ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)
On 21st& 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

# Removal of Selective Black Hole Attack in MANET by AODV Protocol

T.Manikandan, S.Shitharth, C.Senthilkumar, C.Sebastinalbina, N.Kamaraj
Dept of Computer Science, Thiagarajar College of Engineering, Madurai, India
Dept of Computer Science , Thiagarajar College of Engineering, Madurai, India
Dept of Electronics and Electronics, Thiagarajar College of Engineering, Madurai, India
Dept of Electronics and Electronics Thiagarajar College of Engineering, Madurai, India

**Abstract** - Mobile AdHoc networks are self-configuring and self-organizing multi-hop wireless networks. A mobile Adhoc Network (MANET) is a collection of autonomous mobile users communicating over bandwidth constrained wireless links. Due to the mobile nodes, the topology of the network keeps changing unpredictably and rapidly over time. A selective black hole attack on MANET refers to an attack by a malicious node, which forcibly acquires the route from source to a destination by the falsification of sequence number and hop count of the routing message. As selective black hole is a node that can optimally and alternately perform a selective black hole attack or perform as a normal node. In this paper, we propose a method of activating the promiscuous mode and hence further data packet loss is prevented. Finally, we analyze the performance of the nodes after the inclusion of promiscuous mode.

**Keywords –** Adhoc, Source routing, Malicious node.

## I. INTRODUCTION

### *A. Wireless Network Security*

Wireless mobile ad hoc network is a self-configuring network composed of several movable nodes. Ad hoc is a Latin word means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. These mobile nodes communicate with each other without any infrastructure; furthermore all of the transmission links are established through wireless medium. Different protocols are then evaluated based on measures such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc. MANET is very popular because the application areas have the topological network that is changing frequently. MANET is more vulnerable than wired networks because of its mobile nodes. Already existing wired security solutions are not applied to MANET hence new proposals for the MANET security is always needed. MANET also has its own vulnerabilities such as Lack of centralized management, resource availability, scalability, cooperativeness, dynamic topology, and limited power supply and bandwidth constraint. In MANTE there is number of broad casting approaches such as Unicasting, multicasting, broadcasting and geocasting. In security issues they are generalized into two types of attacks. They are of External attacks and Internal attacks.

## II. RELATED WORKS

Selective black hole attacks always have an impact on routing algorithms and it uses sequence number to select the shortest route [12] in routing protocols such as AODV or DSR. Generally, a selective black hole node is reduced to an appropriate extent in AODV protocol as referred by Can Erkin [12]. The Justification is given by the concept of rejecting the first two RREP packets send to the source node because mostly the selective black hole node sends its RREP in one of the first two RREP to the source node. Hence its efficient in detectingBlack Hole Attack in AODV protocol.

Dr.Sankarnarayanan proposed another efficient approach based on AODV protocol [6] as; Usually a source do not send its RREP, only after receiving the first RREP. It waits until all the neighboring nodes to send their RREP. The source sends its reply to the node which has the distance of two from the source node. He also proposed another method to detect Cooperative Black hole attack based on the update of the fidelity level.

Initially, all nodes are provided with a fidelity level, and sends RREQ to all nodes.

Then its select a node with higher fidelity level, that exceeds the threshold value to pass the packets. An ACK is send from the destination node and the source node add one to the fidelity level and it subtracts one if no ACK is received. That indicates the possibility of the presence of the black hole node and sense there may be a loss of data packets before it reaches the destination node.

Nikayama et al. [4] proposed a dynamic learning method to detect a selective black hole node. It is required to observe if the characteristic change of a node exceeds the threshold within a period of time. If yes, this node is judged as a selective black hole node, other-wise, the data of the latest observation is added into dataset for dynamic updating purposes. The characteristics observed in this method include the number of sent RREQs, the number of received RREPs and the mean destination sequence number of the observed RREQs and RREPs. However, it does not involve a detection mode, such as revising the AODV protocol or deploying IDS nodes, thus, it does not isolate selective black hole nodes. Luo et al. [5] added an authentication mechanism into the AODV routing protocol, by combining hash functions, message authentication codes (MAC), and a pseudo random function (PRF) to prevent lack hole attacks.

Djahel et al. [5] proposed a routing algorithm based on OLSR (Optimized Link State Routing) to prevent the attack of cooperative selective black holes, by adding two control packets, namely 3 hop_ACK and HELLO_rep. Mahmood and Khan [10] also surveyed recent research papers involving selective black hole attacks on MANETs, and described seven previous methods, and analyzed their advantages and disadvantages.

