Journal of Computer Science 4 (7): 538-544, 2008
ISSN 1549-3636
© 2008 Science Publications

A Novel Routing Technique against Packet Dropping Attack in Adhoc Networks

[1]N. Bhalaji, [2]Sinchan banerjee and [3]A.Shanmugam
[1]Hindustan University, Chennai, India
[2]Srm University, Chennai, India
[3]Bannari Amman Institute of Technology, Erode, India

Abstract: Problem Statement: Mobile adhoc networks (MANETs) were extensively used in defense and rescue applications. The dynamic topology of MANETs allows nodes to join and leave the network at any point of time. This dynamic property of MANET has rendered it vulnerable to various security attacks. Many trust establishment methods were proposed to increase the security in MANET. In this paper we propose a new trust based relationship among the nodes to combat the packet dropping attack. **Approach:** In the proposed scheme we considered the dynamic source routing protocol for simulation due to its common usage and flexible nature. Network simulator-2 was used for the simulation and the standard DSR and proposed relationship enhanced DSR were compared. **Results:** The result of the proposed scheme was compared with the standard DSR protocol. The performance metrics such as normalized throughput, packet delivery ratio, dropped data packets and ratio between the total drop and malicious drops were used for the comparison study. The results obtained prove that the proposed scheme outscores the traditional DSR protocol in all aspects. **Conclusions/Recommendations:** The proposed trust enhanced dynamic source routing protocol provides the solution for the possible packet dropping attack in an adhoc network. As the results show it has enhanced technique for encountering such type of attacks when compared to the traditional DSR protocol.

Keywords: Mobile adhoc networks, Dynamic source routing protocol, Novel routing, grudger protocol

INTRODUCTION

Mobile Wireless Adhoc Network (MANET) is a group of autonomous mobile nodes or devices connected through wireless links without the support of a communications infrastructure. The topology of the network changes dynamically as nodes move and the nodes reorganize themselves to enable communications with nodes beyond their immediate wireless communications range by relaying messages for one another[1], i.e., multihop.

MANET relies on the cooperation of all the participating nodes. The more nodes cooperate the more powerful a MANET becomes. But supporting MANET requires detecting routes and forwarding packets[2] which may cost them to loose their energy[3]. Therefore there is a strong motivation for a node to deny packet forwarding to other, while at the same time using their services to deliver own data.

Current schemes of detecting node misbehavior in MANET are mostly centered on using incentives, reputation[4] or price-based mechanisms[5] to achieve the desired effect of nodes cooperation.

In an adhoc network one of the major concerns is how to increase the routing security in presence of malicious nodes. In our approach we calculate trust values of nodes based on certain attributes and by using appropriate threshold values. We have classified the nodes in to three categories based on their trust values.

DSR protocol: Dynamic Source Routing is a protocol developed for routing in mobile ad-hoc networks and was proposed for MANET by[6]. In a nutshell, it works as follows: Nodes send out a ROUTE REQUEST message, all nodes that receive this message put themselves into the source route and forward it to their neighbors, unless they have received the same request before. If a receiving node is the destination, or has a route to the destination, it does not forward the request, but sends a REPLY message containing the full source route. It may send that reply along the source route in reverse order or issue a ROUTE REQUEST including the route to get back to the source, if the former is not possible due to asymmetric links. ROUTE REPLY messages can be triggered by ROUTE REQUEST

Corresponding Author: N. Bhalaji, Hindustan University, Chennai, India

messages or are gratuitous. After receiving one or several routes, the source selects the best (by default the shortest), stores it and sends messages along that path. The better the route metrics (number of hops, delay, bandwidth, or other criteria) and the sooner the REPLY arrives at the source, the higher the preference given to the route and the longer it will stay in the cache. When a ROUTE REPLY arrives very quickly after a ROUTE REQUEST has been sent out this is an indication of a short path, since the nodes are required to wait for a time corresponding to the length of the route they can advertise, before sending it. This is done in order to avoid a storm of replies. In case of a link failure, the node that cannot forward the packet to the next node sends an error message towards the source. Routes that contain a failed link can be `salvaged' by taking an alternate partial route that does not contain the bad link. Since DSR has no security mechanism they are vulnerable to many type of attacks. It assumes all nodes cooperate in the network so in its present status cannot defend itself from attacks.

