RESEARCH ARTICLE OPEN ACCESS

Detection and Prevention of Black-Hole Attack in MANETS

Rashmi[1], Ameeta Seehra[2]
Department of Electronics and Communication Engineering,
Guru Nanak Dev Engineering College, Ludhiana,
Punjab-India

ABSTRACT

Secure routing in the field of MANET is one of the most emerging areas of research. Designing a trustworthy security protocol for ad hoc routing is a challenging task due to the unique network characteristics such as, lack of central authority, rapid node mobility, frequent topology changes, insecure operational environment, and limited availability of resources. Due to minimal configuration and quick deployment, MANETs are suitable for emergency situations like Natural disasters or Military applications. Thus data transfer between two nodes must require security. A black-hole attack in the Mobile Ad-hoc NETwork (MANET) is an attack occurs due to malicious nodes, which attracts the data packets by falsely advertising a fresh route to the destination. A clustering approach in AODV routing protocol for the detection and prevention of black-hole attack in MANETs has been proposed. Every member of the cluster will ping once to the cluster head, to detect the peculiar difference between the number of data packets received and forwarded by the node. If anomalousness is perceived, all the nodes will obscure the malicious nodes from the network. The analysis of the system performance has been done in terms of Packet Delivery Ratio (PDelR), Detection Rate (DR) and Throughput and simulation results are obtained using ns2 simulator.

Keywords:- MANET, Routing Protocols, Security, Black-hole attack, AODV, Clustering, Cluster-head.

I. INTRODUCTION

A MANET consists of several mobile nodes that are connected by wireless links and each mobile node acts not only as a host but also as a router to establish a route. When a source node intends to transfer the data packets to the destination node, then the packets are transferred through intermediate nodes, thus quick deployment of the nodes to establish a route is the important issue in MANET.

Routing protocols in MANET are mainly categorized into Proactive and Reactive routing protocols and other type is Hybrid (Reactive/Proactive) routing protocols. Proactive Routing Protocols are table driven protocols maintain the lists of all possible destination nodes in a table and periodically exchanges routing messages, in order to keep the information in the routing table up-to-date and correct. When transmission is required from one node to another, the route is already known and can be used. Optimized Link State Routing Protocol (OLSR) Protocol, Distributed Sequenced Distance Vector (DSDV) Protocols are examples of proactive routing protocols [1]. On the other hand, Reactive Protocols like AODV and DSR protocols are on demand routing protocols i.e. invoke the route determination procedure only on demand [2]. When route is needed, some sort of Route Discovery procedure is employed, because these protocols assume cooperation between two nodes for packet forwarding, a malicious node may lead to routing attack in the network that disrupts the normal routing operations of MANET. Thus decentralized and dynamic nature of MANET may lead to various attacks in the network that can partition or destroy the network.

Generally there are two types of attacks in the MANETs, one is Passive attack and other is Active attack. In Passive attack, the intruder silently listen the communication channel without modifying or destroying the data packets [3]. But in Active attack, intruder can modify or destroy the original data. Due to minimal configuration and quick deployment, MANETs are suitable for emergency situations like Natural disasters rescue operation, hospitals, battlefield, conferences and Military applications. Thus data transfer between two nodes must require security. But the active attacks like Black hole attack, Rushing attack, Wormhole attack have great impact on the performance of the network [4].

Black hole attack is a special type of attack that generally occurs in the Reactive protocols. A black-hole node is the malicious node that attracts the packets by falsely claiming that it has shortest and fresh route to reach the destination, then drops the packets. These Black hole nodes may perform various harmful actions on the network that are [5]:

- Behaves as a Source node by falsifying the Route Request packet.
- Behaves as a Destination node by falsifying the Route Reply packet.
- Decrease the number of hop count, when forwarding Route Request packet.

In this approach, if the ratio of number of packets received to the number of packets sent are less than threshold then the destination node start the detection process. The difference between number of packets received by a node and number of packets forwarded by it is significant then node is declared as the malicious node and is isolated from the network.

II. RELATED WORK

Security has long been an active research topic in MANETs. In [6-13] various security techniques and routing protocols have been proposed for the prevention of single and cooperative black hole attacks in the network.

