Asian Journal of Information Technology 5(6): 591-597, 2006
© Medwell Online, 2006

Security Provisions for Bandwidth Efficient Variance Adaptive Routing Protocol for Mobile Ad Hoc Network

Sanjeev Sharma, R.C. Jain and Sarita Bhadauria
School of Information Technology Rajiv Gandhi Technological
University Bhopal (M.P.) India
Department of Computer Applications Samrat Ashok Technological
Institute Vidisha (M.P.) India
Department of Electronics Engineering Madhav Institute of
Technology and Science Gwalior (M.P.) India

Abstract: Routing in Mobile Ad Hoc Networks faces many challenges that are not faced in other networks. These involve limited resources, mobility of nodes and dynamic topology and security. Thus the aim of the routing protocol should be to improve the secured communication among the nodes in the network. Controlling Delay and Delay Variance plays an important role in the functioning of a routing protocol. It helps in selecting a route that is less congested, thus helping to uniformly distribute the traffic among the underlying nodes. It helps keep the performance of the network to an optimal level. This study investigates the delay and delay variance as the route selection metrics for on demand Distance Vector routing protocol which primarily uses the distance metrics. Security mechanism for this new algorithm involves Public Key Infrastructure for key distribution Digital signatures, Hash functions in a different manner to protect the Bandwidth Efficient Variance Adaptive Routing Algorithm against various security threats..

Key words: Adhoc network, digital signature, hash chain, PKI,. routing

INTRODUCTION

Today modern civilization is bestowed with enormous advancement of Information Technology and Mobile Communication. Internet technology has added much ease and speed in all spheres of our life, from office job to personal entertainment, Emergency services like Ambulance, Natural disaster, Military and police, Besides these applications it is expected in the near future that ad hoc networking will be more intensively used for different applications such as: Digital Battlefield Communications, Movable Base-stations (for military applications), Range Extension for Cellular Telephone. Recently mobile computing has enjoyed a tremendous improvement and enhancement. Excellent rise of processing power and computing power of mobile devices deserves the credit of such proliferation.

Mobile Ad Hoc network users share resources, applications and information quickly and without the need or possibility of any centralised infrastructure. Applications of ad hoc networks include the emergency services and military sectors. Mobile ad hoc networks come together to form a network without any centralised control. Because of the limited transmission range of wireless devices, data hops across the network from source to destination, makes use of intermediate nodes. Ad hoc network nodes accept responsibility for managing the network and routing of data. Routing of data, the most intensive task, is performed in a distributed manner. To send data to a destination who is not an immediate neighbor, a node must first find a route to that destination. Intermediate nodes co-operate to forward packets from the source to the destination.

Because of the sensitive applications of ad hoc network, security is a vital factor for Mobile Ad hoc Networks. We proposed to develop a secured routing algorithm for mobile Adhoc Network which uses Delay Variance as root selection metrics and uses Hash, Digital Signatures for security of the algorithm.

PREVIOUS WORK

Wireless mobile ad hoc nature of MANET brings new security challenge to the network design. Mobile wireless networks are generally more vulnerable to information and physical security threats than fixed wired networks. Vulnerability of channels and nodes, absence of infrastructure and dynamically changing topology,

Corresponding Author: Sanjeev Sharma, School of Information Technology Rajiv Gandhi Technological University Bhopal (M.P.) India

make ad hoc networks security a difficult task[1]. Broadcast wireless channels allow message eavesdropping and injection (vulnerability of channels). Nodes do not reside in physically protected places and hence can easily fall under the attackers_control (node vulnerability). The absence of infrastructure makes the classical security solutions based on certification authorities and on-line servers inapplicable. Finally, the security of routing protocols in the MANET dynamic environment is an additional challenge.

An Intrusion detection system for Mobile Adhoc networks[2] environment proposed a framework for a distributed scheme via a ad hoc architecture that provide efficient and transparent control to the central IDE node. The system we outlined relies on security agents that monitor the network and report security alerts to the central IDS nodes via multicast messages.