In this paper, IDS nodes are deployed in MANETs to identify and isolate selective black hole nodes. An IDS node observes every node’s number of broadcasted RREQs, and the number of forwarding RREQs in AODV, in order to judge if any malicious nodes are within its transmission range. Once a selective black hole node is identified, the IDS node will send a block message through the MANET to isolate the malicious node [3].

## III. Reactive (On-Demand) Routing Protocol

The reactive routing is equipped with another appellation named on-demand routing protocol. Unlike the proactive routing, the reactive routing is simply started when nodes desire to transmit data packets. The strength is that the wasted bandwidth induced from the cyclically broadcast can be reduced. Nevertheless, this might also be the fatal wound when there are any malicious nodes in the network environment. The weakness is that passive routing method leads to some packet loss. Here we briefly describe two prevalent on-demand routing protocols which are ad hoc on-demand distance vector (AODV) and dynamic source routing (DSR) protocol.

AODV is constructed based on DSDV routing. In AODV, each node only records the next hop information in its routing table but maintains it for sustaining a routing path from source to destination node. If the destination node can’t be reached from the source node, the route discovery process will be executed immediately. In the route discovery phase, the source node broadcasts the route request (RREQ) packet first. Then all intermediate nodes receive the RREQ packets, but parts of them send the route reply (RREP) packet to the source node if the destination node information is occurred in their routing table. On the other hand, the route maintenance process is started when the network topology has changed or the connection has failed.

The source node is informed by a route error (RRER) packet first. Then it utilizes the present routing information to decide a new routing path or restart the route discovery process for updating the information in routing table. The design idea of DSR is based on source routing. The source routing means that each data packet contains the routing path from source to destination in their headers. Unlike the AODV which only records the next hop information in the routing table, the mobile nodes in DSR maintain their route cache from source to destination node.

In terms of the above discussion, the routing path can be determined by source node because the routing information is recorded in the route cache at each node. However, the performance of DSR decreases with the mobility of network increases, a lower packet delivery ratio within the higher network mobility.

## IV. Proposed Methodology

Our IDS model is based on the following assumptions. (a) All the nodes are identical in their physical characteristics. If node A is within the transmission range of node B, then node B is also within the transmission range of A. (b) Also our solution assumes that all the nodes are authenticated and can participate in communication, i.e., all nodes are authorized nodes.(c) The source node, destination node and IDS nodes are taken as trusted nodes by default. (d) All the IDS nodes are set in promiscuous mode only when needed, and an IDS node will always be neighbor to some other IDS node. (e) Since there are multiple routes from a source to destination, the source node has to cache the other routes to mitigate the overhead incurred during new route discovery process.

- Protocol Description
- Selective black hole Discovery Process
- Performance analysis

### A. *Protocol Description*

The Ad-hoc on demand routing is like all reactive protocols, is that topology information is only transmitted by nodes on-demand. When a node wishes to transmit traffic to a host to which it has no route, it will generate a route request (RREQ) message that will be flooded in a limited way to other nodes. This causes control traffic overhead to be dynamic and it will result in an initial delay when initiating such communication. A route is considered found when the RREQ message reaches either the destination itself, or an intermediate node with a valid route entry for the destination. For as long as a route exists between two endpoints, AODV remains passive. When the route becomes invalid or lost, AODV will again issue a request.

**RREQ -** A route request message is transmitted by a node requiring a route to a node.

**RREP** - A route reply message is unicasted back to the originator of a RREQ if the receiver is either the node using the requested address, or it has a valid route to the requested address. The reason one can unicast the message back, is that every route forwarding a RREQ caches a route back to the originator.

**RERR** - Nodes monitor the link status of next hops in active routes. When a link breakage in an active route is detected, a RERR message is used to notify other nodes of the loss of the link. In order to enable this reporting mechanism, each node keeps a “precursor list”, containing the IP address for each its neighbors that are likely to use it as a next hop towards each destination.

