Middle-East Journal of Scientific Research 23 (9): 2198-2204, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.09.22451

An Optimal Voting Mechanism for Cluster-Based Certificate Revocation in Mobile Ad Hoc Networks

[1]Mohammed Ali Hussain and [2]Satuluri Naganjaneyulu

[1]Department of Electronics and Computer Engineering, KL University, Guntur Dist, A.P., India
[2]Department of Information Technology,
Lakireddy Bali Reddy College of Engineering, Krishna Dist, A.P., India

Abstract: Mobile Adhoc Networks (MANETS) consists of nodes having routing capabilities. MANETs does not have any fixed infrastructure. Due to this reason, MANET nodes are vulnerable to various types of attacks includes worm hole attack, spoofing attack, black hole attack, DOS, non repudiation attack. There are many existing methods for identifying and blocking such attacker nodes. But the attacker node can perform its operations even though it is blocked. So the main task is to completely disconnect that node from the entire network. This can be done with the help of digital certificates. Nodes having valid digital certificates are considered as legal nodes. Otherwise they are considered as attacker nodes. So a node with a legal digital certificate can communicate with other nodes in the network. Digital certificates are issued by Certificate authority (CA). Certificate authority digitally signs each certificate with its private key and then issue to the nodes. Now nodes can verify each others certificate before communication. If a node is identified as vulnerable then the certificate is revoked from it and then disconnected from the network. In our research work, we use voting mechanism to identify attacker nodes and then revoke certificates from them. In many cases malicious node may make fake claims, this result in revoking certificates from legal nodes. Then the question arises in front of CA that the claim is trustable or not. Therefore the certificate revocation method must be able to distinguish fake claims from valid ones.

Key words: Certificate Authority · Certificate revocation · Cluster · MANET · Voting

INTRODUCTION

The nodes in a fixed network use cables for communication. They have a central administrator for controlling and monitoring the communication. A mobile ad hoc network does not have any fixed infrastructure or any administrator. They are self configuring networks. Fig. 1 shows an example of mobile ad hoc network. MANET allows any node can communicate with any other node wirelessly by forming a network. So nodes can join and leave a network freely. Thus the number of nodes at an instance can increase or decrease in a MANET. The main problem here is security. For example an attacker node can enter into a MANET freely and can launch attacks. Thus security [1] becomes a major concern in MANET. Various types of attacks include black hole attack, worm hole attack, denial of service attack, non repudiation attack.

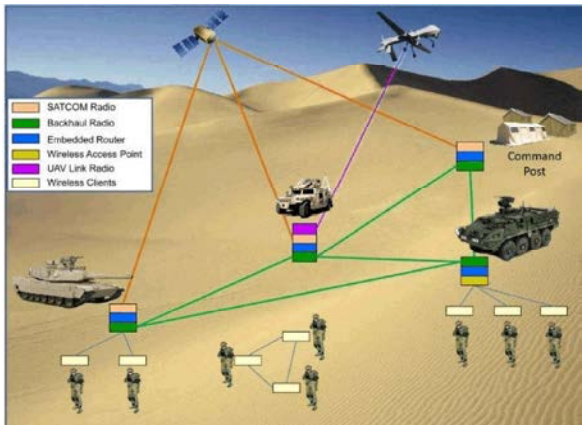

Fig. 1: An Example Mobile Ad Hoc Network

Attacks on MANET can come in any direction and any node in the network can become a target for the

Corresponding Author: Mohammed Ali Hussain, Department of Electronics and Computer Engineering, KL University, Guntur Dist andhra Pradesh, India. E-mail: dralihussain@kluniversity.in.

attacker node. But in a fixed network, an attacker node must physically gain access to network before launching attacks. To defense such attacks, fixed networks use gateways or firewalls to filter network traffic. So MANETs need more security components than fixed networks.

Interestingly, the phenomena that make mobile ad hoc networks paradigms so attractive is that they are being self-organizing, dynamic and decentralized, are the same phenomena that compound the challenges of developing an adequate security mechanisms for these networks. Consider for example the difficulty associated with the use of the digital certificates in mobile ad hoc networks. If the mobile nodes have the necessary computational resources for handling the public key encryption, then the remaining challenges can be briefly outlined as follows [2]:

- Issuing of certificates
- Validating certificates
- Storage and retrieval of certificates
- Revocation of certificates