To secure the data transmission a Secure Message Transmission (SMT) protocol[3] has been presented, a secure end-to-end data forwarding protocol tailored to the MANET communication requirements. SMT safeguards the communication across an unknown, frequently changing network in the presence of adversaries that exhibit arbitrary malicious behavior. In another protoco[4] for end to end secured multi media data transmission AES algorithm in association with Harr wavelet transform is used, which gives batter power efficiency as mobile nodes have limited battery backup. Flooding Attack is a novel and powerful attack against on-demand ad hoc routing protocols. This attack allows attacker to mount a denial of service attack against all on-demand routing protocols for mobile ad hoc networks, even secure on-demand routing protocols. Flooding Attack Prevention (FAP)[5] is composed of two techniques, which are neighbor suppression and path cutoff and it is able to defense the Ad Hoc Flooding Attack effectively. A routing algorithm AO2P[6] is presented for communication privacy in ad hoc networks. Node position, instead of identity, is used for route discovery. Only limited position information is revealed to the network to protect node anonymity. In an enhanced algorithm R-AO2P, the position of a reference point, instead of the position of the destination, is used to further improve destination anonymity. ABRP[7] is a hybrid routing protocol, which combines the advantages of Table based routing approach and geographic routing approach, while avoid the burden-GPS support. SEAD[8] is a secure ad hoc network routing protocol which is based on DSDV distance vector routing protocol. This protocol is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of active attackers or compromised nodes in the network. Together with existing approaches for securing the physical layer and MAC layer within the network protocol stack and shows the overhead created by the security mechanisms and the impact of these mechanisms on the protocols ability to successfully route packets.

In Listen and whisper Protocol[9] considered the problem of reducing the vulnerability of BGP in the face of mis-configurations and malicious attacks. To address this problem two techniques have been proposed: Listen and Whisper. Used together these techniques can detect and contain invalid routes propagated by isolated adversaries and a large number of problems due to misconfigurations.

SECURITY REQUIRMENTS

In most domains, the primary security service is authorization. Routing is no exception. Typically, a router needs to make two types of authorization decisions. First, when a routing update is received from the outside, the router needs to decide whether to modify its local routing information base accordingly. This is import authorization. Second, a router may carry out export authorization whenever it receives a request for routing information. Import authorization is the critical service[10].

Authorization may require other security services such as authentication and integrity. Techniques like digital signatures-and message authentication codes are used to provide these services.

In the context of routing, confidentiality and non-repudiation are not necessarily critical services[11] and non-repudiation is useful in an ad hoc network for isolating misbehaving routers: a router A which received an erroneous message from another router B may use this message to convince other routers that B is misbehaving. This would indeed be useful if there is a reliable way of detecting erroneous messages. This does not appear to be an easy task.

Although of course it would be desirable, it does not seem to be feasible to prevent denial-of-service attacks in a network that uses wireless technology (where an attacker can focus on the physical layer without bothering to study the routing protocol).

Therefore, in this study we consider the following requirements:

Import authorization: It is important to note that in here we are not referring to the traditional meaning of authorization. What we mean is that the ultimate authority on routing messages regarding a certain destination node is that node itself. Therefore, we will only authorize route information in our routing Table if that route information concerns the node that is sending the information. In this way, if a malicious node lies about it, the only thing it will cause is that others will not be able to route packets to the malicious node.

Source authentication: We need to be able to verify that the node is the one it claims to be.

Integrity: In addition, we need to be able to verify that the routing information that it is being sent to us has arrived unaltered.

The two last security services combined build data authentication and they are requirements derived from our import authorization requirement.

