Mobile Ad-hoc Network Security Challenges under AODV Routing Protocol

E.O.Ochola, M.M.Eloff and J.A.van der Poll

School of Computing, University of South Africa, Pretoria, South Africa
e-mail: {ocholeo|eloffmm|vdpolja}@unisa.ac.za

Abstract

Mobile Ad-hoc Network (MANET) is a group of heterogeneous mobile nodes, forming a temporary network which is infrastructure less, multi-hop and dynamic in nature. MANET requires that nodes cooperate to be able to communicate. The nodes, which act as hosts as well as routers, communicate with each other through multiple hops due to limited transmission ranges. Security challenges in MANETs such as channel vulnerability, absence of infrastructure, node vulnerability, dynamic topology, cooperative routing protocols and limited resources, pose new kinds of security threats to such networks. Unlike other types of networks, MANETs are deployed without a centralised control unit. Therefore, the direct application of the conventional routing algorithms may not be feasible. Mutual cooperation amongst the participating entities forms the basis for determining the routes to the destination. This aspect makes MANETs vulnerable to various communication security related attacks. *Black Hole* attacks are launched by participating malicious nodes that agree to forward data packets to a destination but eavesdrop or drop the packets intentionally, which not only compromise the network, but also degrade network performance. Routing protocols, which act as the binding force in these networks, are a common target of malicious nodes. This paper analyses challenges with existing solutions to *Black Hole* attack in MANET and concludes that, better secure approaches can be achieved through utilisation of optimised threshold values during anomaly detections in routing control packets' characteristic changes.

Keywords

Mobile Ad-hoc Network (MANET), AODV Routing Protocol, Black Hole Attack

1. Introduction

Wireless networks are formed by routers and hosts, and use radio frequencies to transmit and receive data instead of using physical cables. Mobile Ad-hoc Network (MANET) (Poongothai and Jayarajan, 2008) is a group of wireless mobile hosts without the required involvement of any offered infrastructure or centralised access point such as a base station. Basic networking devices, such as routers or access points are lacking in a MANET. Thus, data transfer among the network nodes is realised by means of multiple hops, and every node acts as a router to establish and maintain routes rather than just serving as a single mobile terminal host. This presents many challenges, including secure routing protocols, to the research community.

Nodes within each other's radio range communicate directly via wireless links, while those that are far apart use intermediate nodes as relays. The functioning of mobile ad-hoc networks is dependent on the trust and cooperation between nodes. Thus, nodes help each other in conveying information about the topology of the network (Tamilselvan and Sankaranarayanan, 2007). A source node intending to transfer data to a destination node located beyond its transmission range do so through intermediate nodes. It is therefore an important issue in MANET to perform a quick route establishment from, a necessity capitalised on by *Black Hole* attack.

Tamilselvan and Sankaranarayanan (2007:118) agree that security is a major concern in all forms of communication networks. However, mobile ad-hoc networks are faced with greater challenges due to their inherent nature, which can be attributed to characteristics such as: dynamic topology, lack of centralised control, limited battery power and limited bandwidth (Kurosawa *et al.* 2007). Hence, there exist routing attacks that can be launched on mobile ad-hoc networks.

AODV is one of the most popular routing protocols, which has been extensively discussed in research papers (Cerri and Ghioni, 2008:121). Therefore, this paper focuses on *Black Hole* attack detection and prevention scheme on AODV-based MANETs. *Black Hole* attack is one of the Denial of Service (DoS) attacks, in which the communication between nodes is interrupted by ensuring that sent data packets do not reach their intended destination, as they are dropped whenever they have to be relayed by the *Black Hole* nodes.The existing *Black Hole* attack solution approaches do not explicitly address the issues of false positive and negative identifications (mistaken identifications) of *Black Hole* nodes, with tradeoffs on network performance metrics to achieve comparable results. Hence a need to explicitly address the issues through optimised threshold values during anomaly detections.