Security attacks in MANET: The main assumption of the adhoc routing protocols is that all participating nodes do so in good faith and without maliciously disrupting the operation of the protocol[7,8]. However, the existence of malicious entities cannot be disregarded in any system, especially in open ones like adhoc networks. The RPSEC IETF working group has performed a threat analysis that is applicable to routing protocols employed in a wide range of application scenarios[9]. According to this study, the routing function can be disrupted by internal or external attackers. An internal attacker can be any legitimate participant of the routing protocol. An external attacker is defined as any other entity. The strongest assumption for an external attacker is that it is able to eavesdrop the communication between two legitimate network participants, inject fabricated messages and delete, alter or replay captured packets. Weaker assumptions of external attackers include the ability to inject messages but not read them, or read and replay messages but not inject new ones, or just the ability to read messages. Cryptographic solutions can be employed to prevent the impact of external attackers by mutual authentication of the participating nodes through digital signature schemes[10]. However, the underlying protocols should also be considered since an attacker could manipulate a lower level protocol to interrupt a security mechanism in a higher level. Although these attacks are a significant part of a complete threat assessment, our analysis focuses only on network-layer threats and countermeasures.

Internal attackers have the capabilities of the strongest outside attacker, as they are legitimate participants of the routing process. Having complete access to the communication link they are able to advertise false routing information at will and force arbitrary routing decisions on their peers[11]. One of the most difficult to detect problems in routing is that of Byzantine failures. These failures are the result of nodes that behave in a way that does not comply with the protocol. The reasons for the erroneous behavior could be software or hardware faults, mistakes in the configuration, or malicious compromises. Attempts to solve the problem of Byzantine failures have been proposed for both infrastructures[12] and infrastructure less networks[13].

Based on this threat analysis and the identified capabilities of the potential attackers, we will now discuss several specific attacks that can target the operation of a routing protocol in an adhoc network.

Location disclosure[14]: Location disclosure is an attack that targets the privacy requirements of an adhoc network. Through the use of traffic analysis techniques[15] or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, or even the structure of the entire network.

Black hole[11]: In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination. These fake replies can be fabricated to divert network traffic through the malicious node for eavesdropping, or simply to attract all traffic to it in order to perform a denial of service attack by dropping the received packets.

Replay[9]: An attacker that performs a replay attack injects into the network routing traffic that has been captured previously. This attack usually targets the freshness of routes, but can also be used to undermine poorly designed security solutions.

Wormhole[16]: The wormhole attack is one of the most powerful presented here since it involves the cooperation between two malicious nodes that participate in the network. One attacker, say node A, captures routing traffic at one point of the network and tunnels them to another point in the network, say to node B, that shares a private communication link with A. Node B then selectively injects tunneled traffic back into the network. The connectivity of the nodes that have established routes over the wormhole link is completely under the control of the two colluding attackers.

Blackmail[17]: This attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist the offender. An attacker may fabricate such reporting messages and try to isolate legitimate nodes from the network. The security property of non-repudiation can prove to be useful in such cases since it binds a node to the messages it generated[18].

Denial of service: Denial of service attacks aim at the complete disruption of the routing function and therefore the whole operation of the adhoc network. Specific instances of denial of service attacks include the routing table overflow[14] and the sleep deprivation torture[19]. In a routing table overflow attack the malicious node floods the network with bogus route creation packets in order to consume the resources of the participating nodes and disrupt the establishment of legitimate routes. The sleep deprivation torture aims at the consumption of batteries of a specific node by constantly keeping it engaged in routing decisions.