VARIANCE ADAPTIVE ROUTIG PROTOCOL

In this protocol when a node receives a broadcast route request message, it first checks to see whether it has received a route request packet with the same Source IP Address field within the last BCAST_ID_SAVE milliseconds. If such a route request has been received, the node silently discards the newly received route request. Otherwise, the node checks to see whether it has a route to the destination. If the node does not have a route, it rebroadcasts the route request from its interface(s) with the same field values, but using its own IP address in the IP header of the outgoing route request. The Time To Live or hop limit field in the outgoing IP header is decreased by one. The Hop Count field in the broadcast route request message is incremented by one, to account to the new hop through the intermediate node. In this case, the node also creates a reverse route to the Source IP Address in its routing Table with next hop equal to the IP address of the neighboring node that sent the broadcast route request (often not equal to the Source IP Address field in the route request message). This reverse route might be used for an eventual route replay back to the original node making the route request (identified by the Source IP Address). The reverse route is put into the route Table with lifetime REV_ROUTE_LIFE milliseconds.

Node also calculates the route delay and the variance and places these values in the route Table entry. If the node has a route to the destination and the node's existing dest-seqno is greater than or equal to the Destination Sequence Number of the route request, then the node generates a route replay .It checks for the delay in the route request packet against the value in the corresponding route Table entry to ascertain the shortest delay. If the route request delay is smaller than the one that is compared with, than that route is selected and route entry is accordingly updated. If the delay difference is found to be zero, then delay variances are compared. The one with the lower value is selected and route Table entry is accordingly updated. In each case the node generates a route replay.

SECURITY ISSUES IN VARIANCE ADAPTIVE ROUTIG PROTOCOL

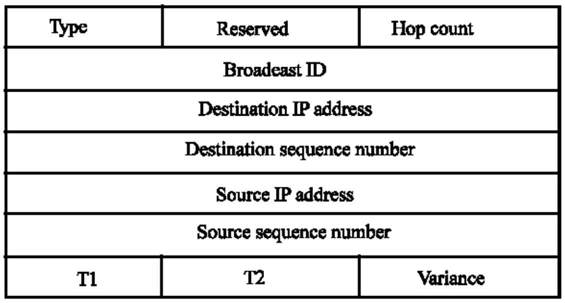
Study of Variance adaptive routing protocol shows that there is no security mechanisms incorporated in the protocol, malicious nodes can perform many attacks just by not behaving according to this protocol rules. A malicious node *M* can carry out the following attacks against this protocol:

- Impersonate an originator node by forging a Route Request with its address as the originator address.
- When forwarding a Route Request generated by source node to discover a route to destination, reduce the hop count field and delay variance by placing illegal timestamps on Route Request packet to increase the chances of being in the route path between source and destination so it can analyze the communication between them. A variant of this is to increment the destination sequence number to make the other nodes believe that this is a 'fresher' route.
- Impersonate a destination node by forging a Route Replay with its address as a destination address.
- Impersonate a node by forging a Route Replay that claims that the node is the destination and, to increase the impact of the attack, claims to be a network leader of the subnet with a big sequence number and send it to its neighbors. In this way it will became a black hole for the whole subnet . In this type of attack a malicious node advertises itself as the shortest path to other nodes and drops all packets which come on it. The trust guarantor of the malicious node will set a low trust value for the malicious node. Therefore, the node that wants to send a packet will discard the routing path that goes through the malicious node. A special case of the black hole attack is an grey-hole attack. In this attack the adversary selectively drops some kinds of packets but not other. For example the attacker might forward routing packets but not data packets this is known as Gray-hole attack.
- Selectively, not forward certain Route Requests and Route Replays not reply to certain Route Replays and not forward certain data messages. This kind of attack is especially hard to even detect because transmission errors have the same effect. It is the major security issue with variance adaptive routing protocol.

