet-gateway nodes.
- Military/Tactical MANETs are used in military units

Issues in Manet

Limited Power Supply: Some or all of the nodes in a MANET may rely on batteries or other exhaustible means for their energy. For these nodes energy conservation is the most important design criteria for optimization. The problem that may be caused by the restricted power supply is the denial of service attacks.

Dynamically Changing Topology: Nodes are free to move arbitrarily; thus, the network topology which is typically multihop may change randomly and rapidly at unpredictable time. Because of this the topology of the ad hoc network is changing constantly. So there is possibility for potential attacks in the network.

Lack of Centralized Management Facility: An ad hoc network does not have a centralized management facility such as a name server. It lead to some vulnerable problems such as detection of attacks, path breakages, transmission impairments and packet dropping also take place.

Scalability: Scalability is the problem in the mobile ad hoc network. Unlike the traditional wired network the scale of the ad hoc network keeps changing all the time: As a result, routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network.

No Predefined Boundary: In mobile ad hoc networks physical boundary of the network is not precisely defined.

Corresponding Author: R. Hemalatha, PG scholar, Department of ECE Saranathan College of Engineering, Trichy, India

The nodes work in a migratory environment where they are allowed to join and leave the wireless network. As an adversary comes in the radio range of node it will be able to communicate with that node.

Threats in Network Security: There are many attacks in the network layer which causes serious security threats in MANET. Black hole attack, warm-hole attack, flooding etc., comes under the network layer attacks.

Black Hole Attack: In a black hole attack, a malicious node sends a fake RREP packet to the source node that has initiated a route discovery process in order to show itself as a destination node or an intermediate node to the actual destination node. In such a case the source node consider that the route discovery process is complete and start to forward the packets to the malicious node which had replied for the route request message. Upon receiving the data packets the malicious node starts to drop the packets without forwarding it to the destination as shown in fig.1. This is called as the blackhole attack. In fig.1 when the source node S sends the route request, the malicious node n_4 send the fake route reply and continue to receive and drop the packet upon receiving it from the source node without forwarding it to the destination.

Collaborative Black Hole Attack: The malicious node could be said to form a black hole in the network. Sometimes these malicious nodes cooperate with each other with the same aim of dropping packets without sending it to the actual destination. These are known as collaborative Black Hole nodes and the attack is known as Collaborative Black Hole attack.

Security Requirements in Manet: In MANET the security depends on the parameters such as authentication, integrity, non-repudiation, availability. If any of these parameters are not satisfied the security will not be obtained and the communication will not be effective. Without authentication the attacker can act as a legitimate node and gain access to the most secure information.

Reason for the Consideration of Security Issue in Manet: Although wireless network is more versatile than a wired one, it is more vulnerable to attacks compared with the wired network. This is due to the nature of radio transmissions, which are made on the air. On a wired network, an intruder would need to break in to a machine of the network or physically tap a cable.

On a wireless network there is possibility for an adversary to eavesdrop on all messages within the emission area. It can be done by operating in promiscuous mode and using a packet sniffer. There are also different tools available to detect and intrude the wireless network.

Hence by simply being within the radio range, the intruder has access to the network and it can intercept the transmitted data without the knowledge of the sender. As the intruder is also potentially invisible, it can also record, alter and then simply retransmit the packets as they are emitted by the sender, even pretending that packets come from a legitimate party. Also the existing security solutions of wired networks cannot be applied directly to MANET, which makes a MANET much more vulnerable to security attacks.

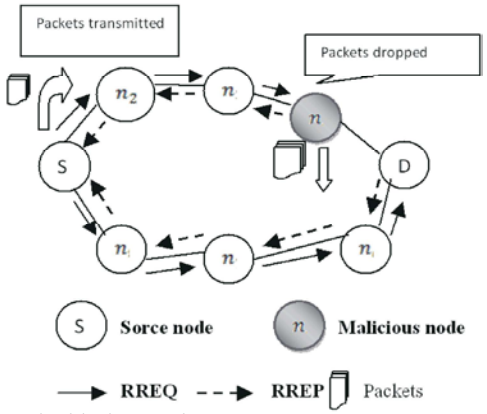

Fig. 1: Blackhole attack

The topology of the adhoc network is also changing constantly. So a detection mechanism is developed to detect some kind of potential attacks.