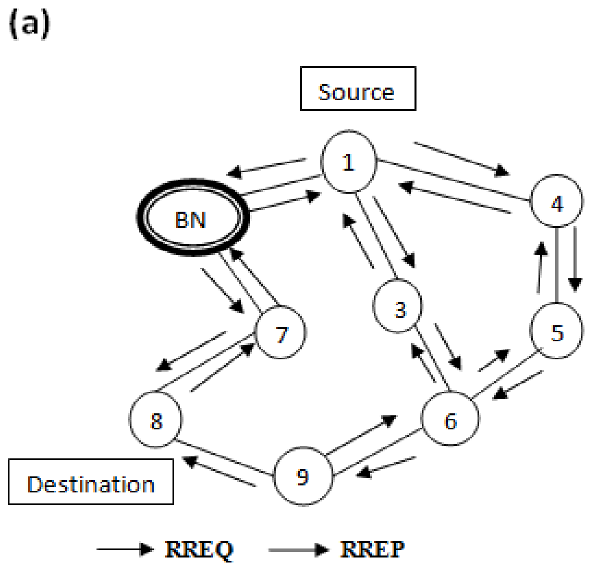
Mohanapriya and Krishnamurthi in [14] presented a Modified Dynamic Source Routing Protocol (MDSR) to detect and prevent selective black hole attack. The source node selects the first shortest path to the destination, to intimate the no. of data packets it sends to the destination. The source node then selects the second shortest path for actual transmission of data. Then packet count and transmitted data both are compared. If difference is significant i.e. abnormality is detected the nearby IDS node broadcast a message informing all nodes to obscure all nodes from network. In [15], a Routing Security Scheme based on Reputation Evaluation (RSSRE) is proposed. The reputation evaluation mechanism is built on the basis of correlation among nodes that need to be evaluated. It has the mechanism to promote the cooperation of cluster members for forwarding data packets to execute improved routing when there are malicious nodes in hierarchical Ad Hoc networks. In [16], authors proposed checkpoint-based Multi-hop Acknowledgement Scheme, for detecting selective forwarding attacks which can select the intermediate nodes randomly as checkpoint nodes which will generate acknowledgements for each packet received. Intermediate node has to send the acknowledgment for every packet that it is receiving; the algorithm has to suffer from overhead. Moreover, the channel is assumed perfect. Gao and Chen [17] proposed three security algorithms such as full proof algorithm, check-up algorithm and diagnosis algorithm. The full proof algorithm was for creating proof and the check-up algorithm was for checking up source route nodes; and the diagnosis algorithm was for locating the malicious nodes in the network. In approach [18], Jaisankar et al. presented that each node should have Black hole Identification Table (BIT) that contains source, target, current node ID, Packet received count (PRC), Packet forwarded count (PFC). If difference between PRC and PFC is significant, then the node is identified as malicious and is isolated from the network. In [19], Chavda and Nimavat proposed an algorithm to remove black hole attack at the cost of overhead. The source node continues to accept RREP packets from the various nodes and compares RREP (RREP R1, RREP R2) which actually compares the destination hop count of two route replies and selects the route reply with high destination hop count if the difference between two hop counts is not significantly high. In [20] Wang et al. proposed an approach basis of cooperation between nodes to improve the scalability and efficiency of MANETs by arranging the nodes on the basis of trust mechanism. In our method, the trust value is calculated on the.

III. PROPOSED METHODOLOGY

Our model is based on following assumptions: (A) All nodes are identical in their physical characteristics. (B) Cluster head is selected as a node located at the centre of cluster. (C) All the black-hole nodes will drop exactly the half of total number of data packets. (D) The source nodes and the destination node are taken as trusted nodes by default.