2. MANET Security Issues

Security is much more difficult to maintain in MANETs due to their vulnerability, than wired networks. The use of wireless links renders a mobile ad-hoc network susceptible to link attacks (Anjum *et al.* 2006). The MANET vulnerabilities include, but are not limited to the following (Kurosawa *et al.* 2007):

a) Dynamically changing network topology: mobile nodes join and leave the network arbitrarily, resulting in dynamic change of network topology. This allows for a malicious node to join the network without prior detection.
b) Lack of centralised monitoring: there is absence of any centralised infrastructure that prohibits any monitoring mechanism in the network. This makes the classical security solutions based on certification authorities and on-line servers inapplicable. Even the trust relationships among individual nodes also change, especially when some nodes are found to be compromised. Hence, security mechanisms need to be dynamic and not static.
c) Cooperative algorithms: MANET routing algorithms require mutual trust between neighbouring nodes, which violates the principles of network security.
d) The absence of a certification authority, as a result of none existing infrastructure.

e) The limited physical protection of each of the nodes: network nodes usually do not reside in physically protected places, such as locked rooms. Hence, they can more easily be captured to fall under the control of an attacker.
f) The intermittent nature of connectivity, as a result of the instability in bandwidth requirements.
g) The vulnerability of the links (open media): messages can be eavesdropped and fake messages can be injected into the network without the difficulty of having physical access to the network components. Eavesdropping might give an attacker access to secret information thus violating confidentiality.

The contemporary routing protocols for mobile ad hoc networks cope well with the dynamically changing topology but are not designed to accommodate defence against malicious attackers. No single standard protocols capture common security threats and provide guidelines to secure routing (Singh *et al.* 2010). Nodes exchange network topology information in order to establish routes amongst them, which is a potential target for malicious attackers. It is difficult to detect compromised nodes through routing information due to the dynamic topology of mobile ad hoc networks (Liu *et al.* 2007). The routing protocol should be able to bypass the compromised nodes, as long as there are sufficient numbers of valid nodes. However, this needs the existence of multiple, possibly disjoint routes between nodes.

3. AODV Routing

AODV is perhaps the most well-known reactive routing protocol for a MANET (Cerri and Ghioni, 2008). It provides a rapid, dynamic network connection, with low processing loads and low memory consumption. Nodes in the network exchange routing information only when they intend to communicate, and keep this information updated only as long as the communication lasts.

A node intending to send a packet to another node starts a route discovery process in order to establish a route to the destination node, by sending a route request message (RREQ) to its neighbours. Neighbouring nodes increment the hop count on receiving the RREQ, and similarly forward (broadcast) the message to their neighbours using a flooding approach. This continues until the destination node is found. The RREQ message forwarding has the side effect of making other nodes learn the *reverse route* to the source node. The RREQ message will eventually reach the destination node, which will react with a route reply message (RREP). The RREP is sent as a unicast to the source node along the *reverse route* established during the RREQ broadcast. Similarly, the RREP message allows intermediate nodes to learn a *forward route* to the destination node. Therefore, at the end of the route discovery process, packets can be delivered from the source node to the destination node and vice versa. A route error message (RERR) allows nodes to notify errors due to link breakage, such as when a previous neighbour moves to a new position and is no longer reachable. Each mobile node would periodically send Hello messages (HELLO), thus, each node knows which nodes are its neighbouring nodes within one hop. Routing messages are either path discovery (RREQ and RREP) or path maintenance (RERR and HELLO) messages. All routing information expires after a timeout in case of an inactive route, and is removed from the routing table.

AODV is a collaborative protocol, allowing nodes to share information about each other. RREQ messages do not necessarily need to reach the destination node during the route discovery process. That is, an intermediate node having a route to the destination simply generates the RREP without any further forwarding of the RREQ. This enables a quicker response to route availability, eliminating unnecessary further flooding of RREQs.