MATERIALS AND METHODS

In our proposed scheme we classify the relationship among the nodes and their neighboring nodes in to three types as below. In an adhoc network the relationship between any node x and node y will be determined as follows.

Unknown:

- Node x have never sent/received any messages to/from node y
- Trust levels between them are very low
- Probability of malicious behaviour is very high
- Newly arrived nodes are grouped in to this category

Known:

- Node x have sent/received some messages to/from node y
- Trust levels between them are neither low nor too high
- Probability of malicious behaviour is to be observed

Friend:

- Node x have sent/received plenty of messages to/from node y
- Trust levels between them are very high
- Probability of malicious behaviour is very less

The above relationships are represented in a relationship table which is part of every node in the adhoc network. Consider the node 1in the diagram the relationship table of the node 1 is shown in Table 1.

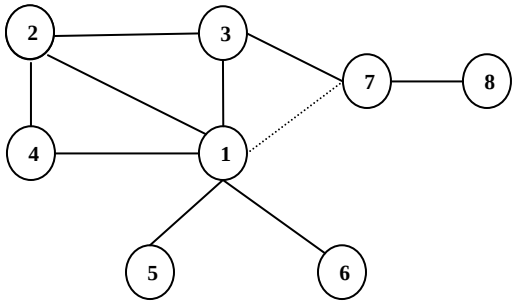

Fig.1: Nodes in Adhoc network

Table I: Relationship Table for Node 1 in Fig.1

Neighbors	Relationship
2	F
3	F
4	K
5	F
7	UK

Relationship estimator technique: The relationship status which we discussed in the previous section depends up on the trust value and threshold values. The trust values are calculated based on the following parameters of the nodes. We propose a very simple equation for the calculation of trust value.

$$R1 = \frac{\text{Number of packets forwardedsuccessfully by neighbor node}}{\text{Total number of packets tobe forwarded by neighbor node}}$$

A = Acknowledgement bit. (0 – 1)
L = Length of Active Association (0-1)
T = Trust value
T = Tanh (R1+A+L)

The threshold trust level for an unknown node to become a known to its neighbor is represented by T_K and the threshold trust level for a known node to become a friend of its neighbor is denoted by T_F. The relationships are represented as:

R (node x → node y) = F when $T \geq T_F$
R (node x → node y) = K when $TK \leq T < T_F$
R (node x → node y) = UK when $0 < T \geq T_K$

Also, the relationship between nodes is asymmetric, (i.e.,) R (node x → node y) is a relationship evaluated by node x based on trust levels calculated for its neighbor node y. R (node y → node x) is the relationship from the friendship table of node y. This is evaluated based on the trust levels assigned for its neighbor. Asymmetric relationships suggest that the direction of data Flow may be more in one direction. In other words, node x may not have trust on node y the same way as node y has trust on node x or vice versa.

The Threshold parameters are design parameters. Simulation is to be carried out with suitable values or all the parameters and the threshold thrust levels so as to obtain optimum performance. There is a trade off between offering good security in adhoc networks and overall throughput of the network. Hence, choosing an optimal value is crucial for the good functioning of the network.

Routing mechanism when any node wishes to send messages to a distant node, its sends the ROUTE REQUEST to all the neighboring nodes. The ROUTE REPLY obtained from its neighbor is sorted by trust ratings. The source selects the most trusted path. If its one hop neighbor node is a friend, then that path is chosen for message transfer. If its one-hop neighbor node is a known or unknown and if the one hop neighbor of the second Best path is a friend chooses F. Similarly an optimal path is chosen based on the degree of Relationship existing between the neighbor nodes. The above said concept is illustrated in Table 2.