A. *Protocol Description*

In AODV protocol, the source node broadcasts RREQ packet to find the path to reach the destination. The destination node



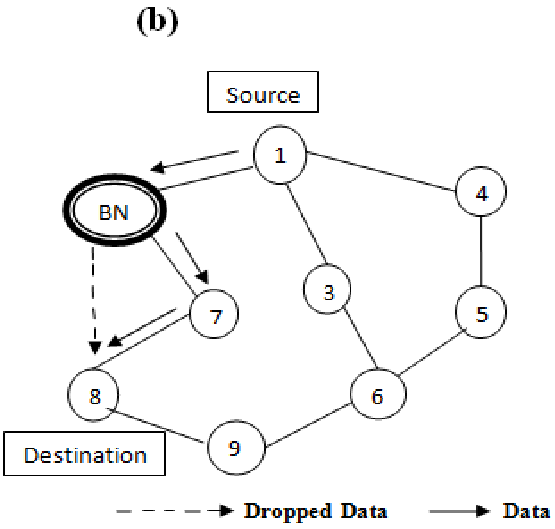


Fig. 1: Route Discovery Process in AODV

having the path will send the RREP to the source node in response. Fig. 1(a) shows the black-hole nodes will also participate in Route Discovery process and will claim for the shortest route to the destination. If the route is chosen through the black-hole node, then it can drop the data packets as shown in Fig. 1(b). Thus to prevent the black-hole attack, a novel approach is drawn. In this approach the deployed nodes are divided into clusters such that each cluster will have a cluster head and the remaining nodes are called the members of that cluster. The cluster head can be chosen randomly from each cluster. Some check-points are deployed in the network so as to check whether the no. of data packets received by the nodes and no. of packets sent by the nodes are equal. Transmissions can take place within the cluster or from one cluster where the source is located to another where destination is.