Related Work: Ayesha Siddiqua and Kotari Sridevi [1] proposed a method for the prevention of black hole attack in MANET using the secure knowledge algorithm. In this approach, every node in a network listens to its neighboring nodes promiscuously. In promiscuous mode, every node monitors the packet being forwarded by its neighbors in order to observe the behavior of neighbor regarding packet operation. Every node compares the neighbor information with the information it stores in its knowledge table. If both are same the node assumes that the packet is forwarded further, otherwise node waits for particular amount of time and checks the reasons for packet dropping.

Jitendra Savner and Vinita Gupta [2] proposed a method for the prevention of blackhole attack in MANET using the clustering approach. In this method the devices are categorized in to mobile nodes, clustering heads and monitoring server. The monitoring server calculate the trust value which is based on the blackhole characteristics. It monitors the communication between

the internal and external clusters and between the unknown nodes. If any of the node is found to only receive the packets without forwarding to the neighbouring node, that node is eliminated from the network and marked as malicious node.

K. Liu, D. Pramod [3] In this paper in order to detect the routing misbehavior two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received.

Y. Xue and K. Nahrstedt [4] This method uses end-to-end acknowledgements to monitor the quality of the routing to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining "good" routes, the source node uses a new route.

Anand A.Aware and KiranBhandari [5] proposed a method for the prevention of blackhole attack on AODV in MANET using the hash function. The source node assumes that the blackhole node will be the first to respond to the route request. So after broadcasting route request to the nodes the source node will reject the first route reply. For a malicious node it is difficult to become the part of the second shortest route as it has to continuously monitor the entire network which is not easy in MANET. The source node selects the second shortest path to the destination and authenticates the packet using the hash function.

Ruo Jun Cai, Peter Han Joo [6] Chong proposed a method to prevent single and colluded blackhole attack using trust based routing with neighborhood connectivity. In this method each node maintains a neighborhood connectivity information table (NCIT) and broadcast a hello message to the other nodes. When a node receives the route reply message it first verifies its NCIT table to find whether the replied node is the neighbor node of the destination. If it is not indicated in the NCIT table that node is considered as the attacker node.

Methodology: MANET is highly susceptible to many attacks because of its infrastructure less network. The aim of the proposed approach is to detect the collaborative blackhole attacks in MANET using the Secured Bait Detection Scheme (SBDS). SBDS is based on dynamic source routing [DSR] protocol which involves the process of route discovery and route maintenance [13]. This method merges the advantage of both proactive and reactive defense architecture. In this method a bait node is chosen randomly by the source node in order to detect the blackhole node. The SBDS scheme involves four steps

- Initial bait step
- Reverse tracing step
- Reactive defense step
- Encrypting the data for transmission

Initial Bait Step: The source node randomly selects an adjacent node with one hop neighborhood as the bait node. The goal of the bait phase is to make the malicious node to send the route reply to the bait route request *RREQ'*. Initially in the bait step the address of the bait node is used as the destination address and bait route request *RREQ'* is broadcast to all the nodes. In order to know the information about the adjacent nodes hello message is exchanged between the nodes.

If malicious node is not present within the network then the route reply RREP will not be from any other node other than this bait node. If malicious node is there in the network then the reply will be from that node too in addition with this bait node. Thus the presence of malicious nodes in the network is indicated and reverse tracing operation in the next step will take place to detect that node.