- Forge a Route Error message pretending it is the originator node and send it to its neighbor destination node is also possible in the variance adaptive routing protocol. In this case the Route Error message has a very high destination sequence number for one of the unreachable destinations. This might cause destination node to update the destination sequence number corresponding to unreachable destinations with the value dsn and therefore, future route discoveries performed by destination to obtain a route to unreachable destinations will fail.
- In this protocol, the originator of a Route Request can put a much bigger destination sequence number than the real one. In addition, sequence numbers wraparound when they reach the maximum value allowed by the field size. This allows a very easy attack in where an attacker is able to set the sequence number of a node to any desired value by just sending two Route Request messages to the node. This problem is also available with AODV[12] routing protocol which is most popular routing protocol in Mobile Adhoc Network.
- Variance adaptive routing protocol keeps a sequence number for duplication suppression at every node. An attacker can distribute a large number of route requests with increasing sequence numbers forged to appear to be from other nodes. This way when the actual route request is sent out many nodes suppress it as a duplicate and thereby disrupt the actual route discovery; this is known as Rushing Attack[13].

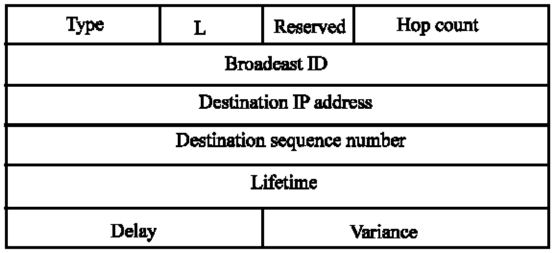
SECURITY PROVISIONS FOR VARIANCE ADAPTIVE ROUTIG PROTOCOL

We assume that there is a key management sub-system that makes it possible for each ad hoc node to obtain public keys from the other nodes of the network. Further, each ad hoc node is capable of securely verifying the association between the identity of a given ad hoc node and the public key of that node. How this is achieved depends on the key management scheme.



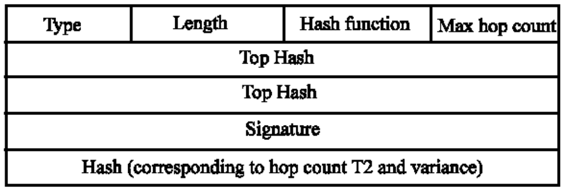
Type	Reserved	Hop count
Broadcast ID		
Destination IP address		
Destination sequence number		
Source IP address		
Source sequence number		
T1	T2	Variance

Fig. 1: Route request message format of variance adaptive routing protocol



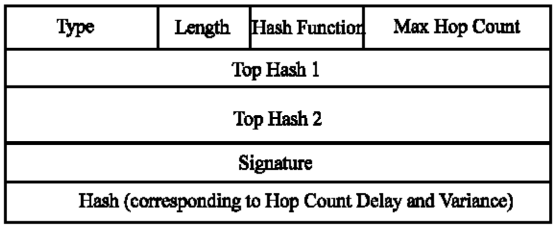
Type	L	Reserved	Hop count
Broadcast ID			
Destination IP address			
Destination sequence number			
Lifetime			
Delay		Variance	

Fig. 2: Route replay message format of variance adaptive routing protocol



Type	Length	Hash function	Max hop count
Top Hash			
Top Hash			
Signature			
Hash (corresponding to hop count T2 and variance)			

Fig. 3: Route request security extension of variance adaptive routing protocol



Type	Length	Hash Functio	Max Hop Count
Top Hash 1			
Top Hash 2			
Signature			
Hash (corresponding to Hop Count Delay and Variance)			

Fig. 4: Route replay security extension of variance adaptive routing protocol

Like SAODV[14] two mechanisms are used to secure the Variance Adaptive Routing Protocol messages: digital signatures to authenticate the non-muTable fields like Destination IP address, Destination sequence number, Source IP address, Timestamp and Source sequence number of the messages and hash chains to secure mutable information like hop count information, Variance and Timestamp at current node. For the non-mutable information, authentication is performs in an end-to-end manner, but the same kind of techniques cannot be applied to the mutable information. Fig. 1 shows the structure of the Variance adaptive routing protocol route request message and Fig. 2 shows the route reply messages format and indicate what are the mutable fields of the messages.