B. *Methodology*

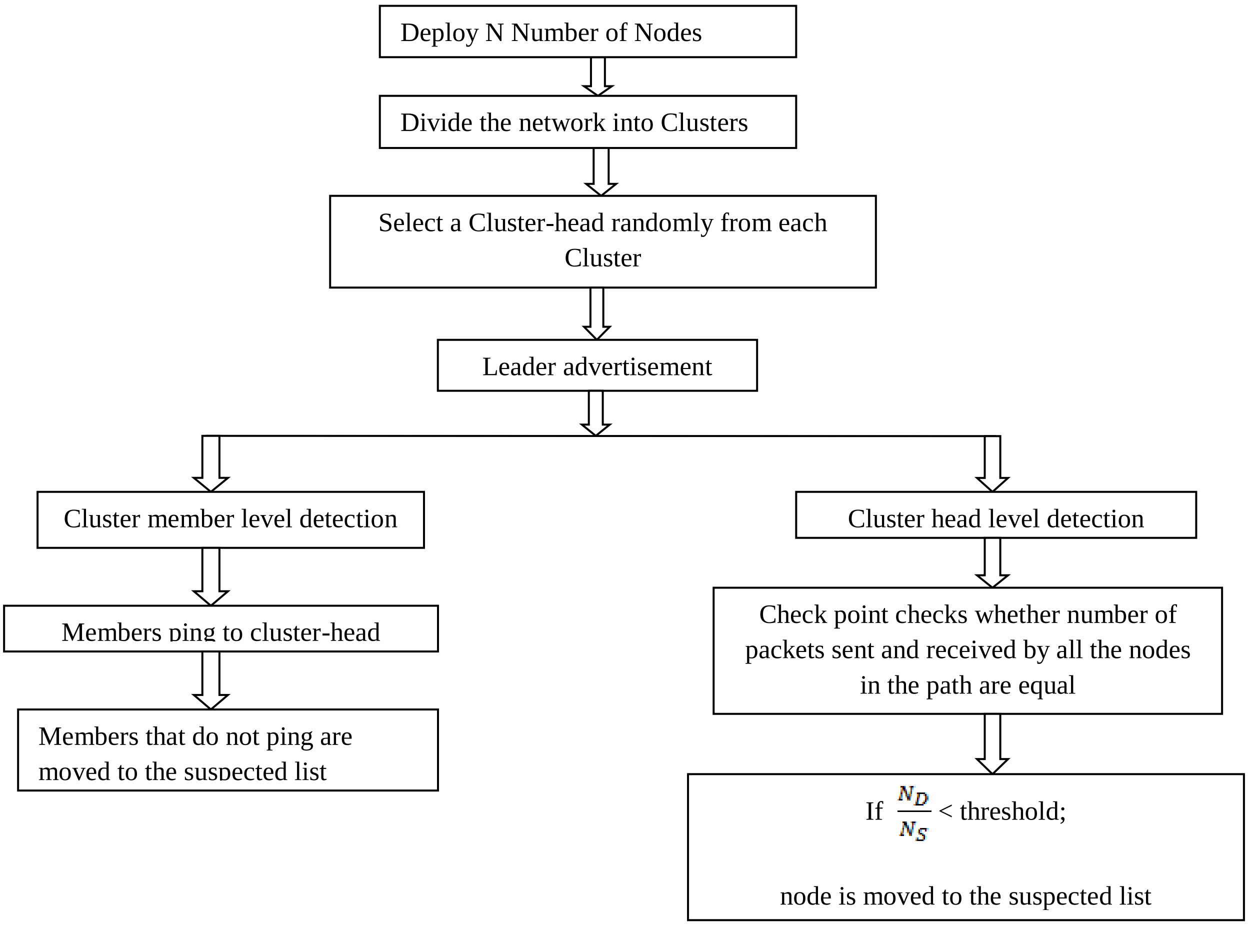

Deploy N Number of Nodes
Divide the network into Clusters
Select a Cluster-head randomly from each Cluster
Leader advertisement
Cluster member level detection
Members ping to cluster-head
Members that do not ping are moved to the suspected list
Cluster head level detection
Check point checks whether number of packets sent and received by all the nodes in the path are equal
If $\frac{N_D}{N_S}$ < threshold;
node is moved to the suspected list

Fig. 2: Steps for Implementation

Let the no. of data packets forwarded by the source (node 4) to the destination (node 19) be N_s and (4, 5, 15, 19) be the route for data forwarding as shown in Fig. 3. Check-point (CP) keeps count of the number of packets each node receives and forwards to the downstream. When the destination node receives the data packets from the source, check-point keeps the count of the number of packets the destination received. Let the destination (node 19) receives N_d number of packets. Then the probability of packets received at destination is as follows: $P_d = \frac{N_d}{N_s}$. If P_d < T, then the check-point starts the process of detecting whether the malicious node is present in the route. If not, then it receives positive acknowledgment from the destination. Here packet loss threshold takes the value from 0 to 0.2. In this approach if the packet loss exceeds 20% of the total packets sent by the source node the check-point starts black-hole detection process. Source node will transmit next packet of data only after receiving the positive acknowledgement from destination.

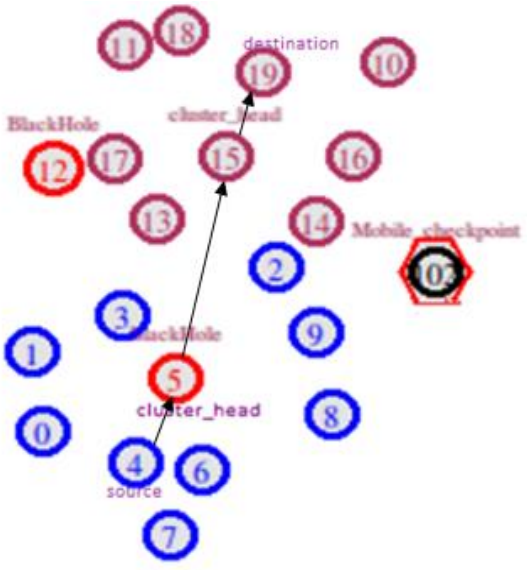


Fig. 3: Clustering in MANET

IV. EXPERIMENTAL SET UP AND ANALYSIS

This paper is applied to ns-2 to validate the detection and isolation efficiency of the proposed method against black-hole nodes. In an area of 1500×1500 m^2, 100 normal nodes executing AODV routing protocol were randomly distributed, and a couple of malicious nodes performing black-hole attack, and 4 Check-point nodes are randomly located. The major parameters of experiment are listed in Table1 and the data in this section is obtained by taking average value, which results from 10 experiments.

Also our approach is also compared with an existing Modified DSR approach proposed in [14]. In order to evaluate the performance of clustering approach following metrics have been measured:

Table1. Simulation parameters

Properties	Value
Simulator	ns2
Coverage area	1500 × 1500
Number of nodes	104
Simulation time	600 s
Mobility	Random way point model
Mobility speed	20 m/s
Number of black-hole nodes	5
Mobile check-point nodes	4
Traffic type	UDP-CBR

- **Packet delivery ratio:** Ratio of total number of packets received at the destination to the total number of packets sent.
- **Throughput:** The rate of successful delivery of packets over a communication channel. It is usually measured in bits per second (bps).
- **Detection rate:** Total number of suspected nodes over misuse and anomaly detecting nodes.