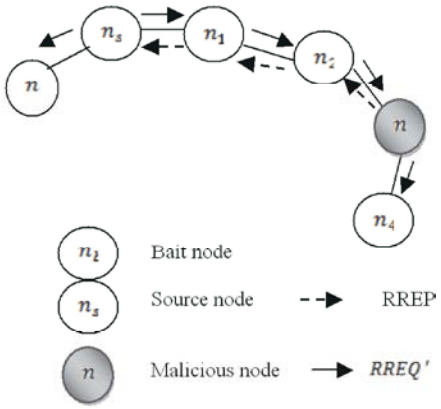

Fig. 2: Selection of cooperative bait address

Reverse Tracing Step:

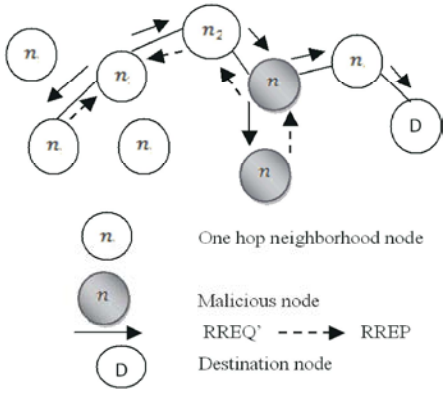

Fig. 3: Reverse tracing approach

The reverse tracing step is used to detect the malicious node through the route reply RREP it has sent to the bait route request message. When the malicious node n_m replies with a false RREP its address list is recorded in the reply message. That is $P = \{n_1, ... n_k, ...n_m, ...n_r\}$. Node receiving this RREP will separate the address list with the destination address and get the address $K_k = \{n_1, ... n_k\}$ where K_k represents the route information from source node to destination node. This address list K_k is differentiated from the address list P and a new address list $K'_k = P\text{-}K_k = \{n_{k+1},...n_m,...n_r\}$ is created where K'_k represents the route information to the destination node. Each node performs this and this address list is stored in RREP and sent to the source node. In order to prevent the interference by malicious nodes, the node that receives the RREP will compare the source address in RREP, next hop of node n_k and one hop of n_k When the source node obtains K'_k the dubious path information sent by the malicious node can be detected by,

$$S = K'_1 \cap K'_2 \cap K'_3 ... \cap K'_k$$

The source node enters the promiscuous mode to confirm that the malicious node is in set S. The source node send the packet for testing in this route a monitored also send the message to the second node towards the last node in T. The node monitors whether the next node forwards the packet and fed the result to the source node. If not so, that node is stored in the blackhole list.

Likewise as in figure 3 n_b is chosen as the bait node by the source node n_3. Bait request is transmitted by the source node to all the other nodes. Malicious node n_3 will send the fake route reply. Now the source node receives the route reply from both the bait node and the malicious node. This indicates that the malicious node is present in the network and so the source node will start the reverse tracing operation to detect that malicious node. If n_3 wants to send the route reply it will first create the address list

$$P = \{n_3, n_1, n_2, n_3, n_4, n_b\}$$

If node n_2 receives this, it will separate the list P by the destination address n_b. It will result in the address list $K_2 = \{n_3, n_1, n_2\}$. Then set difference operation is conducted between the list P and K_2. It will result in $K'_2 = P - K_2 = \{n_3, n_4, n_b\}$.

It will then send the list K'_2 and the RREP to the source node. The node n_1 also perform the same operation and obtain the list $K'_1 = \{n_2, n_3, n_4, n_b\}$. This will be transmitted to the source node along with the route reply. When the source node receives this, it will perform the operation $S = K'_1 \cap K'_2 = \{n_3, n_4, n_b\}$ and $T = P - S = \{n_3, n_1, n_2\}$. Then the source node sends the recheck message to the node n_1 and request it to operate in the promiscuous mode. Now the node n_1 transmit the test packets and listen whether the nodes are transmitting the packets towards the destination node and fed the result to the source node. If any of the node is found to drop the packet without transmitting it will be stored and the black hole list and this information will be transmitted to all the nodes.

Reactive Defense Step: After the initial bait step and the reverse tracing step the dynamic source routing [DSR] route discovery process is activated. After the route is established, if the packet delivery ratio is found to fall below the threshold value the detection mechanism is triggered again. The threshold is set to be varied in the range [85%, 95%] that can be adjusted according to the current network efficiency. Initial threshold value is set to 90%.The dynamic threshold algorithm is designed to control the time when the packet delivery ratio falls below the threshold. When the packet delivery ratio falls below the threshold it indicates that the malicious nodes are still present in the network and the threshold is adjusted upward, otherwise the threshold will be lowered.