### *B. Selective black hole Discovery Process*

A selective black hole problem means that one malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node, but drops the routing packets but does not forward packets to its neighbors. A single selective black hole attack is easily happened in the mobile ad hoc networks. An example is shown as Figure, node 1 stands for the source node and node 4 represents the destination node. Node 3 is a misbehavior node who replies the RREQ packet sent from source node, and makes a false response that it has the quickest route to the destination node. Therefore node 1 erroneously judges the route discovery process with completion, and starts to send data packets to node 3. As what mentioned above, a malicious node probably drops or consumes the packets. This suspicious node can be regarded as a selective black hole problem in MANETs. As a result, node 3 is able to misroute the packets easily, and the network operation is suffered from this problem.

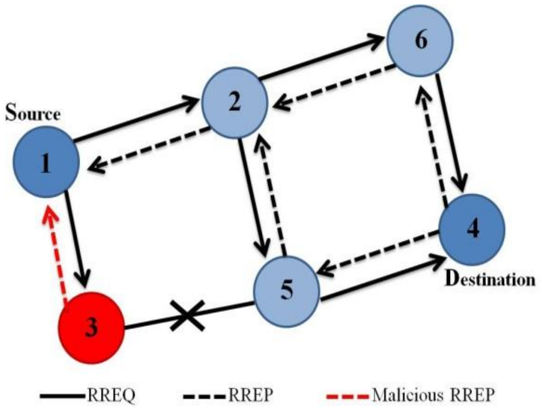

Fig. 1 Selective black hole attack

### *C. Promiscuous mode*

Promiscuous mode is a mode for a wireless network interface controller (WNIC) that causes the controller to pass all traffic it receives to the central processing unit (CPU) rather than passing only the frames that the controller is intended to receive. This mode is normally used for packet sniffing that takes place on a router or on a computer connected to a hub (instead of a switch) or one being part of a WLAN.

### *D. Performance Analysis*

To analyze the performance of proposed Routing protocol is by considering packet delivery ratio, collision rate and delay. The result shows that the proposed protocol improves the above mentioned constraints. $N_F$ =number of packets forwarded to destination node by the source node. $P_R$ =probability of packets received. $N_R$ = number of of packets received

$$P_R = \frac{N_R}{N_F}$$

## V. Flow Chart

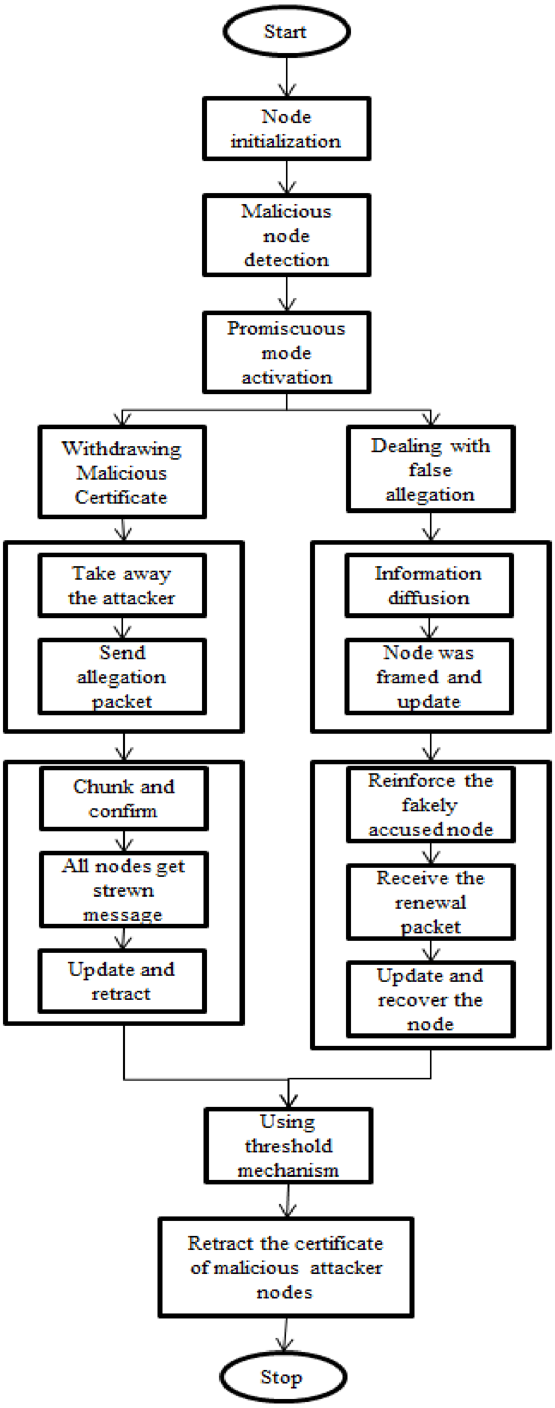
Start
Node initialization
Malicious node detection
Promiscuous mode activation
Withdrawing Malicious Certificate
Dealing with false allegation
Take away the attacker
Send allegation packet
Information diffusion
Node was framed and update
Chunk and confirm
All nodes get strewn message
Update and retract
Reinforce the fakely accused node
Receive the renewal packet
Update and recover the node
Using threshold mechanism
Retract the certificate of malicious attacker nodes
Stop