The information relative to the hash chains and the signatures is transmitted with the Variance adaptive routing protocol message as an extension message that we will refer to as Signature Extension. The format of the Secured Variance adaptive routing protocol Signature Extensions is shown in Figs 3 and 4.

Hash chains: Proposed protocol uses hash chains to authenticate the hop count of RREQ and RREP messages in such a way that allows every node that receives the message (either an intermediate node or the final destination) to verify that the hop count, variance and have not been decremented and timestamp has not been altered by an attacker. This prevents an attack when forwarding a Route Request generated by sender node to discover a route to destination, reduce the hop count field and delay variance by placing illegal timestamps on Route Request packet to increase the chances of being in the route path between sender and destination so it can analyze the communication between them. A hash chain is formed by applying a one-way hash function repeatedly to a seed. Every time a node originates a route request or a route replay messages, it performs the following operations:

- Generates a random number (seed).
- Sets the Max Hop Count field to the TTL value (from the IP header).

Max_Hop_Count = TTL

- Sets the Hash field to the seed value.

Hash = seed

- Sets the Hash _Function field to the identifier of the hash function that it is going to use.

Hash Function = h

- Calculates Top Hash by hashing seed Max Hop Count times.

Top_Hash = $h^{\text{Max Hop Count}}$ (seed)

Where:

– h is a hash function.

– hi (x) is the result of applying the function h to x i times.

- Sets the Max Delay field to the double TTL value (from the IP header).

Max Delay = 2*TTL

- Sets the Hash field to the seed value.

Hash = seed

- Sets the Hash _Function field to the identifier of the hash function that it is going to use.

Hash Function = h

- Calculates Top Hash by hashing seed Max Delay times.

Top_Hash = $h^{\text{Max Delayt}}$ (seed)

Where:

– h is a hash function.

– hi (x) is the result of applying the function h to x i times.

In addition, every time a node receives a route request or a route replay message, it performs the following operations in order to verify the hop count:

- Applies the hash function h Maximum Hop Count minus Hop Count times to the value in the Hash field and verifies that the resultant value is equal to the value contained in the Top Hash field.

Top Hash1 = $h^{\text{Max Hop Count-Hop Count}}$(Hash)

Top Hash2 = $h^{\text{Max Delay-variance}}$(Hash)

Where:

– a = = b reads: to verify that a and b are equal.

- Before rebroadcast a route request or forwarding a route replay, a node applies the hash function to the Hash value in the Signature Extension to account for the new hop.

Hash = h(Hash)

The Hash Function field indicates which hash function has to be used to compute the hash. Trying to use a different hash function will just create a wrong hash without giving any advantage to a malicious node. Hash Function, Max Hop Count, Top Hash1, Top Hash2 and Hash fields are transmitted with the AODV message, in the Signature Extension. And as it will be explained in the next subsection, all of them but the Hash fields are signed to protect its integrity

Digital signatures: By using Digital Signatures we can prevent attacks for Impersonation of sander node by forging a Route Request with its address as the originator address and for Impersonation of destination node by forging a Route Replay with its address as a destination address.

Like SAODV this protocol uses digital signatures to protect the integrity of the non-mutable data in route request and route replay messages. That means that they sign everything but the Hop Count, variance and timestamp T1 of the variance adaptive routing protocol message and the Hash from the extension. The main problem in applying digital signatures is that like AODV this protocol also allows intermediate nodes to reply route request messages if they have a ‘fresh enough’ route to the destination. While this makes the protocol more efficient it also makes it more complicated to secure. The problem is that a route replay message generated by an intermediate node should be able to sign it on behalf of the final destination. And in addition, it is possible that the route stored in the intermediate node would be created as a reverse route after receiving a route request message.