Sequence numbers are used by AODV to identify fresher routing information. Every node maintains its own sequence number, incrementing it before sending either a new RREQ or RREP message. The sequence numbers are included in routing messages and recorded in routing tables. AODV favours newer information, thus nodes update their routing table whenever they receive a message with a higher sequence number (a larger number refers to newer information) or a smaller hop count (smaller hop count refers to shorter path) than what exists in the routing table for a given destination. However, a sequence number is given a higher priority than a hop count. That is, a route with newer information is favoured even if it is longer.

Being a reactive routing protocol, AODV does not give nodes a complete view of network topology. That is, each node only knows its neighbours, and for the non-neighbours, it only knows the next hop to reach them and the distance in hops. However, the security of AODV is compromised by the *Black Hole* nodes, as it accepts the received RREP having fresher route.

The standard AODV routing protocol cannot fight the threat of *Black Hole* attacks, because during the phase of route discovery, malicious nodes may counterfeit a sequence number and hop count in the routing message; thereby, acquiring the route, eavesdropping or/and dropping all the data packets received for relay to intended next hop intermediate nodes.

4. Black Hole Attack

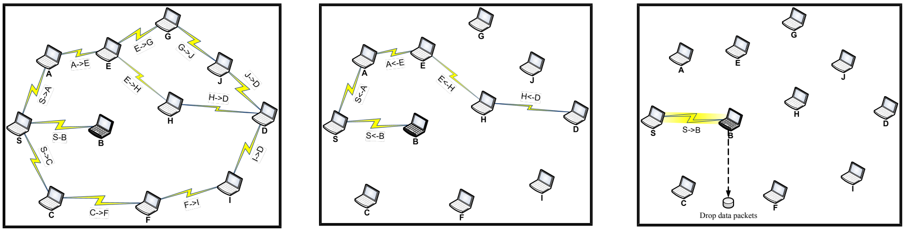
Due to the nature of instances that prompt the use of MANETs such as communication during natural disasters, on the battlefield, and business conferences, there is a need for guaranteed safety of data transfer between two communicating nodes. A *Black Hole* attack (Su, 2011) forges the sequence number and hop count of a routing message to forcibly acquire the route, and then eavesdrop or drop all data packets that are supposed to be relayed. A malicious (*Black Hole*) node impersonates a destination node by sending a spoofed RREP to a source node that initiated a route discovery.

A *Black Hole* node has two properties (Tamilselvan and Sankaranarayanan, 2007): (1) the node exploits the ad hoc routing protocol and advertises itself as having a valid route to a destination, even though the route is spurious, with the intention of intercepting packets, and (2) the node consumes the intercepted packets.

The behaviour of a *Black Hole* attack is depicted in Figure 1, where a source node S intends to establish a route to a destination node D. In an AODV routing protocol, a source node would broadcast a RREQ packet to establish a route to a destination; with the normal intermediate nodes receiving and continuously broadcasting the

RREQ, except the *Black Hole* node. Everything works well if the RREP from a normal node reaches the source node first; but the RREP from *Black Hole* could reach the source node first, if it is nearer to the source node. Moreover, a *Black Hole* node does not need to check its routing table when sending false RREP message; its response is likely to reach the source node first. This makes the source node to conclude that the route discovery process is complete, ignoring all other RREPs and beginning to send data packets. The *Black Hole* node would directly send a route reply (RREP) to the source node S, with an extremely large sequence number and hop count of 1, as shown in Figure 1(a). The destination node D would also select a route with a minimum hop count upon receiving RREQs from normal nodes, and send a RREP packet as illustrated in Figure 1(b). Based on the AODV protocol, a source node S would select the latest and shortest (i.e., largest sequence number and minimum hop count) route to send the data packets from the RREPs packets received. It implies that a route via the *Black Hole* node would be selected by node S. The received data packets by the *Black Hole* node will then be eavesdropped or dropped as in Figure 1(c). Therefore, source and destination nodes are unable to communicate with each other as highlighted in (Kurosawa *et al*. 2007).