Dynamic Threshold Algorithm:

- Initialize the threshold value for the packet delivery ratio.
- Calculate the time (T1) taken for the PDR to drop down to the threshold value.
- Find whether the PDR is less than threshold.
- If PDR < threshold the initial proactive defense step takes place (i.e., initial bait step and reverse tracing step)
- Again calculate the time (T2) taken for the PDR to drop down to threshold value.
- If T2 <T1 the threshold value is adjusted upwards else the threshold value will be lowered.

Encryption of Data: In MANET even after the detection of blackhole attacks there is possibility for an unauthorized node to gain access to the confidential information transmitted between the nodes. So the concept of encryption is added for improving the security in the network. Elliptic Curve-ElGamal cryptographic technique is used for encrypting the data before transmission between the nodes which preserves the privacy at the intermediate nodes and homomorphic MAC [14] is generated to verify the authenticity of the cipher text.

Ec-Elgamal Cryptosystem: This technique involves the components such as key generator, encryption algorithm and decryption algorithm.

- A large prime value 'p' is selected
- An elliptic curve E is chosen over a finite field F_p and a point P is chosen over the elliptic curve.
- Secret key s_k value is randomly generated and the public key p_k value is calculated using $p_k = s_k . P$.
- A random integer r is chosen and the cipher text is computed using $c_1 = r.P$ and $c_2 = m+r.p_k$.
- The decrypted text is computed using $D(c) = c_2 - s_k . c_1 = m$

In this the first three steps denote the key generation, steps 4 and 5 denote the concept of encryption and decryption respectively.

Homomorphic MAC:

- Two keys k_1 and k_2 are generated using the pseudo random generators G and F which are used for MAC construction.
- Let 'id' is an identifier of vector space. The message is divided in to a sequence of vectors.
- To generate the MAC tag T,

$U \leftarrow G(k_1)$

$B \leftarrow F(k_2,id,i)$

$T \leftarrow (U.v)+b$

Where T is a tag generated for the vector v.

Encryption Protocol:

- The bait node generates a key pair (p_k , s_k) using the EC-ElGamal cryptosystem.
- Each node I shares a pair-wise symmetric key (i,j) with the neighboring nodes j as well as the pair-wise symmetric key (i , j_m) with the nodes at m hops away j.
- The source node encrypts the message using the public key generated using the EC-ElGamal cryptosystem.
- The source node then generates the MAC for this cipher text and this MAC is encrypted using the symmetric key shared with the neighboring nodes.
- Each intermediate node j_m decrypts the received MAC using the symmetric key shared between this node and the node i.
- Now the node j_m computes the MAC for the cipher text using the symmetric key that was shred and compares it with the decrypted MAC computed in the previous step. If both are equal the cipher text is accepted and transmitted.
- Finally the destination node performs the decryption over the received cipher text to obtain the message transmitted by the source node.

Implementation

Simulation: The proposed SBDS scheme is simulated using network simulator version 2.35. CBR (Constant Bit Rate) traffic is used to generate UDP packets. For simulation fifty nodes are generated and packet size of 512 bytes is used.

Performance Analysis: Performance of SBDS is analyzed using the parameters such as packet delivery ratio, throughput, routing overhead and delay for different threshold values and compared with the DSR scheme.

Packet Delivery Ratio: It is defined as the ratio of the number of packets received at the destination to the number of packets sent by the source. The average packet delivery ratio denoted as PDR for the traffic n is given as,

$$PDR = \frac{1}{n}\sum_{i=1}^{n}\frac{pktd_i}{pkts_i}$$

Where $pktd_i$ is the number of packets received by the destination in the ith application and $pkts_i$ is the number of packets sent by the source in the ith application