Fig.2 Overall process flow of the proposed method

## VI. Experimental Setup And Result Analysis

Network Simulation 2 is applied in this paper for the detection and isolation of selective black hole nodes. In the area 1000 1000 m, 75 normal nodes executing the AODV routing protocol were randomly distributed, and few malicious nodes, to perform selective black hole attack. Randomly chosen pairs for data communication send 5 kb UDP-CBR per second. Speed of the nodes moving in a range between 0 and 20m/s. Pause times of the nodes are of 0 s, 5 s, 10 s and 15 s were considered. Pause time is defined as the time taken by node to move from one place to another.

TABLE 1. SIMULATION PARAMETERS

| Property | Value |
|---|---|
| Region covered | 1000 1000m |
| Number of nodes | 75 |
| Simulation time | 600 S |
| Transmission range | 250 m |
| Mobility | 5 Kb UDP packets, Data Payload 512 bytes |
| Mobility speed | 20m/s |
| No. of selective black hole nodes | 5 |
| Connections | 20 pairs(40 nodes) |
| Traffic Type | UDP-CBR (type) |
| Pause time | 0,5,10 and 15 secs |
| IDS nodes | 9 nodes(fixed) |

- Packet Drop Ratio is defined as the total number of data packets dropped by the malicious nodes or due to any congestion among the nodes.
- Overhead (bit/s): Amount of traffic prevails over the network by our approach.
- End to end delay (s): It's the time elapsed between time when the source node is triggered off to the time the destination node receives.
- Formula used to detect the probability of the malicious node is
- Pm = Na / (Nc + Na)

1. Number of detected cooperation (Nc)
2. Number of detected attacks (Na)
3. Probabilities that the node is a malicious node (Pm).

### A. Packet drop ratio

The packet loss rate of AODV under attack without the application of promiscuous mode is about 40% while the packet loss rate of AODV with promiscuous mode was approximately 30% reduced by 10%. The packet loss rate of AODV was approximately 25% in the approach [23] which was which was decreased by 5% when compared to our scheme.

PM -Promiscious Mode
NPM- Non Promisious Mode

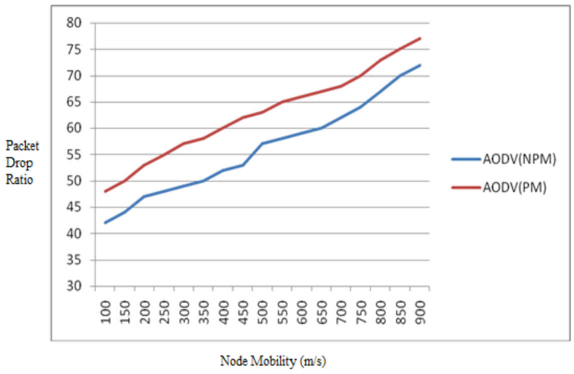

Fig. 3 Comparison of packet delivery ratio in PM and NPM

### B. Overhead ratio

This is the ratio of transmissions like RREQ, RREP and RERR. Some routing packets like RREQ and QUERY packets are broadcast to all neighbors and packets like RREP and RRER travel along only in a single path.

The Control Packet overhead ratio in our approach was approximately 40% and it is decreased by 5% when compared to the overhead ratio of AODV which was approximately 45%. But still our approach leads in a better way in control overhead ratio when compared with the approach [23] that is having 60% overhead ratio.