(a)Packet delivery ratio: PDelR in both the cases differs only with time. Fig 4 shows that in clustering approach at the period of 9 seconds, the PDelR becomes 1. But in Modified DSR approach it becomes 1 at the period of 23 seconds. In clustering approach, mobile checkpoints will detect the number of data packets forwarded to and forwarded by the nodes in the route and monitor the data packet loss.

(b)Detection Rate: Detection Rate is the total number of nodes detected (whether these are malicious or not) from the overall network, therefore the detection rate for the MANET should be as high as possible. In the proposed approach, detection rate is about three times the Modified DSR approach [14]. Simulation results are shown in Fig 5.

(c)Throughput: is number of data packets delivered per second. It is also expressed in number of bits per second. Fig. 6 shows the simulation results of throughput. In our proposed approach throughput obtained is near about three times that in Modified DSR approach. At the period of 27seconds; throughput for Modified DSR approach is 1.5367 Kb/sec and for clustering approach it is 4.8192.

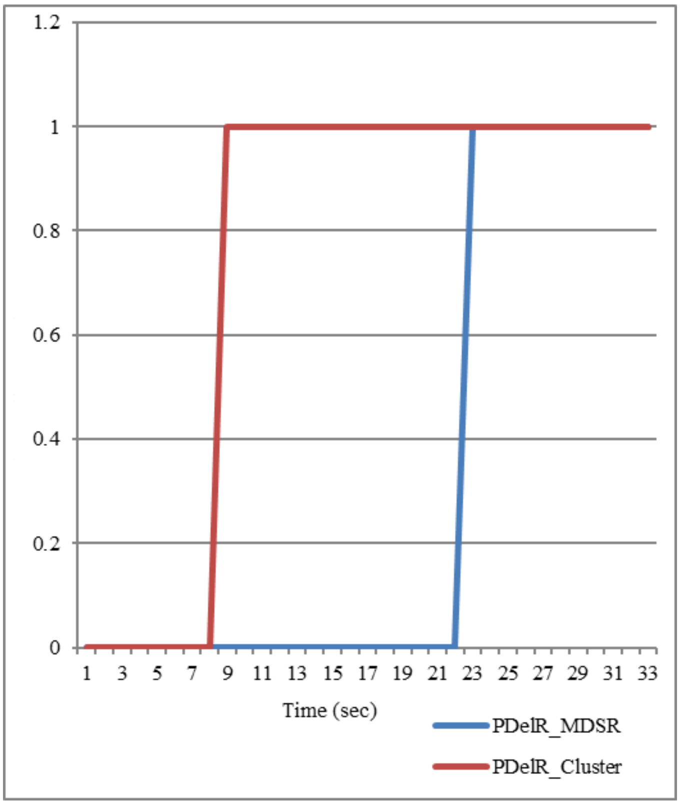


Fig. 4: Packet Delivery Ratio

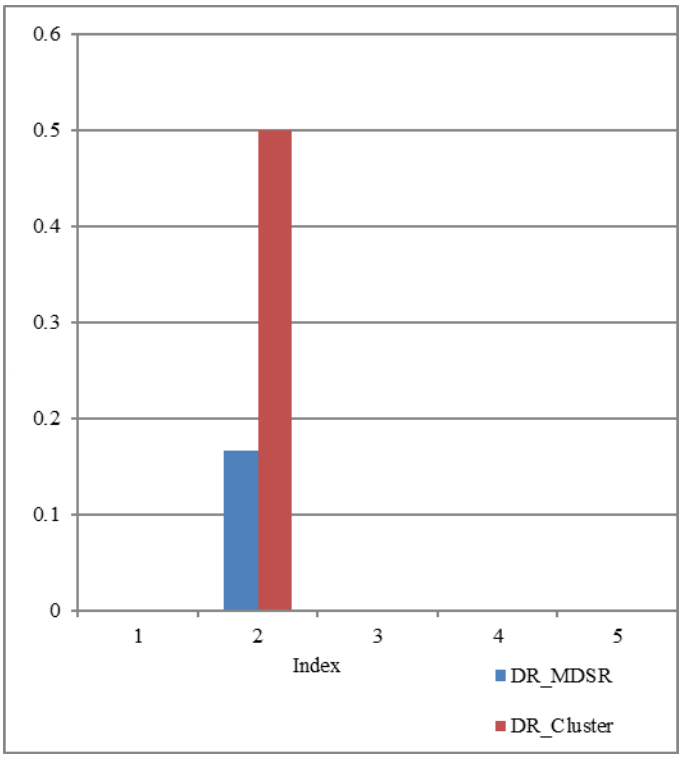


Fig. 5: Detection Rate

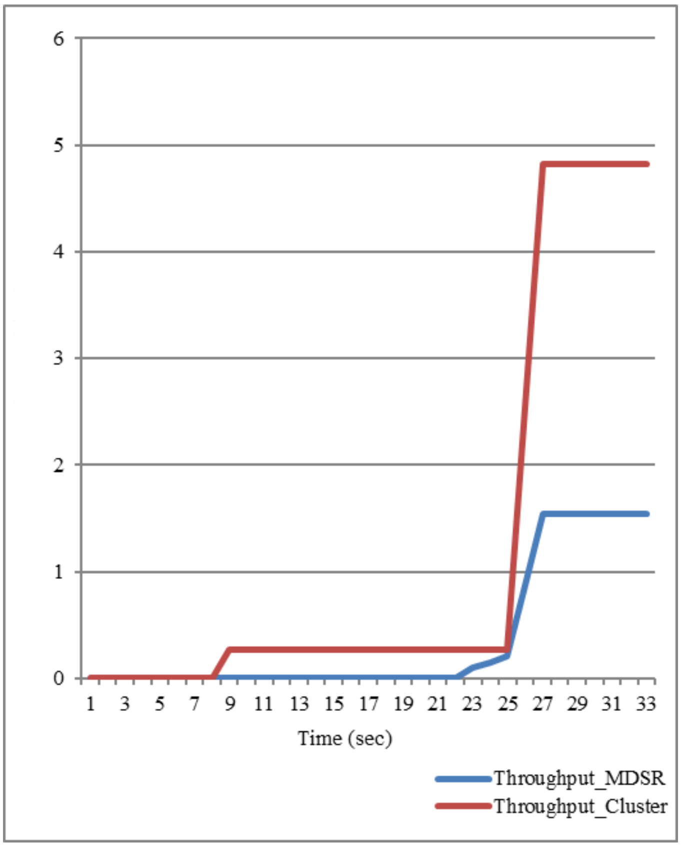


Fig. 6: Throughput

V. CONCLUSION