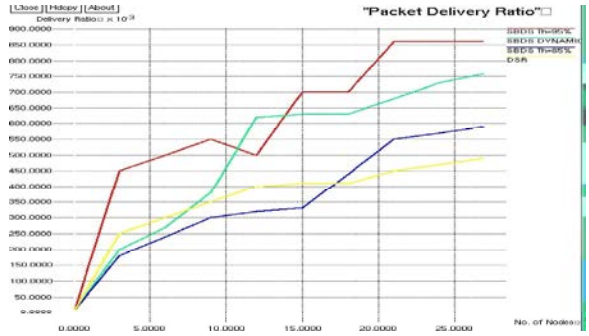

Fig. 4: Packet delivery ratio

The SBDS scheme successfully detects those malicious nodes while keeping the packet delivery ratio above 90%. A threshold of 95% would then result in earlier route detection than when the threshold is 85% or

is set to the dynamic threshold value. Thus, the packet delivery ratio when using a threshold of 95% is higher than that obtained when using a threshold of 85% or the dynamic threshold. DSR drastically suffers from blackhole attacks when the number of malicious nodes increases. This is attributed to the fact that DSR has no secure method for detecting/preventing blackhole attacks. SBDS scheme shows a higher packet delivery ratio compared with that of DSR even in the case when the number of malicious nodes is increased.

Throughput: This is defined as the ratio of the total amount of data that the destination receives from the source to the time taken by the destination to get the final packet. The throughput T for the application traffic n is given by,

$$T = \frac{1}{n}\sum_{i=1}^{n}\frac{b_i}{t_i}$$

Where b_i is the amount of data that the destination received from the source and t_i is the time taken by the destination to get the final packet

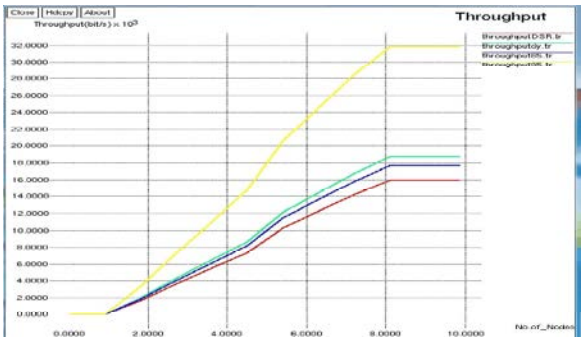

Fig. 5: Throughput

For all the threshold values the throughput of the SBDS scheme is higher when compared to the DSR scheme. This is because all the malicious nodes are detected the communication takes place efficiently and also the throughput increases.

Routing Overhead: This is defined as the ratio of the amount of routing-related control packet transmissions to the amount of data transmissions. The average routing overhead of the application traffic n, which is denoted as RO is given by

$$RO = \frac{1}{n}\sum_{i=1}^{n}\frac{cpk_i}{pkt_i}$$

Where cpk_i is the number of control packets transmitted in the ith application traffic and pkt_i is the number of data packets transmitted in the ith application traffic.

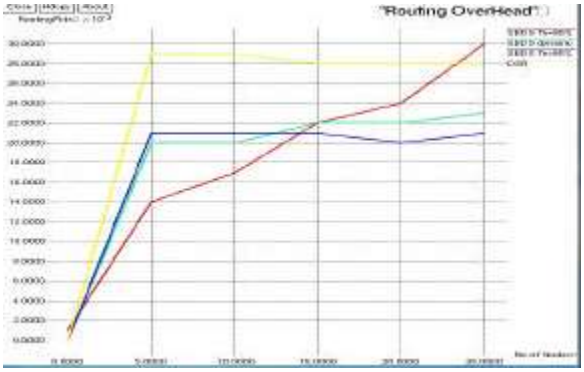

Fig. 6: Routing overhead

The routing overhead of DSR is minimum when compared to the SBDS scheme. This is due to the fact that DSR has no security method or defensive mechanism as in SBDS scheme. The routing overhead produced by SBDS for different threshold value is also larger when compared to the DSR scheme. When the threshold is set to 95% the detection mechanism is triggered faster when compared to the threshold of 85% or the dynamic threshold. Thus the bait packets will be sent many times in the network and the routing overhead increases. Thus there is tradeoff between the routing overhead and the packet delivery ratio.