For solving such problem there are two approaches the first one is that, if an intermediate node cannot reply to a route request message because it cannot properly sign its route replay message, it just behaves as if it didn’t have the route and forwards the route request message. This approach compromises efficiency of protocol and thus delay in route discovery is result.

The second one is complex but works without compromising efficiency of protocol. In this approach when every time a node generates a route request message, it also includes the route replay flags with it, the prefix size and the signature that can be used (by any intermediate node that creates a reverse route to the originator of the RREQ) to reply a route request that asks for the node that originated the first route request. Moreover, when an intermediate node generates a route replay message, the lifetime of the route has changed from the original one. Therefore, the intermediate node should include both lifetimes (the old one is needed to verify the signature of the route destination) and sign the new lifetime. In this way, the original information of the route is signed by the final destination and the lifetime is signed by the intermediate node.

When a node receives a route request, it first verifies the signature before creating or updating a reverse route to that source. Only if the signature is verified, will it store the route. If the route request was received with a Double Signature Extension, then the node will also store the signature for the route replay and the lifetime in the route Table. An intermediate node will reply to a route request with a route replay. The node has the corresponding signature and old lifetime to put into the Signature and Old Lifetime fields of the route replay Double Signature Extension. Otherwise, it will rebroadcast the route request.

When a route request is received by the destination itself, it will reply with a route replay. This route replay will be sent with a route replay Single Signature Extension. When a node receives a route replay, it first verifies the signature before creating or updating a route Table entry to that host. Only if the signature is verified, it will store the route with the signature of the route replay and the lifetime.

Key management: To secure the routing within the ad hoc network the security extensions for variance adaptive routing protocol are used. The extension is basically a signature of the message and a hash-value used in a hash chain to secure the hop count, variance and timestamp at current node. For the protocol to work as expected each node must be able to verify the signatures which is the main problem in this setup. Also, the verification process of the agent advertisement is also in need of a certificate of authenticity.

To be able to verify a signature the verifying node must know the public key of the source node. The key can simply be sent by the source node along with the data packet. However, this will not be very secure since just about anyone can send out a key claiming to belong to someone else. Authentication is very necessary. As always, this is usually provided with the help of certificates. But a certificate itself is often relatively large and does not fit well to bee sent around in each routing packet. Instead an ad hoc protocol is needed to get the certificate of a specified host. In this case I propose to use a limited broadcast to ask any neighbor for the valid certificate. The assumption is that each node has a certificate containing its own public key and that the certificate is signed by some Certification Authority. Certification Authority is a trusted third party (TTP) for all nodes in the network, either explicit or implicit.

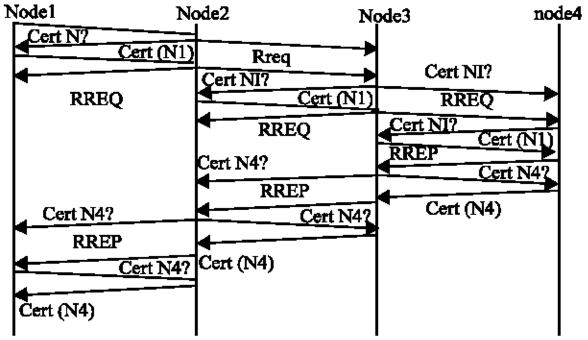


Fig. 5: Route discovery and on demand distribution of certificates. N1is trying to find a route to N4

When a node needs to find a specific certificate for verification of routing packets it can send out a limited broadcast. That is, a broadcast with a time to live set to one. This way it will not pollute the entire network. Since the request is only used for getting the certificate for routing packets it is guaranteed that at least one. of the neighbors already knows about this certificate and can forward it to the one in need.