The first three steps can be dealt with in an intuitive way. Yes, there is no centralized entity in mobile ad hoc networks to play the role of the certificate authorities (CAs). However, as is the case with fixed networks with high security requirements, whereby entities identities are verified off-line before digital certificates are issued; the same principle can be applied for mobile ad hoc networks. Mobile network nodes can be required to have valid digital certificates from trusted CAs prior to joining the ad hoc network. The validation of digital certificates can be easily done if each network node stores the public keys of the trusted CAs that issued the digital certificates of the peers it needs to communicate with. Similarly, each network node can store the certificates of its communicating peers; thus the digital certificates will be readily available when they are required. The greater challenge is certificate revocation process. For various reasons, digital certificates will need to be revoked periodically; for example, if the private key associated with a digital certificate is compromised, the digital certificate will need to be revoked and information be made available to network peers in a timely manner. For fixed networks, CAs issue Certificate Revocation Lists (CRLs)—containing data about revoked certificates—at regular intervals. The CRLs [3-11] are either placed in the online repositories where they are readily available or they may be sending to the individual nodes alternatively. Online certificate status protocol (OCSP), can be used to ascertain the information about the status of a certificate [9].

Whether CRLs, OCSP, or any other certificate validation protocols, are used in the conventional networking settings, a necessary requirement is the availability of the network connection to the CAs, the central repositories where CRLs are stored, or to the centralized servers running the digital certificate validation protocols. The problem with adapting this scenario to mobile ad hoc network is: in any given mobile ad hoc network, there may neither be network connection to the centralized CAs nor central repositories where CRLs can be retrieved, or centralized servers running certificate validation protocol(s). Thus, ascertaining whether or not a digital certificate is revoked presents a challenge in ad hoc networks environments [3].

To-date, the security schemes utilizing the digital certificates, proposed for mobile ad hoc networks, either do not explicitly address the issue of the certificate revocation, or they require that digital certificates of nodes be revoked when the nodes are accused of misbehavior. Either approach can be critical. The Certificate revocation is too important an issue to be ignored; nonetheless, if adequate safeguards are not built into the process of determining when a digital certificate should be revoked, the malicious nodes can wrongfully accuse other nodes of misbehavior and cause the certificates of good, uncompromised nodes to be revoked. Compromised or malicious nodes can in fact use this procedure (we called it malicious accusation) as an exploit for isolating and ultimately cutting off the legitimate, well-behaving nodes from a network.

MANET Attacks: Attacks on mobile ad hoc networks reduce the efficiency of the overall network. The following are some of the attacks on MANETs.

Worm Hole Attack: Worm hole attack [2-13] is a severe attack in mobile ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the hacker has not compromised any nodes and even if all communication provides confidentiality and authenticity. In this attack, an attacker records packets (or bits) at one location in the mobile network and tunnels them (possibly selectively) to another location and then retransmits them there into the network. The wormhole attack can form a serious vulnerability in mobile networks, especially against many mobile ad hoc network routing protocols and location-based wireless security systems. For example, most existing mobile ad hoc network routing protocols, without some mechanism to defend against this attack, would be

unable to find routes longer than one or two hops, severely disrupting communication.

Black Hole Attack: In black hole attack [3-12], an attacker node uses its routing protocol in order to advertise itself for having the optimal path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of new routes irrespective of checking its routing table. In this way malicious node will always have the availability in replying to the route request and thus intercept the data packet and retain it. In protocol based on flooding technique, the attacker node reply will be received by the requesting node before the reception of reply message from the actual node; hence an attacked and forged route is created. When this route is establish, now it is up to the node whether to discard all the packets or forward it to the unknown address.

Black hole attacks are of two types

- Internal black hole attack
- External black hole attack

Internal black hole attack is a type of black hole attack which has an internal malicious node which fits in between the routes of given source and the destination. As soon as it gets the chance this attacker node make itself an active data route element. At this stage it is now capable of conducting the attack with the start of the data transmission. This is an internal vulnerability because the node itself belongs to the data route. Internal attack is more susceptible to defend against because of difficulty in detecting the internal misbehaving node.

External black hole attacks physically stay outside of the network and deny access to the network traffic or creating congestion in network or by disrupting the entire network. External attack can become a kind of internal black hole attack when it take control of the internal malicious node and control it to attack other nodes in MANET.

Spoofing Attack: In this attack, the attacker assumes the identity of another legal node in the network; hence it receives the messages that are meant for that node. Usually, this type of attack is launched in order to gain access to the network so that further attacks can be launched in the network, which could seriously harm the entire network. This type of attack can be launched by any attacker node that has enough information of the network to forge a false identification of one its member nodes and utilizing that identification and the node can misguide the other nodes to establish route towards itself rather than towards the original node.