The malicious (*Black Hole*) node always sends RREP as soon as it receives RREQ without performing standard AODV operations, while keeping the destination sequence number very high. Since AODV considers RREP having higher value of destination sequence number to be fresh, the RREP sent by the malicious (*Black Hole*) node is treated fresh. Thus, the malicious nodes succeed in injecting *Black Hole* attacks.



a) RREQ flooding b) RREP Replying c) Black Hole attack

Figure 1: A Black Hole attack illustration

5. Black Hole Attack Solution Challenges

Routing algorithms using sequence numbers and hop counts in determining best routes such as AODV are likely to experience *Black Hole* attacks. Numerous approaches have been proposed in the literature to guard the algorithms against such attacks. The AODV routing protocol was revised in (Dokurer *et al*. 2007) to reduce opportunities for a *Black Hole* node to acquire a route by the source node dropping the first two received RREPs, but selectively picking any subsequent RREP packets. This approach will likely be appropriate in cases where a *Black Hole* node is located nearer to a source node and is likely to underperform when it is located many hops away from the source node.

A proposal that a source node waits for a predetermined time value to receive other RREPs with next hop details from the other neighbouring nodes, without sending the DATA packets to the first RREP node at once is presented in (Tamilselvan and Sankaranarayanan, 2007). Upon the expiry of the timer, it checks in its routing table to find out any repeated next hop node. It then assumes that the paths are correct or the chance of malicious path is limited if any repeated next hop node is present in the RREP paths. And upon comparison of the received RREPs, it randomly selects a neighbour which has the same next hop as other alternative routes to send the data packets. This solution adds a delay and decreases throughput as more RREPs are waited for, and the process of finding repeated next hop is an extra overhead.

The PCBHA (Prevention of a Co-operative Black Hole Attack) proposed in (Tamilselvan and Sankaranarayanan, 2008) is another revised AODV routing protocol aimed at preventing cooperative *Black Holes* attack. It begins by providing each legal user with a default fidelity level. After broadcasting a RREQ, a source node waits for RREQs from its neighbours and then selects a neighbour with a higher fidelity level, which exceeds the threshold value, for data packets forwarding. The destination node sends an acknowledgement message (ACK) after receiving a data packet and the source node may increase the neighbour's fidelity level by 1, upon receiving the ACK response. A neighbour's fidelity level will be reduced by 1 if no ACK response is received by the source, which indicates a possible *Black Hole* node on the route, which drops data packets before reaching the destination node. The approach works well where the malicious node is not in a position to generate an ACK packet with a faked destination identity (ID). This implies that a source node has to counter check the IDs in the ACK table entities to verify that it is indeed from the destination node. However, the selection of an optimal threshold fidelity level still needs to be determined for accurate detection.

A dynamic learning method intended to detect a *Black Hole* node is proposed in (Kurosawa *et al*. 2007). It observes if the characteristic change of a node exceeds the threshold within a given time period. A node is declared a *Black Hole* node if its characteristic change exceeds the threshold. Otherwise, the latest observation data is added into dataset for dynamic updates. The characteristics observed are the number of sent RREQs, the number of received RREPs, and the mean destination sequence numbers of the observed RREQs and RREPs. However, there is no detection mode such as revising the AODV protocol, thus, *Black Hole* nodes are not isolated by this approach. Furthermore, this comes with increased processing overhead and the determination of optimal threshold values remains unresolved.

An attempt to address the survivability problem of the routing service when selective dropping attacks were launched, using trusted nodes to monitor neighbours is presented in (Marti *et al.* 2000). However, the method could not work well in a sparse network where there were no enough neighbours to act as the monitoring nodes. A proposal that each node overhears all traffic of its neighbours and then compares the values observed with some metric to detect abnormal behaviours in the network is made in (Huang and Lee, 2003). The approach requires nodes to be in promiscuous mode and process all overheard packets, which can be energy consuming, impacting negatively on energy constrained mobile nodes. Furthermore, nodes might not overhear neighbours' transmissions in a sparse network due to insufficient transmission power, which limits transmission ranges.