Table 2: Path preference among nodes

Next hop Neighbor in the best path P1	Next hop neighbor in the next best path P2	Action taken
F	F	F is chosen in P1 or P2 based on the length of path
F	K	F is chosen in P1
K	F	F in path P2
K	K	A is chosen in P1 or P2 based on the length of the path
F	UK	F is chosen in P1
UK	F	F in path P2

The source selects the shortest and the next shortest path. Whenever a neighboring node is a friend, the message transfer is done immediately. This eliminates the overhead of invoking the trust estimator between friends. If it is a known or unknown, transfer is done based on the ratings. This protocol will converge to the DSR protocol if all the nodes in the adhoc network are friends.

For the performance analysis of the protocol extensions, a regular well-behaved DSR network is used as a reference. We then introduce compromised stranger nodes into the network which doesn't forward the packets. The network should identify these malicious nodes and not upgrade them to known nodes. In the similar manner, some known are later made to be malicious. Simulations are carried out for the forwarding defection of the nodes. The simulation is being implemented In Network Simulator 2[24], a simulator for mobile adhoc networks. The simulation parameters are tabulated in Table 3.

Table 3: Simulation parameter

Parameter	Value
Application traffic	CBR
Radio range	250 m
Packet size	512 bytes
Transmission rate	4 packets sec^{-1}
Pause time for nodes	60 s ec
Maximum speed	1 m sec^{-1}
Simulation time	600 sec
Number of nodes	25
Area	1000*1000 m
Available bandwidth	1 Mb sec^{-1}

The speed of 1 m sec^{-1} corresponds to slow moving. For a simulation that last 600 sec, approximately 30000 CBR packets are sent. This number is considered high enough to eliminate any deviations influence on the results. With 1 Mb sec^{-1} bandwidth, a packet size of 512 bytes and a transmission rate of 4 packets sec^{-1}, congestion of the network is not likely to occur.

RESULTS

In this section we discuss about the performance metrics used for analyzing the performance of both standard and proposed protocols.

Performance metrics: In our simulations we use several performance metrics to compare the improved DSR protocol with the existing one. Studies of performance evaluations of routing protocols for mobile adhoc networks indicate that the following metrics are defined:

Packet delivery ratio: it is the ratio of the number of packets received and the number of packets sent.

Throughput: This gives the fraction of the channel capacity used for data transmission.

For the performance analysis of the Relationship enhanced DSR protocol the throughput is compared with the standard DSR with malicious nodes. The other parameters to be considered are path optimality and

routing overhead. Due to the introduced acknowledgment scheme in the standard DSR number acknowledgement packets will be the overhead for the proposed protocol. The Protocol is also tested based on the malicious drops over total drops in the network. The path optimality is another concern because when there is only choice of route containing the malicious nodes. As far as number of alternative routes exists this protocol well works by choosing the optimal paths.

The relationship enhanced DSR protocol is tested under different scenarios by varying the number of malicious nodes and node moving speed. It is also tested varying the number of nodes in simulation used.

The Packet Delivery Ratio is used to compare the existing DSR protocol and the Relationship enhanced DSR protocol to determine the influence of the trust based routing to the DSR protocol. The simulation results are presented in Fig. 2.

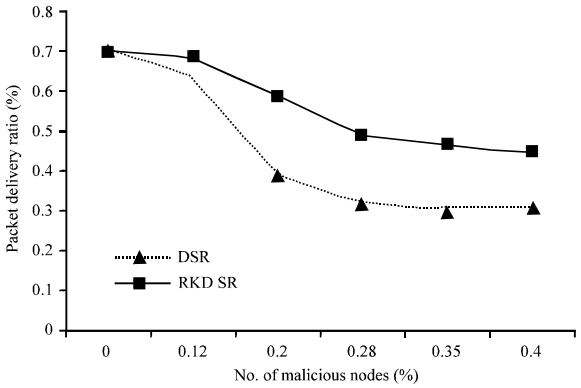

Fig. 2: Comparison of packet delivery ratio

We carried out another simulation to determine the amount of packets that are dropped by malicious nodes from the total dropped packets.

