Asian Journal of Information Technology 15 (8): 1382-1388, 2016
ISSN: 1682-3915
© Medwell Journals, 2016

Avoidance of Blackhole Attack Using Enhanced OLSR with ABHA Algorithm

[1]T. Manikandan, [2]N. Kamaraj, [1]S. Rakeshkumar and [1]J. Gautam
[1]Department of Computer Science and Engineering,
[2]Department of Electrical and Electronics Engineering, Thiagarajar College of Engineering,
Thiruparankundram, 625015 Madurai, Tamil Nadu, India

Abstract: MANET is an infrastructure less modelcomprised of movable nodes. Security issues in MANET are a testing assignment these days. Because of its dynamic nature MANET are more vulnerable to attacks. Especially, a blackhole attack refers to an attack by malicious nodes which forcibly acquires the route from a source to destination by falsely reporting the shortest hop count to reach the destination node. Selective blackhole attack is a special kind of blackhole attack where malicious nodes drop the data packets selectively. If selective blackhole attack exists in a network and if a node tends to acts with malicious behavior IDS technique is implemented to maintain the reliability. This technique increases the efficiency of the network. This study proposed a modified routing protocol called Enhanced OLSR (EOLSR) that uses Avoidance of Blackhole Attack (ABHA) algorithm to detect and isolate the blackhole node thereby maintaining the reliability of the network.

Key words: MANET, Blackhole Attack, IDS, EOLSR, India

INTRODUCTION

Ad hoc network has no definite infrastructure and no fixed topology. All nodes are allowed to move freely in network. There is lack of centralized control to control transmission and movement of nodes and also there are no basic network devices such as routers or access points (Djahel *et al*., 2008). Network management is done in distributed manner since the task is performed by all nodes in the network. Each node in the network functions both as router and host. The network is dynamic as all the nodes are free to move and change its position. This factor brings more challenges in security of Ad hoc network. In a protocol, every node in the network searches proactively for routes to other nodes and in parallel exchange routing messages in order to verify the information provided by the routing table is up to date and correct, such as DSDV (Destination sequence distance vector) by Perkins and Bhagwat, 2000) and OLSR. The power and bandwidth of a node in MANET is limited to a certain limit, thus continuous transmission of routing messages results in congestion of the network. Due to the privation of centralized control in MANET environment, they are vulnerable to attacks from Black hole nodes. Blackhole attack in MANET is a crucial security issue to be fixed. In this issue, a Blackhole node make the most of any one of the routing protocols to publicize itself as it owns the shortest path to the destination. Blackhole nodes which are responsible for the packet drop has to be detected and isolated from the routing process in MANET to improve the efficiency of the network. The proposed work is to avoid Blackhole nodes in the routing process and improve the Quality of service and security of the entire network, notably in terms of packet delivery ratio and throughput.

Literature review: A path based detection technique is proposed where every single node is not responsible to watch every other node in their neighborhood but it only examines the next hop in the current route that is established (Cai *et al*., 2010). Each node in the network has a FwdBktBuffer. Based on the FwdBktBuffer overhear rate is calculated. If the overhear rate is less than the threshold value, then the neighbour node is considered as blackhole node. Blackhole attack is not detected by transferring extra control packets.

Awerbuch *et al*. (2002) study a secure new on-demand routing protocol has been designed. It covers link weights which are taken into account in the event of route discovery. The weights are computed from the packet delivery ratio of individual link. A Link weight is increased when that link does not deliver an amount of packets beyond a fixed threshold then it is considered to be such that the link is opted with lesser probability

Corresponding Author: T. Manikandan, Department of Computer Science and Engineering, Thiagarajar College of Engineering, Thiruparankundram, 625015 Madurai, Tamil Nadu, India

in the upcoming route discovery process. The method finds a blackhole at once the influencing occurs, rather than the blackhole is built.