IP address spoofing is one of the most frequently used spoofing attack mechanisms. In an IP address spoofing attack, the attacker sends IP packets from a false (or "spoofed") source address in order to disguise itself. Denial-of-service attacks (DOS) often use IP spoofing to overload the networks and the devices with packets that appear to be from legitimate source IP addresses. There are two ways that IP spoofing attacks can be used to overload the targets with traffic. One method is to simply to flood a selected target with the packets from multiple spoofed addresses. This method works by directly sending the victim more data than it can handle. The other method is to spoof the target's IP address and then send packets from that address to many different recipients on the network. When another system receives a packet, it will automatically transmit the packet to the sender in response. Since the spoofed packets appear to be sent from the target's IP address, all the responses to the spoofed packets will be sent to (and flood) the target's IP address [14].

IP spoofing attacks can also be used to bypass the IP address-based authentication. This process can be very difficult and is primarily used when the trust relationships are in place between machines on a network and internal systems. Trust relationships use IP addresses (rather than user logins) to verify the machines' identities when attempting to access systems. This enables the malicious parties to use spoofing attacks to impersonate the machines with access permissions and bypass trust-based network security measures.

The following are the examples of spoofing attacks:

- Man-in-the-middle attack: In this attack, the packet sniffs on link between the two end points and can therefore pretend to be one end of the connection
- Routing redirect: This attack redirects routing information from the original machine to the hacker's host (this is another form of man-in-the-middle attack).
- Source routing: This attack redirects individual packets by hackers host
- Blind spoofing: This attack predicts responses from a host, allowing commands to be sent, but cannot get immediate feedback.
- Flooding: In this, SYN flood fills up receive queue from random source addresses; smurf spoofs victims address, causing everyone respond to the victim [15].

Resource Consumption Attack: An attacker node acting as intermediate node may initiate frequent generation of beacon packets, unnecessary route requests or forwarding stale routes to nodes in the network. This result in over consumption of the nodes limited resources and keeps the nodes unnecessary occupied.

Denial of Service (DOS) Attack: A Denial-of-Service (DoS) attack is an attack meant to shut down a computer system or network, making it in accessible to its legal users. DoS attacks accomplish this by flooding the target with the traffic, or sending it information that triggers a crash. In both instances, this attack deprives the legitimate users (i.e. employees, members, or account holders) the service or resource they expected. Victims of the DoS attacks often target the web servers of high profile organizations such as commerce, banking and media companies, or government and trade organizations. Though these attacks do not typically result in the theft or loss of significant information or other resources, they can cost the victim a great deal of time and money to handle.

There are two general methods of these attacks: flooding services or crashing services. Flooding attacks occur when the system receives too much traffic data for the server to buffer, causing them to slow down and eventually stop. The popular flood attacks include:

Buffer Overflow Attacks: This attack is the most common DoS attack. The main aim of this attack is to send more traffic to a network address than the programmers have built the system to handle. It includes the attacks ICMP flood and SYN flood in addition to others that are designed to exploit bugs specific to certain applications or networks.

ICMP Flood: This attack leverages misconfigured network devices by sending spoofed packets that ping every computer on the targeted network, instead of just one specific host. The mobile network is then triggered to amplify the traffic. This attack is also known as the smurf attack or also termed as ping of death.

SYN Flood [14]: This attack sends a request to connect to a remote server, but never completes the handshake. Continues until all open ports are saturated with many requests and none are available for legitimate users to connect to.

Non Repudiation Attack: Non repudiation is a method of guaranteeing message transmission between communication parties via digital signature and encryption. It is one of the five pillars of the information assurance (IA). The other four are availability, confidentiality, integrity and authentication. Non repudiation is often used for digital contracts, digital signatures and email messages. By using a data hash, proof of authentic identifying information and data origination can be obtained. Along with the digital signatures, public keys can be a problem when it comes to non repudiation if the message recipient has exposed, either knowingly or unknowingly, their encrypted or the secret key.

This attack ensures that sender or receiver of a message cannot disallow that they have ever sent or received such a message. This will be helpful when we want to discriminate if a node with some undesired function is compromised or not.