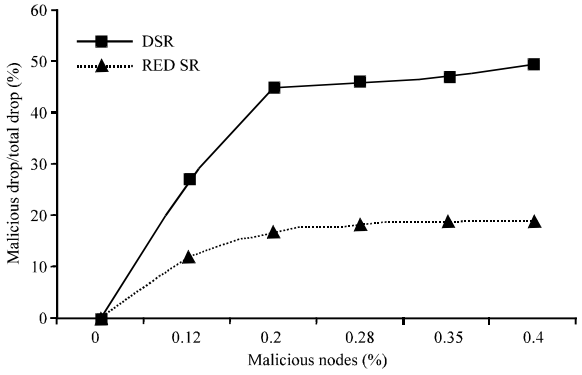

Fig. 3: Comparison of malicious drop/total drop

The next simulation was done to evaluate the throughput. The normalized throughput of proposed Relationship enhanced DSR protocol and standard DSR were compared.

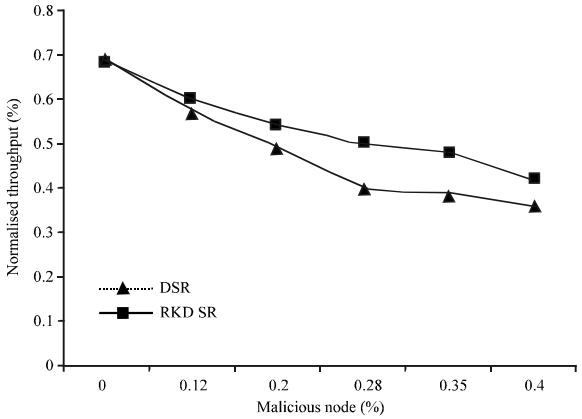

Fig. 4: Comparison of Normalised Throughput

We also conducted another simulation to determine the percentage of dropped data packets for proposed one and standard protocol.

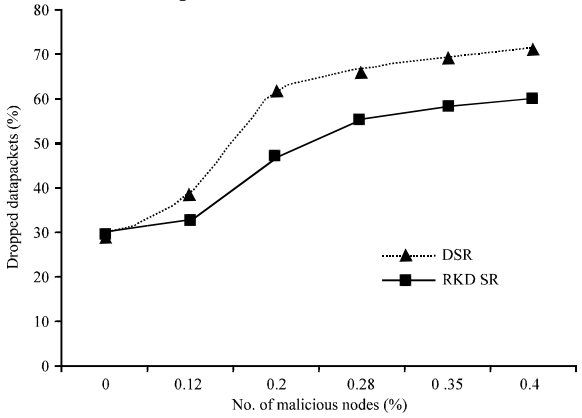

Fig. 5: Comparison of dropped packets

DISCUSSION

In our proposed study we use a very simple and effective way of calculating trust so as to select the reliable route in presence of the malicious nodes which do not forward packets. The standard protocols are vulnerable to nonforwarding attacks. From the graphs illustrated in results we can easily infer that the performance of the standard DSR drops under the presence of malicious nodes, where as the proposed scheme of relationship enhanced DSR performs well as

it selects the nodes, based on the calculated trust values. In our scheme the nodes are separated in to three categories based on their nature of operation and trust value which they possess.
In this section we have discussed about the various works which acted as a background for our proposed assumption and which also served as a foundation for conducting the experiments.

As explained in[20] it is an application from a biological example proposed by Dawkins, which explains the survival chances of birds grooming parasites off each others head. Dawkins introduces three categories of the birds namely

- Suckers which are good natured, helpful and favor others by grooming parasites off others head
- Cheats which get help from others but fail to return the favor
- Grudger who starts out being helpful to every bird, but bears a grudge against those birds that don't return the favor and subsequently no longer help them

In an adhoc network, grudger nodes[21] are introduced which employ a neighborhood watch by keeping track of what is happening to other nodes in the neighborhood, before they have a bad experience themselves. They also share information of experienced malicious behavior with friends and learn from them. The protocol consists of the following components.