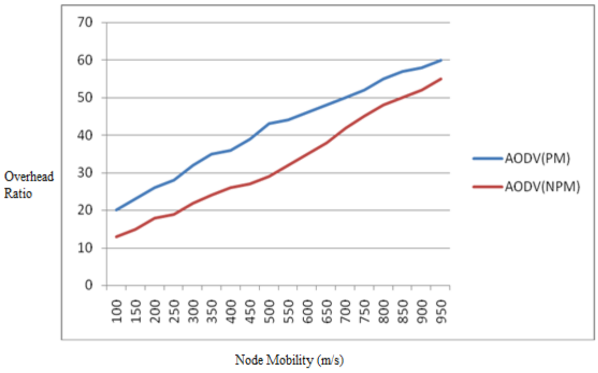

Fig. 4 Comparison of overhead ratio in PM and NPM

### C. End to End delay

Compared to the approach in [23] our end-to-end delay is quite better. Usually the end-to-end delay is increased with higher the possibility of malicious nodes. We avoid the overhead in the system by avoiding the frequent checking of the malicious nodes that causes selective black hole attack. As the overhead is decrease, involuntarily the end-to-end delay is decreased. As for our approach is concerned, we implement promiscuous mode as soon the malicious node is detected. So it will avoid further data loss and our IDS nodes isolate the malicious nodes so that we no need to check frequently for the malicious nodes .Obviously, our overhead is decreased as such the end-to-end delay.

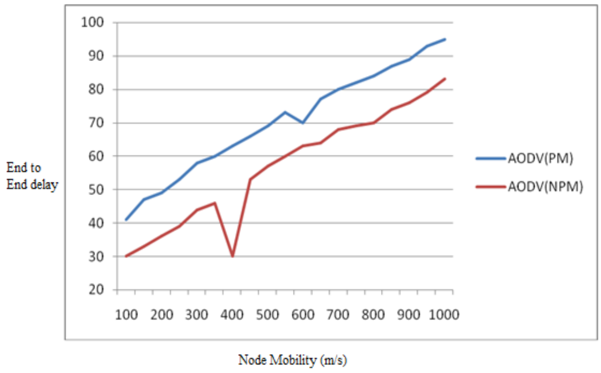

Fig. 5 Comparison of end to end delay in PM and NPM

### D. *Throughput*

The amount of data transferred from one place to another or processed in a specified amount of time. Usually, the throughput value is indirectly proportional to the packet loss. AODV with the activation of Promiscuous mode always show good throughput value since it loss data packets in less rate. In our comparative graph throughput increases as the no.of.node increases but after a break point it drops from 20% to 50% gradually.

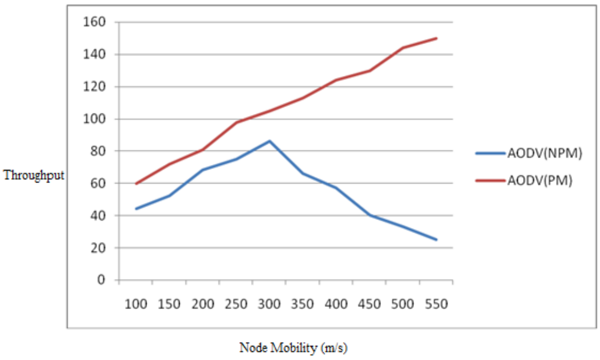

Fig. 6 Comparison of throughput in PM and NPM

## VII. Conclusion

Mobile Ad-Hoc Networks has the ability to deploy a network where a traditional network infrastructure environment cannot possibly be deployed. In our approach, we have analyzed the behavior and challenges of security threats in mobile Ad-Hoc networks and implemented the promiscuous mode in a better way. Although many solutions have been proposed but still these solutions are not perfect in terms of effectiveness and efficiency. If any solution works well in the presence of single malicious node, it cannot be applicable in case of multiple malicious nodes. After referring many approaches, applying promiscuous mode after the detection of selective black hole attack would surely decrease the rate of loss in data packet. More ever, the promiscuous mode is applied only for nodes that were attacked rather for applying for all the nodes. Hence loss of energy is surely avoided. In future, we enhance our work to stop even the initial data packet loss by applying the promiscuous mode to Proactive routing protocols.

## References

[1] ShilaDevuManikantan, Cheng Yu, Anjali Tricha Channel-aware detection of selective black hole attacks in wireless mesh networks. In: IEEE global telecommunications conference, December 2009. P. 1-6.

[2] Nasser and Y. Chen, “Enhanced Intrusion monitoring nodes with selection of Malicious nodes in mobile ad hoc networks,” in Proc. IEEE Int.Conf. on Communication (ICC’07), June 2007, pp. 1154-1159.