Certificate Authority and Certificate Revocation: A digital certificate is a digitally signed statement binding the key holder's identification to a public key and various other attributes. The issuer of the digital certificate is commonly called a certificate authority (CA). Certificates are tamper proof. This means they cannot be modified, if modified they becomes invalid. No one can forge digital certificates, because CA uses its private key for generating digital certificates. Private Key of CA is not available to public. During the issuance of digital certificates, an expiry date is fixed in the certificate. The certificate is valid up to that period only. Whenever the expiry period is completed or the node is identified as malicious, then CA revokes the certificate. This is called certificate revocation [4, 5]. Nodes cannot communicate with each other without valid digital certificates. The following are some of the reasons for certificate revocation:

- If a node becomes compromised.
- If certificates authority's private key becomes compromised.
- Discovery that a certificate was obtained fraudulently.
- Change in the status of the certificate subject as a trusted entity.
- Change in the name of the certificate subject.

Related Work: Certificate Revocation List (CRL) is the first and the simplest method of certificate revocation mechanisms. A CRL is a periodically issued and digitally signed list containing the serial number of all the revoked certificates issued by a particular certificate authority. However, it is widely recognized [6] that CRLs are too costly and cannot provide a good degree of timeliness. Certificate Revocation System (CRS) [7] was introduced by Micali and could answer the user queries with exceptional efficiency. The main problem with this system is that it is not suitable in case of a distributed query answering system. The certificate authority to directory communication1 is too high shooting up the overall cost of the system.

Another technique for certificate revocation is the Online Certificate Status Protocol or OCSP designed by Internet Engineering Task Force (IETF). In OCSP, the certificate authority simply digitally signs the response to a certificate status query. Thus, OCSP may provide very high degree of timeliness but it is recognized to be non-scalable since the CA is required to compute a signature for answering every query. In [8], the authors proposed a new cryptosystem having attractive properties in terms of revocation. However it was not a generic revocation solution and could not be used with existing cryptosystems like RSA.

Proposed Work: In our proposed work, the MANET nodes after deployment form various clusters. For that purpose we use fuzzy C- means algorithm. After the formation of clusters, a cluster head (CH) is selected for each cluster. Each cluster head must have long transmission power and high storage of energy, so that it can operate for a long time. This avoids the task of re-electing another cluster head. After the election of each cluster head, then each CH is assigned the task of Certificate Authority (CA) by the base station. Now CHs can issue certificates to all the cluster members in its cluster. Fig. 2 shows the formation of clusters in MANET.

Certificate Revocation: Any node in the cluster can send information to the CH of that cluster. Assume that a node A suspects another node B as attacker node. Then node A informs CH about node B. Now CH alerts all the neighbouring nodes of node B to send their votes. Each vote indicates whether node B can suspect as attacker node. If the frequency of votes is greater than some threshold FT_T and the mean confidence weight is greater

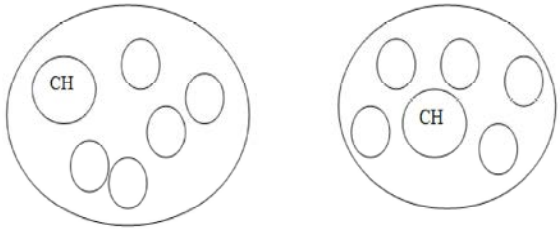

Fig. 2: Formation of Clusters

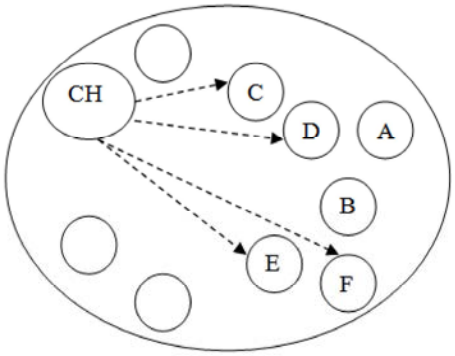

Fig. 3: Alerting by Cluster Head

than some threshold CW_T, then node B is consider as attacker node and disconnected from the network. Confidence weight of a node is calculated based on the success of votes by that node in the past voting process. Mean confidence weight is the sum of all confidence weights of the nodes involving in the voting process. For voting purpose, assume that each node in a cluster shares a public- private key pair with CH. This helps in securing the communication between CH and its members.

Let an encrypted message $E_{PRV_A}(M)$, encrypted by node A's private key, is sent by node A to CH informing that it suspects node B. The message M is

$$M = id_A || Sus(id_B) \quad (1)$$

where id_A denoted identifier of node A, $Sus(id_B)$ means that it suspecting node B. Now CH decrypts the message with node A's public key as follows:

$$M = D_{PUB_A}\,[E_{PRV_A}(id_A || Sus(id_B))] \quad (2)$$

After receiving message from node A, the CH starts voting process by sending alert messages (Fig. 3) to nodes around the suspected.