Hu *et al*. (2005), new protocol Ariadne is proposed. The legitimacy of Route Requests is examined with use of Message Authentication Codes (MAC) in Dynamic Source Routing Protocol (DSR) which is considered to be more secured. Moreover, the researchers introduce three ways for legitimating data in Route Requests and Route Replies. TESLA uses digital signatures to legitimate routing messages. Added, the authors introduces per-hop hashing to examine that null node is present in the node list of the Route Request (Perrig *et al*., 2001).

Perrig *et al*. (2000), proposed two efficient schemes, TESLA and EMSS for secure lossy multicast streams. Five schemes for authentication is presented. The basic scheme has a lot of redundancy. All the supporter packets carry the same hash value of a given packet. Removing this redundancy might give us a lower communication overhead and improved robustness against loss.

A distributed trust model is designed by Rahman and Hailes (1998). This is a decentralized method to trust management that make use of a recommendation protocol to interchange trust-related information. The model assumes that relationships exist between any two entities (nodes) and unidirectional as well. The quality of a recommendation of trust is judged by the nodes, depending on their policies, i.e., trust relationships hold some values. The recommendation protocol operates by demanding trust target for a trust value with contradiction to a specific classification. An evaluation function is employed to acquire an trust value as an whole in the target node. The protocol also permits recommendation refreshing and revocation and is apposite for discovering trust relationships that are less formal and temporary in nature.

Several password-based key exchange technique has been brought by Asokan and Ginzboorg (2000) to organize a secure session among a bunch of nodes in the absence of infrastructure. In this methodology, nodes that are aware of initial password are capable of acquiring the session key. A weak password is distributed to the members of group. Each member then assigns itself to generate a part of the key and signs uses the weak password to sign it.

Decentralized trust management middleware for ad-hoc, peer-to-peer networks, based on reputation of nodes is proposed by Stajano and Anderson (20001). The reputation information of each single peer is saved in its neighbours and piggy-backed on its responds. The originality of the middleware lies in the fact that it relies on the lack of network structure to accomplish reputation information in a secure way.

The resurrecting duckling security protocol is improved to develop a trust in MANET. The protocol is specifically suited for embedded devices systems and systems with no display. The fundamental authentication issue is fixed by a secure transient association concerning two devices inaugurating a relationship of master-slave. It is secure since the master and the slave exchange a common secret. The protocol is unstable since the master can terminate the association at any instant (Deng *et al*., 2002).

Singh and Jena (2011), intrusion detection system to identify the malicious nodes in the networks. Two methods are used to detect the malicious nodes detect during route establishment, detect during data forwarding. A trust-based data management methodology where mobile nodes call up distributed information, storage and sensory resources present in pervasive computing environment. The researchers have taken assumption thatconsiderstrust security, data and privacy and make use of collaborative mechanism that offers trustworthy data management platform in MANET.

To minimize the mischief of malicious nodes that drop data packets (Marti *et al*., 2000) has opted two tools namely watchdog and pathrater. The watchdog detects misbehaving node by examining the neighbors and the pathrater locally values the reliability of nodes individually. On account on these two schemes, authors try to obtain the robustness of networks.

Authors exhibit a detection method to overwhelm the blackhole issues and the collaborative attacks and produce the simulation result by Weerasinghe and Fu (2008). The experiment result shows that this solution performs an almost 50% better than other solutions.

Blackhole attack: MANET is to be deeply concerned with blackhole attack (Table 1). The attackers make use of the blackhole to exhibit their malicious behaviours since the route discovery activity is mandatory and inevitable. A blackhole attack is defined as a malicious node that drops all packets which is supposed to be forwarded to exact destination by falsely claiming that it has the nearest path to the desired node.