Monitor: It registers deviation of normal behavior and manages them in the watch table. On detection of bad behavior, an alarm is sent to the reputation system and trust manager.

Reputation system: It manages a table consisting of entries for nodes and their rating. Local rating lists or black lists are maintained with friends and potentially exchanged with friends.

Path manager: It performs functions like path re-ranking according to security metric, path deletion containing malicious nodes and action to be taken on receiving request for a route from a malicious node.

Trust manager: It calculates trust levels, manages trust table entries for trust level administration, forwarding of alarm messages and filtering of incoming message based on the trust level of a reporting node.

Watchdog and pathrater: The routing misbehavior is mitigated by including components like watchdog and pathrater in the scheme proposed by[22]. Every node has a Watchdog process that monitors the direct neighbors by promiscuously listening to their transmission. Main draw back of this idea is that it enables the misbehaving node to participate in the network cooperation without punishing.

Confidant: (Cooperation of Nodes: Fairness in Dynamic Adhoc Networks) The CONFIDANT protocol works as an extension to reactive source routing protocols like DSR[23]. The basic idea of the protocol is that nodes that does not forward packets as they are supposed to, will be identified and expelled by the other nodes. Thereby, a disadvantage is, if a node is found to be intolerable then all the routes which consists of this node will be deleted.

CONCLUSION

In this study we have discussed the characteristics of mobile adhoc network. We also analyzed the different types of attacks in an adhoc environment. This proposed scheme of Relationship Enhanced DSR protocol increases the security in routing and also encourages the nodes to cooperate in the adhoc structure. It identifies the malicious nodes and isolates them from the active data forwarding and routing.

REFERENCES

1. Siva Ram Murthy, C. and B. S. Manoj, 2004. Adhoc Wireless Networks: Architectures and Protocols. Ist Edn., Prentice Hall, USA., ISBN: 10: 013147023X, pp: 880.
2. Murthy, S. and J.J. Garcia-Luna-Aceves, 1996. An efficient routing protocol for wireless networks. ACM Mobile Networks Appl., 1: 183-197. DOI: 10.1007/BF011933336.
3. Djamel Djenouri and Nadjib Badache, 2006. New power-aware routing protocol for mobile adhoc network. Int. J. Adhoc Ubiquit. Comput., 1: 126-136. DOI: 10.1504/IJAHUC.2006.009882.
4. Sonja Buchegger and Jean-YvesLe Boudec, 2001. The selfish node: Increasing routing security for mobile adhoc networks. LCA-Report-2001-008. http://infoscience.epfl.ch/record/396.
5. Chen, K. and K. Nahrstedt, 2004. IPass: An incentive compatible auction scheme to enable packet forwarding service in MANET. Proceeding of the 24th International Conference on Distributed Computing System, 2004, Tokyo, pp: 534-542. Doi: 10.1109/ICDCS.2004.1281620.