[3] SemihDokurer, Y.M. Erten, Can ErkinAcar, “Performance Analysis of Ad-hoc Networks under Selective black hole Attacks”, in: Proc. of the IEEE southeastCon, pp.148-153, 2007.

[4] SoufineDjahel, FaridNait-Abdesselam, AshfaqKhokhar, “An Acknowledgement-Based Scheme to Defend Against Cooperative Black Hole Attacks in Optimized Link State Routing Protocol”, in:Proc, of the IEEE International Conference on Communications (ICC), pp. 2780-2785, 2008.

[5] SoufineDjahel, FaridNait-Abdesselam, AshfaqKhokhar, “An Acknowldgement-Based scheme to Defend Against Cooperative Black hole Attacks in Optimized Link State Routing Protocol”, in: Proc. of the IEEE International Conference on Communications (ICC). Pp 2780-2785, 2008.

[6] A. Hasswa, M.Zulker, and H.Hassanein, “Routeguard: an intrusion detection and response system for mobile ad hoc networks,” Wireless and Mobile Computing, Networking and Communication, vol.3, August 2005, P336-343.

[7] M.K.Rafsanjani, A.Movaghar, “Identifying monitoring nodes with selection of Authorized nodes in mobile ad hoc networks,” World Applied Sciences Journal, Vol.4, no3, pp. 444- 449, 2008.

[8] R.A.RajaMahmood, A.I. Khan, “A survey on Detecting Selective black hole Attack in AODV-based Mobile Ad Hoc Networks”, in: Proc. of the International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET), pp. 1-6, 2007.

[9] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipor, Yoshiaki Nemoto, Detecting blackhole attack on AODV-based Mobile Ad Hoc Networks by Dynamic learning method, International Journal of Network Security 5 (3), pp. 338-346, 2007.

[10] N. Komnios, D. Vergados, and C. Douligeris, “Detecting unauthorized and compromised nodes in mobile ad hoc networks,” Elsevier Ad hoc network, vol. 5, No. 3, pp. 289-298, 2007.

[11] LathaTamilselvan, Dr.V.Sankarnarayanan, “Prebention of co-operative selective Black hole attack in MANET, Journal of Networks 3(5), pp.13-20, 2008.

[12] SemihDokurer, Y.M. ErtenAcar, “ Performance Analysis of Ad-hoc Networks Under Selective Black hole Attacks”, in: Proc: of the IEEE SoutheastCon, pp.148-153, 2007.

[13] Latha Tamil selvan, Dr.V.Sankarnarayanan, “Prevention of Black-hole Attack in MANET”, in: Proc. of the International Conference on Wireless Broadband and Ultra Wideband Communication, 2007.

[14] S. Xu, “Integerated Prevention and Detection of Byzantine Attacks in Moble Ad Hoc Networks”, PhD thesis, PhD in Computer Science, The University of Texas at San Antonio, 2009.

[15] Cheng Bo-zchao, Tseng Ryh-Yuh A context adaptive Intrusion detection System for MANET, Computer Communication 2011:34:310-8.

[16] Yao Yu, Guo Lei, Wang Xingwei, Liu Cuixiang Routing security scheme based on reputation evaluation in hierarchical ad hoc networks. ComputNetw 2010:54:14609.

[17] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. Elsevier’s Ad hoc Networks J September 2003:1(2-3):293-315 [Special Issue on Sensor Network Applications and Protocols].

[18] Xiao B, Yu B, Gao C. CHEMAS: Identify suspect nodes in selective forwarding attacks. J Parallel Distributed Comput2007:67(11):1218-30.

[19] XiaopengGao, Wei Chen. A novel selective black hole attack detection scheme for Mobile ad-hoc networks. In: IFIP international conference on network and parallel computing workshops, 2007. p. 209-14.

[20] Wang Shun-Sheng, Yan Kuo-Qin, Wang Shu-Ching. An optimal solution for Byzantine agreement under a hierarchical cluster-oriented mobile ad hoc network ComputElectrEngJanusry 2010:36(1):100-13.

[21] Sukla Banerjee. Detection/removal of cooperative and selective black hole attack In mobile ad-hoc networks. World CongrEngComputSci 2008:337-42.

[22] T.Anantvalee and J. Wu. ”A Survey on Intrusion Detection in Mobile Ad Hoc Networks”, Book Series Wireless Network Security, Springer, pp. 170 – 196, ISBN:978-0-387-28040-0 (2007).

[23] Ming-Yang Su. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. ComputCommun 2010.