Types of blackhole attack

Single blackhole attack: This kind of attack is occurred by the existence of single blackhole node in the routing path. In this type of attack, oneblackhole node drops the data packets instead of

Table 1: Various detection schemes for blackhole attack in OLSR

Schemes	Simulator	Publication years	Results
Detection scheme based on Time (Zhang and Yeo, 2011)	GloMoSim	2011	The PDR of AODV is around 80% when SAODV is around 90-100% but when the malicious node is away from the source node the end-to-end delay increases
Bayesian Detection scheme and Random Two-hop ACK (Murty and Das, 2011)	GloMoSim	2012	The true positive rate can obtain100% when existing 2 witnesses but the scheme put forward is not effective when k equals to 3. It minimizes the positive values
Anti black hole mechanism (2)	NS-2	2012	The packet loss rate is reduced to about 10.05% (threshold set as 5) or 13.04% (threshold set as 10) and detection rate was 100%
Guard node based scheme (Raza and Hussain, 2008)	NS-2	2013	The process of identification of malicious node is dynamic and efficient based on the trust level of a node and also provides better throughput
Path validation and attack finder message (Abdalla *et al.*, 2014)	NS-2	2014	By utilizing the backlist created, the misbehavior nodes are isolated from the network and broadcasting to other nodes in the network
Mechanism based on watchdog (Augustine and James, 2015)	NS-2	2015	It detects misbehavior nodes by monitoring the transmission of next hop neighbor. In watchdog, the copies of the packets that are transported by a node are placed in a buffer and it eavesdrops on the transmission of next link to confirm that it forwards packet reliably
Cooperative bait detection scheme (Ramya and Mylsamy, 2016)	NS-2	2016	By the use of address of a node that is adjacent addresses to bait malicious nodes to transmit a reply message (RREP) and unfamiliar nodes are identified with a reverse tracing technique that ensures security

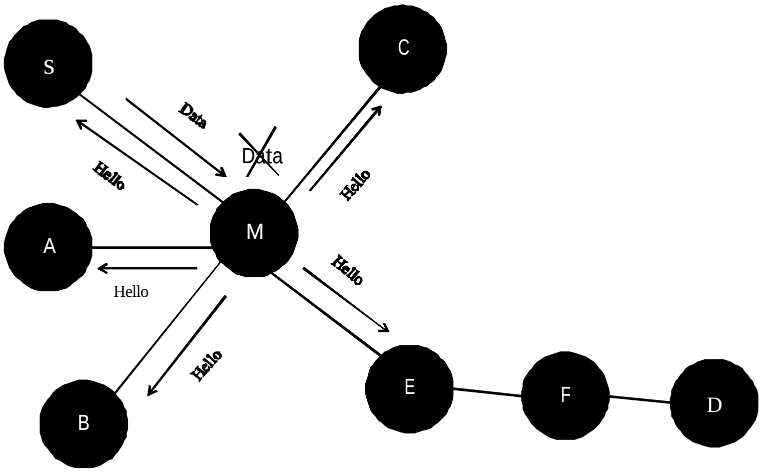

Fig. 1: Blackhole attack in OLSR

forwarding to its neighbors by claiming itself of being closest to the destination node. Single blackhole attack frequent occurrence in MANETsince the blackhole nodes does not depend upon any other nodes to exhibit such attack.

Cooperative blackhole attack: The attack produced by blackhole nodes that function together as a group to advertise a shortest path and then drop the packets. This kind of attack is referred as cooperative black hole attack (Vishnu and Paul, 2010). A severe damage occurs if blackhole nodes function together as a group. The intent of the node may be to intercept the path establishing process or interpret the packet being sent to destination.

Blackhole attack in OLSR: In OLSR the device topology data is operated with HELLO and Topology Control messages. A node acting as blackhole transmits a fake HELLO message. In these messages the blackhole node claims that it has a larger number of links to neighbors than it originally has.

And hence, there is a greater plausibility of choosing this node as a MPR node of the source. The more neighbors the attackernode has, the larger the destruct influence of the attack. Due to the fake messages of the attacker, in its neighborhood falsely representing TC messages with few sections or no TC messages because of a void MPR attacker has the ability to catch routes (Mohanapriya and Krishnamurthi, 2014) (Fig. 1).