The proposed lightweight methodology is based on simple acknowledgement scheme to detect the black-hole nodes in MANET. This approach can be incorporated with any existing on demand routing protocols. It has been concluded that the proposed approach provide better results as compared to Modified DSR approach. Packet Delivery Ratio (PDelR) in both the approaches is 1 i.e. the system will lead to full delivery of packets. Detection Rate (DR) in the proposed approach is about three times the Detection Rate in Modified DSR approach. In case of MANETs the Detection Rate should be as high as possible so as to detect maximum number of nodes in the network whether these are malicious or not. Higher the value of DR, more secure is the network. In the clustering approach, Throughput is about three times the modified DSR approach. Thus the data transmission rate is higher in the proposed approach.

REFERENCES

[1] A. Mehran, and W. Tadeuz, "*A review of routing protocols for mobile ad hoc networks*", International

Journal on Ad hoc Networks, Vol. 2, No.1, pp.1–22, 2004.

[2] D. B. Johnson, D. A. Maltz, and C. Y. Hu, "*The dynamic source routing protocol for mobile ad-hoc network (DSR)"*, IETF Internet Draft, 2004.

[3] R. K. Bar, J. K. Mandal, and M. Singh, "*QoS of MANet Through Trust Based AODV Routing Protocol by Exclusion of Black Hole Attack",* International Conference on Computational Intelligence: Modeling Techniques and Applications, India, pp. 530-537, 2013.