After receiving votes from neighbouring nodes of the suspected node B, if the vote's frequency is greater than some threshold FV_T, then CH calculates mean confidence weight. If it is greater than CW_T, then CH revokes certificate from B and then disconnected from the network.

Algorithm

Step 1: Deploy nodes and form a MANET.
Step 2: Form cluster using fuzzy c- means all procedure FUZZY ( )
Step 3: Elect a cluster head for each cluster
Step 4: Assign the authorities of CA to each CH
Step 5: If a node X suspects some node Y
Then: Node X sends E_{PRIVx} (M) to CH
Step 6: CH decrypts it and alerts the neighbouring node of the Suspected node Y
Step 7: If number of votes > FV_T and mean confidence weight > CW_T
Then : Node Y is suspected as intruder and revoke certificate from it.
Step 8: Disconnect node Y from network.

Procedure FUZZY( )

Step 1: Consider a membership matrix having elements with values between 0 and 1, assigned randomly based on the following equation:

$$\sum_{i=1}^{C} U_{ij} = 1 \forall_j = 1, 2, ..., n \tag{3}$$

Step 2: Calculates cluster centres $c_1, c_2, \ldots, c_n$ based on

$$c_i = \frac{\sum_{j=1}^{n} u_{ij}^m x_j}{\sum_{j=1}^{n} u_{ij}^m} \tag{4}$$

Step 3: Compute cost function using

$$J(U, c_1, \ldots, c_c) = \sum_{i=1}^{c} J_i = \sum_{i=1}^{c} \sum_{j}^{n} u_{ij}^m d_{ij}^2 \tag{5}$$

where d_{ij} is the Euclidean distance between cluster centre c_i and member j.
Step 4: Compute a new matrix using

$$u_{ij} = \frac{1}{\sum_{k=1}^{c} \left(\frac{d_{ij}}{d_{kj}} \right)^{2/(m-1)}} \tag{6}$$

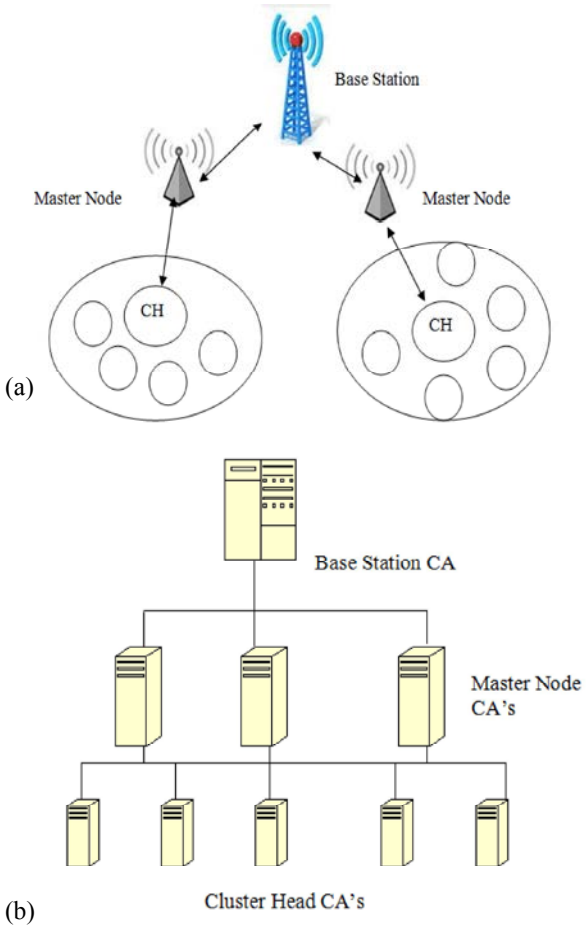

Fig. 4: (a) MANET structure (b) Hierarchy CA's

Step 5: Go to step 2.

The CA can also identify falsely accused nodes by monitoring the status of the suspected node for a predetermined time. Within that time, if it does not detect any misbehaviour from that node, then that node will be considered as legal and it informs to all its cluster members.

Hierarchical CAs: The base station, the master nodes and the cluster heads from a hierarchical structure for issuing digital certificates. The base station controls and issue certificates to master node. The master node, in turn, controls and issue certificates to cluster head of each cluster. Each cluster head manages and issue certificates to all its cluster members. If a cluster member is identified as malicious, then its certificate is revoked by its CH. If CH is identified as malicious, then its certificate will be revoked by the master node and then a new CH is elected. Fig. 4 shows clustered MANET and CA hierarchy.