MATERIALS AND METHODS

The proposed work is to construct a optimal route by modifying the OLSR protocol as Enhanced OLSR. This technique therefore increases the packet delivery ratio and throughput. Initially, when there is no Blackhole node, the packet delivery ratio approaches nearly 80% in OLSR. The packet delivery ratio in all protocols reduces sharply as the number of Blackhole nodes increases. A MANET environment is created using Network simulator 2 with 100 nodes. In selective, we are dealing with a attack in which aintermediate node selectively drops packets forwarded to some destination. Since, normal network congestion can produce the same effect, it is quite challenging to differentiate a dropped packet due to a Blackhole behaviour. Recent networks randomly drop packets whenever the load exceeds their buffering capacities temporarily. Too many dropped packets imply Blackhole intent. We have designed a model that identifies the Blackhole nodes that drops packet while forwarding and calculated the packet delivery ratio and end to end delay. The calculated throughput value is lower than already existed throughput value without any Blackhole behaviour in the network in all existing routing protocols. It is also ensured, in the modified protocol the route optimality and broadcast performance is not degraded. Since these two vital parameters are not influenced in Enhanced OLSR, it produces a real uptime throughout the entire routing process.

Enhanced OLSR (E-OLSR): The vital reason for the attacks in MANET is that the existing protocol for routing does not admit any confirmation for the Route discovered. Hence, it is significant to procure a confirmation mechanism for the route established in the routing protocol. This mechanism should be efficient enough to isolate the blackhole attack in the network. It is exhausted by introducing a distinct mode of message in existing protocol called Route Confirmation Request (CREQ) and Route Confirmation Reply (CREP). These messages assist to keep away from blackhole attack.

Steps in E-OLSR:

- The Route Request (RREQ) is broadcasted to all its neighbors by the source node to discover a path to the destination
- As destination receives RREQ it generates a RREP message and sends to Source node to acknowledge the path established
- Once the Destination node sends a RREP to source node furthermore it also sends a CREQ (Confirmation Request) to its next bouncing node. If the next bounce node has a path to the source then it generates a CREP and forwards it to the source node

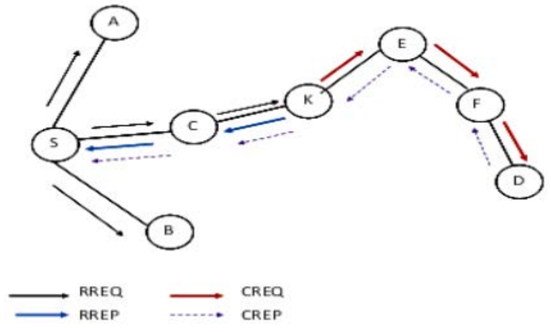

Fig. 2: Enhanced-OLSR

- Finally, CREP reaches the source node following the RREP. After accepting the CREP, the source node can affirm the authority of the way by contrasting the way in RREP and the one in CREP. In the event that both are matched, the source nodes judges that the path is optimal and starts sending the packets. This method keeps the misbehaving nodes away from the routing process as they cannot insist the normal nodes to generate a false CREP packet

This technique is more effective for attack with one blackhole node participate in the routing process and it cannot insist its neighbors to produce a false CREP to confirm the path established. Hence, this method does not involve any misbehaving nodes in the routing process. However this protocol cannot overcome this issue when the blackhole nodes act as a group so called Cooperative blackhole attack. This is because when two consecutive nodes are blackhole they can generate false CREQ and CREP as well. Hence, this method is not incorporated for cooperative blackhole attack (Fig. 2).