6. Johnson, D.B. and D.A. Maltz, 1996. Dynamic source routing in adhoc wireless networking. Mobile Comput., 353: 153-181. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.37.1126.
7. Johnson, D.B., D.A. Maltz, Y.C. Hu and J.G. Jetcheva, 2002. The dynamic source routing protocol for mobile adhoc networks (DSR). Internet Draft. http://www.ietf.org/proceedings/02jul/I-D/draft-ietf-manet-dsr-07.txt.
8. Perkins, C.E., E.M. Royer and S. Das, 2003. Adhoc On-demand Distance Vector (AODV) routing. RFC 3561. http://tools.ietf.org/html/rfc3561.
9. Murphy, S., 2002. Routing protocol threat analysis. Internet Draft, draft-murphy-threat-00.txt. http://citeseerx.ist.psu.edu/showciting;jsessionid=C10C469F3E9E96526FB22CAD224CEDCF?cid=731548.
10. Zhang, K., 1998. Efficient protocols for signing routing messages. Proceeding of the Symposium Network and Distributed Systems Security, March, San Diego, CA., pp: 29-35. http://www.isoc.org/isoc/conferences/ndss/98/zhang.pdf.
11. Papadimitratos, P. and Z.J. Haas, 2002. Securing the internet routing infrastructure. IEEE Commun., 10: 60-68. DOI: 10.1109/MCOM.2002.1039858.
12. Perlman, R., 1988. Network layer protocols with byzantine robustness. Ph.D. Dissertation, MIT/LCS/TR-429, MIT, October 1988. http://www.vendian.org/mncharity/dir3/perlman_thesis.
13. Awerbuch, B., D. Holmer, C. Nita-Rotaru and H. Rubens, 2002. An on-demand secure routing protocol resilient to byzantine failures. Proceedings of the 1st ACM Workshop on Wireless Security, September 8-8, ACM Press, Atlanta, Georgia, USA., pp: 21-30. http://portal.acm.org/citation.cfm?id=570684.
14. Lundberg, J., 2000. Routing security in adhoc networks. http://citeseer.ist.psu.edu/old/400961.html.
15. Raymond, J.F., 2001. Traffic analysis: Protocols, attacks, design issues and open problems. Lecture Notes Comput. Sci., 2009/2001: 10-29. DOI: 10.1007/3-540-44702-4.
16. Hu, Y.C., A. Perrig and D.B. Johnson, 2003. Packet leashes: A defense against wormhole attacks in wireless adhoc networks. Proceeding of the 22nd Annual Joint Conference IEEE Computer and Communications Societies, March 30-April 3, IEEE Xplore Press, San Francisco, CA., USA., pp: 1976-1986. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1209219.
17. Hu, Y.C., D.B. Johnson and A. Perrig, 2002. SEAD: Secure efficient distance vector routing for mobile wireless adhoc networks. Proceeding of the 4th IEEE Workshop on Mobile Computing Systems and Applications, June, Callicoon, USA., pp: 3-13. DOI: 10.1109/MCSA.2002.1017480.
18. Lidong Zhou and Zygmunt Haas, 1999. Securing adhoc networks. IEEE Network Mag., 13: 24-30. DOI: 10.1109/65.806983.
19. Stajano, F. and R. Anderson, 1999. The resurrecting duckling: Security issues for adhoc wireless networks. Proceeding of the 7th International Workshop on Security Protocols, April, Cambridge, UK., pp: 172-194. http://www.cl.cam.ac.uk/~fms27/papers/1999-StajanoAnd-duckling.pdf.
20. Richard, D., 1976. The Selfish Gene. 1st Edn., Oxford University Press, UK., ISBN: 019857519X, pp: 224.
21. Sonja Buchegger and Jean-Yves Le Boudec, 2002. Nodes bearing grudges: Towards routing security, fairness and robustness in mobile adhoc networks. Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-Based, January 2002, IEEE Xplore Press, Canary Islands, Spain, pp: 403-410. DOI: 10.1109/EMPDP.2002.994321.
22. Sergio, M., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehaviour in Mobile adhoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, August 06-11, Boston, Massachusetts, United States, pp: 255-265. DOI: 10.1145/345910.345955.
23. Sonja Buchegger and Jean-Yves Le Boudec, 2002. Performance analysis of the CONFIDANT protocol. Proceedings of the 3rd ACM International Symposium on Mobile adhoc Networking and Computing, June 09-11, Lausanne, Switzerland, pp: 226-236. http://doi.acm.org/10.1145/513800.513828.
24. Kevin, F. and K. Varadhan, 2001. The Ns Manual [EB/LO]. http://www.isi.edu/nsnam/ns/doc/index.html.