CONCLUSION

Security is a major issue in mobile ad hoc networks. Identifying an intruder is the primary task of MANET security. Otherwise it degrades the performance of the overall network. In this paper, we identify a malicious node using voting mechanism. The proposed mechanism requires the formation of clusters after the deployment of MANET nodes. This helps in reducing the task of managing nodes and improving the performance and robustness of the network. After formation of clusters, a cluster head is elected for each cluster and is assigned as certificate authority for issuing certificates. Whenever a node suspects another node, it can inform CH. Now CH can alert the neighboring nodes around the suspected node and performs voting process. The voting process is based on frequency of votes as well as confidence weight of each node. This helps in identifying suspected node easily. Some times a node can falsely identify as malicious. This situation can be recovered, by assigning some predetermined time for monitoring the suspicious node by CH. If the behavior of the suspicious node is not malicious, then it can continue to work in the network. Otherwise if the node is identified as malicious, then CH revokes certificate from it and is permanently disconnected from the network. This method is energy efficient because as soon as a node is suspected by another node, then the process of intrusion detection starts, which helps in quickly identifying the malicious node.

REFERENCES

1. Goyal, P., S. Batra and A. Singh, 2010. A literature review of security attack in mobile ad-hoc networks. International Journal of Computer Applications IJCA, 9(12): 24-28.
2. Khin Sandar Win, 2008. Analysis of Detecting Wormhole Attack in Wireless Networks, World Academy of Science, Engineering and Technology, pp: 48.
3. Sitapara, N. and Prof. SB. Vanjale, 2010. International Conference, ICETE-2010 on Emerging trends in engineering on 21st Feb 2010 organized by J.J. Magdum | College Of Engineering, Jasingpur. Detection and Prevention of Black Hole Attack in Mobile Ad-Hoc Networks.
4. Yang Lu, Jiguo Li and Junmo Xiao, 2009. Threshold Certificate-Based Encryption: Definition and Concrete Construction,International Conference on Networks Security, Wireless Communications and Trusted Computing, pp: 278-282.
5. Liu, W., H. Nishiyama, N. Ansari and N. Kato, 2011. A Study on Certificate Revocation in Mobile Ad Hoc Network, Proc. IEEE Int'l Conf. Comm. (ICC).
6. Goyal Vipul, 2004. Certificate revocation lists or online mechanisms. In Eduardo Fernnandez-Medina, Julio Caesar Hernandez Castro and L. Javier Garca-Villalba, editors, WOSIS, pages 261-268. INSTICC Press.
7. Papapanagiotou, K., G.F. Marias and P. Georgiadis, 2007. A Certificate Validation Protocol for VANETs, Globecom Workshops, IEEE, pp: 1-9.
8. Yang Lu and Jiguo Li, 2009. Forward-Secure Certificate-Based Encryption, Fifth International Conference on Information Assurance and Security, pp: 57-60.
9. Jaha, A.A., F. Ben-Shatwan and M. Ashibani, 2008. Proper Virtual Private Network (VPN) Solution, International Conference on Next Generation Mobile Applications, Services and Technologies, pp: 309-314.
10. Xu Zhao, Zhai Wenyan and Cao Shanshan, 2009. New Certificate Status Verification Scheme Based on OCSP for Wireless Environment, nternational Forum on Computer Science-Technology and Applications, pp: 195-198.
11. Housley, R., W. Polk, W. Ford and D. Solo, 2002. Internet x.509 public key infrastructure certificate and certificate revocation list (crl) profile. Internet Request for Comments (RFC 3280).
12. Jaspal Kumar and M. Kulkarni, Daya Gupta, 2013. Effect of Black Hole Attack on MANET Routing Protocols, IJCNIS, 5(5).
13. Sebastian Maria and P. Arun Raj Kumar, 2013. A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and Transitory Buffer, IJCNIS, 5(8).
14. Bogdanoski Mitko, Tomislav Shuminoski and Aleksandar Risteski, 2013. Analysis of the SYN Flood DoS Attack, IJCNIS, 5(8).
15. Wei Liu, H. Nishiyama, N. Ansari and N. Kato, 2011. A Study on Certificate Revocation in Mobile Ad Hoc Networks, IEEE International Conference on Communications (ICC), pp: 5-9.