Algorithm 1; ABHA Algorithm for avoidance of blackhole attack:

```
Input: S-Source, D-Destination, K-intermediate nodes.
RREQ-Route Request, RREP-Route Reply, RERR-Route Error.
CREQ-Confirmation route request, CREP-Confirmation Route
Reply.
1. S initiates route discovery by RREQ.
2. If K received RREQ then
3.     If K has route in its cache then
4.         K generates RREP to S.
5.         K generates CREQ to D.
6.     Else generates RREP.
7.     End If.
8. Else generates RERR.
9. End if.
10. If D receives CREQ then
11. D generates CREP to K.
12.     If K receives CREP then
13.     K forwarded CREP to S.
14.     Else K generates RERR to D.
15.     End if.
16. Else Rebroadcast RREQ.
```

```
End if
If CREP ==RREP then
    Select the path as optimal
Else discard the path
```

In this scenario, the source initially broadcasts a RREQ. The intermediate node K at once receives the RREQ, it checks for a route to the destination in its cache memory. If route exist the intermediate node K sends a RREP to the source and replies a Confirmation Request (CREQ) as well and forwards it to the destination. Destination, at receiving a CREQ checks for the route to source and immediately sends a CREP to source via the same route through K. Hence, Source receives both RREP and CREP. It checks the sequence number in CREP and RREP. It confirms the route as optimal if the sequence numbers of both are same.

Hence, the optimal route will not allow any Blackhole nodes to claim a false path. If there is a Blackhole node present in the path claiming for a shortest path it could possibly generate only RREP and a node with blackhole behavior in the path will never receive a CREP from the destination. Added, the source node will not receive any CREP from the false path. As a result only optimal routes are established.

The process resumes after route discovery in EOLSR. Cost metrics are computed for every node and the path with the nodes having a cost value greater than a threshold value is selected as the optimal path to send packets (Fig. 3). This results in better efficiency for packet delivery. Data packet loss rate, L is calculated as follows:

$$L = \frac{\sum_{i=1}^{n}\left(N(i)^{s} - N(i)^{p}\right)}{\sum_{i=1}^{n} N(i)^{s}} \times 100\%$$

Where:

$N(i)^s$ = Data packets sent by the sender

$N(i)^p$ = Data packets received by the receiver

n = Number of applications

T denotes Throughput Ratio, is computed as follows:

$$T = \frac{\sum_{i=1}^{n} T(i)^{r}}{\sum_{i=1}^{n} T(i)^{s}} \times 100\%$$

Where:

$T(i)^r$ = Average receiving throughput for the ith application

$T(i)^s$ = Average sending throughput for the ith application

n = Number of applications

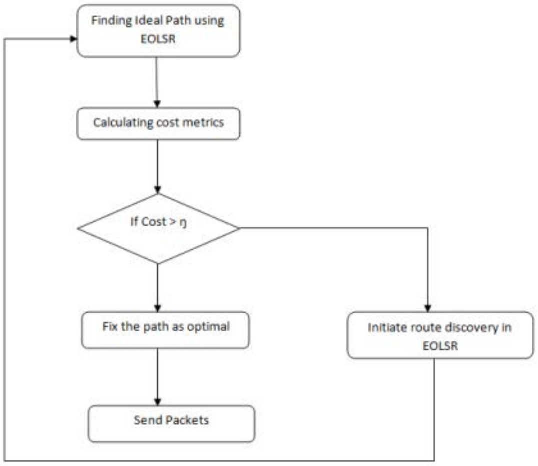

Fig. 3: Flowchart for fixing optimal path

End to End delay is calculated using the formula:

$$d_{end\text{-}end} = N\left[(d_{trans} + d_{prop} + d_{proc})\right]$$

Where:

$d_{end\text{-}end}$ = End-to-end delay

d_{trans} = Transmission delay

d_{prop} = Propagation delay

d_{proc} = Processing delay

N = Number of links (Number of routers + 1)

Each router will have its own d_{trans}, d_{prop}, d_{proc} hence, this formula gives a rough estimate.

RESULTS AND DISCUSSION

The simulation results in NS2 (version-2.35) proclaims that our protocol avoids blackhole nodes in the routing process and consequently improves the overall performance of normal OLSR in presence of blackhole nodes. In an area of 500×500 m, 50 normal nodes executing the OLSR routing protocol were randomly distributed and 10 blackhole nodes performing selective blackhole attack. UDP-CBR is used as the traffic type and the maximum time for simulation is 600 sec. Random way Point is used as the mobility model. The simulation parameters are defined in Table 2.