[4] H. Deng, P. Agarwal, "*Routing security in wireless ad hoc networks*", IEEE Communication Magzine, Vol. 40, No. 10, pp. 70–75, 2002.

[5] S. Lee, B. Han, and M. Shin, *"Robust routing in wireless ad hoc networks*", In: ICPP Workshops, pp. 73-79, 2005.

[6] S. Dokurer, Y. Erten, and C. Erkin, *"Performance analysis of ad-hoc networks under black hole attacks*" In: Proc. of the IEEE South-east Conference, pp. 148–53, 2007.

[7] L. Tamilselvan, and V. Sankaranarayanan, "*Prevention of black hole attack in MANET",* In: Proc. of the international conference on wireless broadband and ultra wideband, communication, 2007.

[8] L. Tamilselvan, and V. Sankaranarayanan, "*Prevention of co-operative black hole attack in MANET*" International journal on Networks, Vol. 3, No.5, pp. 13–20, 2008.

[9] K. Satoshi, N. Hidehisa, K. Nei, J. Abbas, and N. Yoshiaki, "*Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method*". International Journal on Network Security, Vol. 5, No. 3, pp. 338–346, 2007.

[10] J. Luo, M. Fan, and Y. Danxia, "*Black hole attack prevention based on authentication mechanism*" In: Proc. of the IEEE international conference on communication systems, Singapur, pp. 173–177, 2008.

[11] D. Soufine, N. Farid and K. Ashfaq, "*An acknowledgment-based scheme to defend against cooperative black hole attacks in optimized link state routing protocol*" In: Proc. of the IEEE international conference on communications, pp. 2780–2785, 2008.

[12] S. Lu, and L. Li, "*SAODV: a MANET routing protocol that can withstand black hole attack*", In: International conference on computational intelligence and security, IEEE Computer Society, pp. 421–425, 2009.

[13] C. Chao, and T. Yuh, "*A context adaptive intrusion detection system for MANET*', international journal on Computer Communications, Vol. 34, No. 4, pp. 310–318, 2011.

[14] M. Mohanapriya, and L. Krishnamurthi, "*Modified DSR protocol for detection and removal of selective black hole attack in MANET",* International Journal on computers and electrical engineering, Vol. 40, No. 2, pp. 530-538, 2014, Elsevier.

[15] Y. Yao, L. Guo, X. Wang, and C. Liu, "*Routing security scheme based on reputation evaluation in hierarchical ad hoc networks",* IEEE Journal on Computer Network, Vol. 5, No. 4, pp. 1460-1469, 2010.

[16] B. Xiao, B. Yu, and C. Gao, "*CHEMAS: identify suspect nodes in selective forwarding attacks*" International Journal in Parallel Distributed Computer networks, Vol. 67, No. 11, pp. 1218–1230, 2007, Elsevier.

[17] X. Gao and W. Chen, *"A novel gray-hole attack detection scheme for mobile ad-hoc networks".* In: International Conference on network and parallel computing workshops, , pp. 209–14, 2007.

[18] N. Jaisankar, N. Saravanan, and K. D. Swamy, "*A Novel Security Approach for Detecting Black Hole Attack in MANET",* Proc. Business Administration and Information Processing Heidelberg, pp. 217-223, 2010.

[19] K. S. Chavda, and A. V. Nimavat, "*Removal of Black Hole Attack in AODV Routing Protocol of Manet*", Proc. IEEE conference on computer networks, Tiruchengode, India, pp. 207-212, 2013.

[20] W. Wang, G. Zeng, J. Yao, W. Hanli, and T. Daizhong, "*Towards Reliable Self-Clustering Mobile Ad hoc Networks"* International Journal on Computer and Electronics Engineering, Vol. 38, No. 1, pp. 551-562, 2012.

[21] N. Kalia, and K. Munjal, "*Multiple Black Hole Node Attack Detection Scheme in MANET by Modifying AODV Protocol"* International Journal of Engineering and Advanced Technology (IJEAT), Vol. 2, No. 3, pp. 529-533, 2013.

[22] S. Abid, and S. Khan, "*Improving Performance of Routing Protocols Using MRP Framework"* International Journal of Ambient Systems and Applications (IJASA), Vol. 2, No. 1, pp. 1-8, 2014.