The process of finding a route between two hosts in an ad hoc network is exemplified in Fig. 5. In this example the node1 is trying to reach node 4 in a simple network. Broadcasts are shown as messages going to more than one destination. To make the route requests more efficient in the future each node should cache the certificates. This way a certificate may only be asked for once for each node. The size of the cache should be large enough to hold a reasonable amount of certificates for proper operation. The number of certificates could be managed by a simple cache algorithm that throws out the least recently used certificate if the cache space is limited.

DISCUSSION

This protocol is not meant to yield any confidentiality since this is usually not needed or desired in general Adhoc networks. The protocol does provide means to get authentication, integrity and non-repudiation of the routing control packets. The protocol extensions use asymmetric cryptography to achieve authentication by signing the data packets with the private key. This allows for the destination node and all intermediate nodes, to validate the request. Also, this allows for the nodes to be certain that no one has altered the packets. So provides batter security as it allows hashing variance as well as hop count.

ACKNOWLEDGMENT

The authors are grateful to their colleagues at School of Information Technology, Center of excellence in Information Technology, Rajiv Gandhi Technological University M.P. India for their advice and encouragement and providing us such a nice infrastructure for doing our research work.

REFERENCES

1. Buttyan, L. and J.P. Hubaux, 2002. Report on a working session on security in wireless ad hoc networks, Mobile Computing and Communications Review, pp: 4.
2. Sanjeev Sharma and Gunjan Saxena, 2005. ”The Autonomous agent system for intrusion detection in wireless ad hoc networks” Networks 2005, National conference on Networks, Organised by CSI, DAVV, pp: 7-14.
3. Panagiotis Papadimitratos and J. Zygmunt Haas, 2003. Secure message transmission in mobile ad hoc networks” Ad Hoc Networks, Elsevier pp: 193-209.
4. Sharma Sanjeev, R.C. Jain Bhadauria, Sarita Singh, (In Press) A Power Efficient Encryption Algorithm for Multimedia Data in Mobile Adhoc Network, J. Trends in Applied Science Reserch, Academic press.
5. Ping Yi, Zhoulin Dai, Yiping Zhong and Shiyong Zhang, 2005. “Resisting Flooding Attacks in Ad Hoc Networks” Proceedings of the IEEE Intl. Conference on Information Technology: Coding and Computing (ITCC’05).
6. Xiaoxin Wu and Bharat Bhargava, 2005. AO2P: Ad Hoc On-Demand Position-Based Private Routing Protocol IEEE Transactions on Mobile Computing, pp: 335-348.
7. Huaizhi Li and M. Singhal, 2005. A Scalable Routing Protocol for Ad Hoc Networks, in the Proc. of IEEE 61st Semiannual Vehicular Technology Conference, (Mobile Networks), Stockholm, Sweden.
8. Yih-Chun Hu, B. David Johnson B., Adrian Perrig, 2003. “SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks” Intl. J. Ad Hoc Networks, Elsevier Press, pp: 175-192.
9. Lakshminarayanan Subramanian, 2004. Volker Roth, Ion Stoica, Scott Shenker and Randy H. Katz. Listen and Whisper: Security Mechanisms for BGP, First Symposium on Networked Systems Design and Implementation (NSDI'04).
10. Kumar, B., 1993. “Integration of Security in Network Routing Protocols”. In ACM SIGSAC, pp: 18-25.
11. Zhou, L. and Z.J. Haas, 1999. Securing ad hoc networks. IEEE Network Magazine, pp: 24-30.
12. Perkins, C.E., E.M. Royer and S.R. Das, 2002. Ad hoc on-demand distance vector (AODV) routing. IETF INTERNET DRAFT, MANET working group draft-ietf-manet-aodv-10.txt.
13. Yih-Chun Hu, Adrian Perrig and David Johnson, 2003. Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. Proceedings of ACM Workshop on Wireless Security (WiSe 2003), ACM Press, pp: 30-40.
14. Manel Guerrero Zapata, 2005. Secure ad hoc on-demand distance vector (SAODV) routing, draft-querrero-manet-saodv-03, Mobile Ad Hoc Networking Working Group.