The results of existing routing protocols and enhanced OLSR has been compared. The results inferred clearly implies that the enhanced OLSR provides a better packet delivery ratio and throughput as all the misbehaving nodes have been isolated from the routing process which are responsible for blackhole attacks that reduces the reliability of the network as shown in Fig. 4-6.

Table 2: Simulation parameters

Parameters	Values
Coverage area	500×500 m
Simulation time	600 sec
No. of nodes	50
No. of blackhole nodes	10
Traffic type	UDP-CBR
Packet size	512 bytes
Maximum speed	20 m sec^{-1}
Routing protocol	OLSR
Mobility model	Random way point

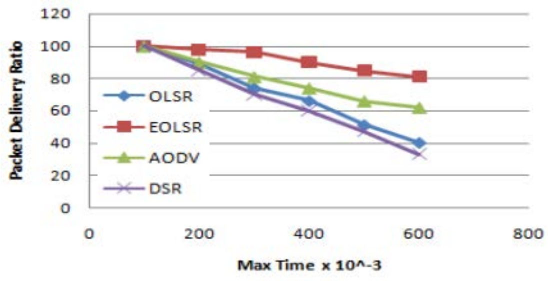

Fig. 4: PDR Comparison between Enhanced OLSR and other Protocols

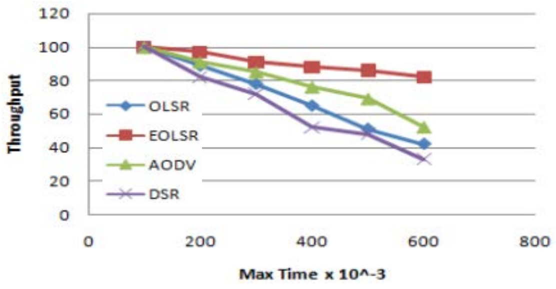

Fig. 5: Throughput Comparison between EOLSR and other Protocols

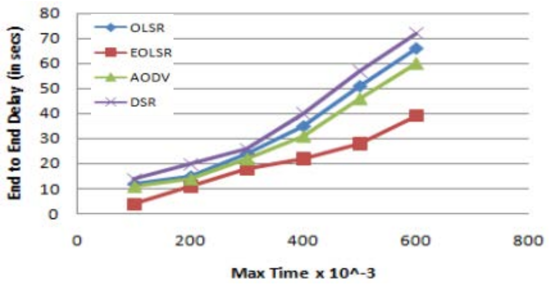

Fig. 6: End to End Delay Comparison between EOLSR and other Protocols

CONCLUSION

An Ad-hoc network is a distributed type of wireless network. It has a set of limited range of wireless nodes that function in a cooperative manner to increase the overall efficiency of the network. The selective blackhole attack which is considered to be one of the major issues in the network has been identified and the misbehaving nodes that are responsible for such attacks. These misbehaving nodes are avoided from the routing process by Enhanced OLSR using ABHA algorithm. This results in increased packet delivery ratio since no malicious nodes are made to participate in the routing process. The lifetime of the network is also made efficient by choosing the reliable nodes for routing the packets. Our future work is to enhance this technique for Cooperative blackhole attack and other security threats in MANET since, this technique is not applicable when blackhole nodes work as a group.

REFERENCES

Abdalla, A.M., I.A. Saroit, A. Kotb and A.H. Afsari, 2011. Misbehavior nodes detection and isolation for MANETs OLSR protocol. Procedia Comput. Sci., 3: 115-121.

Asokan, N. and P. Ginzboorg, 2000. Key agreement in ad hoc networks. Comput. Commun., 23: 1627-1637.

Augustine, A. and M. James, 2015. Detection and isolation of black hole node in MANET. Int. J. Curr. Eng. Technol., 5: 2347-5161.