Average End-to-End Delay: This is defined as the average time taken for a packet to be transmitted from the source to the destination. The average end-to-end delay of the application traffic n, which is denoted by E, is obtained as

$$E = \frac{1}{n}\sum_{i=1}^{n}\frac{d_i}{pktd_i}$$

Where d_i is the total delay of packets received by the destination node and $pktd_i$ is the number of packets received by the destination node.

For all threshold values SBDS incurs a little bit more end-to-end delay compared with that of DSR. This is because SBDS involves initial bait step to detect the malicious nodes. Even when there are more malicious nodes in the network, the SBDS would still detect them simultaneously when they reply with a RREP.

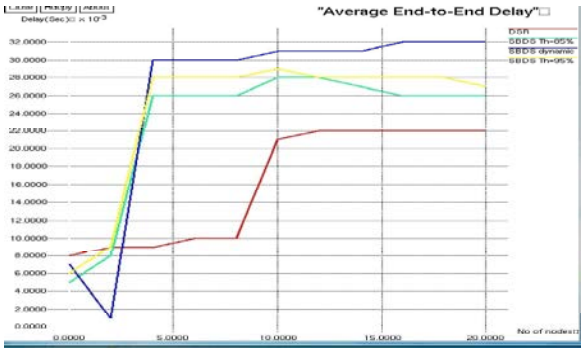

Fig. 7: Average end-to-end delay

CONCLUSION

The proposed method called as the Secured Bait Detection Scheme detects the malicious nodes in MANET and makes the communication successful. It also outperforms the DSR scheme. The encryption concept used improves the communication security in MANET by preserving the privacy of the information. As a future work we intend to minimize the delay and routing overhead.

REFERENCES

1. Ayesha Siddiqua and Kotari Sridevi, 2015. Prevention of blackhole attack in MANET using secure knowledge algorithm, pp: 421-425.
2. Jitendra savner and Vinita gupta, 2014. Clustering of Mobile Ad Hoc Networks: An Approach for BlackHole prevention, 2014 international conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp: 361-365.
3. Liu, K. and D. Pramod, 2007. An Acknowledgement based approach for the detection of routing misbehavior in MANETs, IEEE trans.Mobile Comput., 6(5): 536-550.
4. Xue, Y. and K. Nahrstedt, 2004. Providing fault-tolerant ad hoc routing service in adversarial environments, Wireless Pers. Commun., 29: 367-388.
5. Anandh Aware A. and Kiran Bandhari, 2014. 'Prevention of blackhole attack on AODV in MANET using hash function', International conference on Reliability, Infocom technologies and optimization, pp: 1-6.
6. Ruo Jun Cai and Peter Han Joo Chong, 2014. Poster: Trust-based Routing with Neighborhood Connectivity to Prevent Single and Colluded Active Black Hole, 9th International Conference on Communications and Networking in China, pp: 684-685.
7. Rubin, I., A. Behzad, R. Zhang, H. Luo and E. Caballero, 2002. TBONE: A mobile-backbone protocol for ad hoc networks,in Proc. IEEE aerosp. Conf, 6: 2727-2740.
8. Baadache, A. and A. Belmehdi, 2010. Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks, Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1.
9. Maeti, S., T.J. Giuli, K. Lai M. Baker and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks, in Proc 6th Annu. Intl. Conf. Mobi Com, pp: 255-265.
10. Tsou, P.C., J.M. Chang, H.C. Chao and J.L. Chen, 0000. CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture, in Proc. 2nd internatonal conference. Wireless comm. VITAE, Chennai, India,
11. Corson, S. and J. Macker, RFC 2501,Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). available: http://www.elook.org/computing/rfc/rfc2501.html
12. Chang, C., Y. Wang and H. Chao, 2007. An efficient Mesh-based core multicast routing protocol on MANETs,"J.Internet.technol., 8(2): 229-239.
13. Johnson, D. and D. Maltz, 1996. Dynamic source routing in adhoc wireless networks, Mobile Comput., pp: 152-181.
14. Shweta Agarwal and Dan Boneh, Homomorphic MACs: MAC based integrity for network coding, In Applied Cryptography and Network Security, springer 2009, pp: 292-305.