Awerbuch, B., D. Holmer, C.N. 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 28, 2002, ACM, New York, USA., ISBN:1-58113-585-8, pp: 21-30.

Cai, J., P. Yi, J. Chen, Z. Wang and N. Liu, 2010. An adaptive approach to detecting black and gray hole attacks in ad hoc network. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, April 20-23, 2010, IEEE, New York, USA., ISBN: 978-0-7695-4018-4, pp: 775-780.

Deng, H., W. Li and D.P. Agrawal, 2002. Routing security in wireless ad hoc networks. IEEE Commun. Mag., 40: 70-75.

Djahel, S., F. Nait-Abdesselam and A. Khokhar, 2008. An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol. Proceedings of the IEEE International Conference on Communications, May 19-23, 2008, Beijing, pp: 2780-2785.

Hu, Y.C., A. Perrig and D.B. Johnson, 2005. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 11: 21-38.

Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking, August 6-11, 2000, Boston, MA., USA., pp: 255-265.

Mohanapriya, M. and I. Krishnamurthi, 2014. Modified DSR protocol for detection and removal of selective black hole attack in MANET. Comput. Electr. Eng., 40: 530-538.

Murty, M.S. and M.V. Das, 2011. Performance evaluation of MANET routing protocols using reference point group mobility and random waypoint models. Int. J. Ad Hoc Sens. Ubiquitous Comput., 2: 33-43.

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic Destination-Sequenced Distance-Vector routing (DSDV) for mobile computers. Proceedings of the Conference on Communications Architectures, Protocols and Applications, August 31-September 2, 1994, England, UK., pp: 234-244.

Perrig, A., R. Canetti, D. Song and J.D. Tygar, 2001. Efficient and secure source authentication for multicast. Proceedings of the Internet Society Network and Distributed System Security Symposium, February 23-26, 2001, San Diego, CA., USA., pp: 35-46.

Perrig, A., R. Canetti, J.D. Tygar and D. Song, 2000. Efficient authentication and signing of multicast streams over lossy channels. Proceedings of the IEEE Symposium on Security and Privacy, May 14-17, 2000, Berkeley, CA., USA., pp: 56-73.

Rahman, A.A. and S. Hailes, 1998. A distributed trust model. Proceedings of the 1997 Workshop on New Security Paradigms, September 23-26, 1997, ACM, New York, USA., ISBN:0-89791-986-6, pp: 48-60.

Ramya, V. and S. Mylsamy, 2016. Removal of malicious nodes launching blackhole attack in MANETs. Wireless Commun., 8: 6-10.

Raza, I. and S.A. Hussain, 2008. Identification of malicious nodes in an AODV pure ad hoc network through guard nodes. Comput. Commun., 31: 1796-1802.

Singh, Y. and S.K. Jena, 2011. Intrusion Detection System for Detecting Malicious Nodes in Mobile Ad Hoc Networks. In: Advances in Parallel Distributed Computing. Nagamalai, D. and E. Renault (Eds.). Springer Berlin Heidelberg, Heidelberg, Germany, ISBN: 978-3-642-24037-9, pp: 410-419.

Stajano, F. and R. Anderson, 2000. The resurrecting duckling: Security issues for Ad Hoc wireless networks. Proceedings of the 7th International Workshop on Security Protocols, April 19-21, 1999, Cambridge, UK., pp:172-194.

Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comp. Commun., 34: 107-117.

Vishnu, K. and A.J. Paul, 2010. Detection and removal of cooperative black/gray hole attack in mobile ad hoc networks. Int. J. Comput. Appl., 1: 38-42.

Weerasinghe, H. and H. Fu, 2008. Preventing cooperative black hole attacks in mobile ad hoc networks: Simulation implementation and evaluation. Int. J. Software Eng. Appl., 2: 39-54.

Zhang, D. and C.K. Yeo, 2011. Distributed court system for intrusion detection in mobile ad hoc networks. Comput. Secur., 30: 555-570.