An improved ferry based detection method (MUTON) in which the transitive property was considered, achieving a better detection performance than FBIDM is proposed in (Ren *et al*. 2010). However, MUTON similarly uses trusted ferry nodes in its detection mechanism, thus, requiring additional devices to be deployed in the network, which may not be economical or feasible. The concept of encounter tickets to secure the evidence of nodes' communication is introduced in (Li *et al*. 2009). The nodes uniquely interpret the contact history by making observations based on the encounter tickets. However, the method can only prevent the attacker from claiming non-existent encounters, but cannot address the packet dropping.

Secure AODV (Zapata, 2002) defines a set of message extensions to RREQ, RREP and RERR messages in AODV. New messages also exist for detecting duplicate network addresses. The mechanism provides the authentication of the originator and destination nodes. However, it has weaknesses; nothing prevents a node from increasing a hop count arbitrarily or leaving it unchanged. Malicious nodes can acquire routes by consistently declaring high hop counts. Further weakness is that it does not protect the sender IP address field. A malicious (*Black Hole*) node can impersonate another node while forwarding a RREP to acquire routes. Hence, encryption solution approaches do not address packet dropping by a *Black Hole* node.

Two *Black Hole* attack detection approaches are proposed in (Ning and Sum, 2003): sending a ping packet to the destination to confirm the established route and waiting for the receipt of an acknowledgement, failure of which the presence of a *Black Hole* is deduced; and keeping track of sequence numbers since *Black Hole* nodes usually temper with them, sending packets with unusually high sequence numbers. However, the ping packet increases delay and traffic overhead.

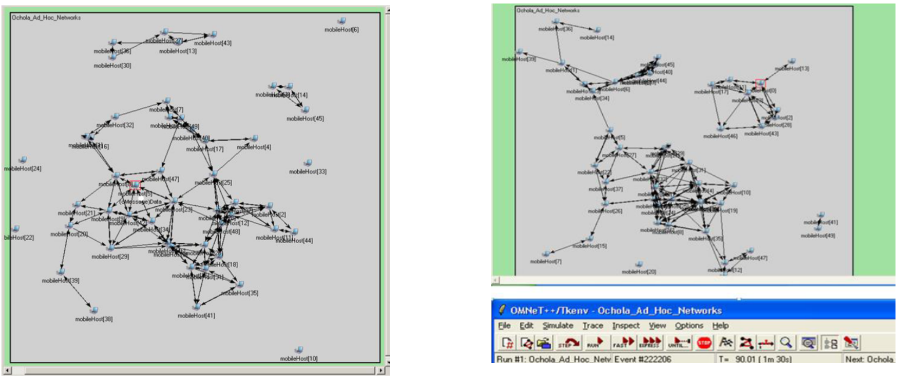
A dynamic learning system (DPRAODV) which checks to detect the existence of a RREP sequence number (RREP_seq_no) that is higher than the threshold value is proposed in (Raj and Swadas, 2009). A node is then suspected to be malicious (*Black Hole*) if its RREP_seq_no is higher than the threshold value, and is added to the black list. The threshold value is dynamically updated at every time interval. And a node sends a control packet ALARM, to its neighbours whenever it detects an anomaly. The ALARM packet has the black list node as a parameter, notifying the neighbouring nodes to discard any RREP packet from any suspected malicious node (i.e., no processing is done to the packet). However, the dynamic update of the threshold value at every time interval leads to overheads. Similarly, the determination of an optimal threshold value is necessary for accurate anomaly detection.

A protocol requiring intermediate nodes to send RREP packets containing next hop information is proposed in (Deng *et al*. 2002). A source node receiving a RREP will send a RREQ to the next hop to verify the existence of a route to the RREP generator from the next hop, and another route from the next hop to the destination. When the next hop receives the route verification RREQ, it sends back a further reply to source node with check results. The source node finally judges the validity of the route based on the further reply information. This approach leads to an increased delay.

The existing solutions analyses show the loopholes in detections and eliminations of *Black Hole* attacks in AODV routing protocol. Hence, there is a need for the development of a ‘perfect’ *Black Hole* attack detection and elimination mechanism.

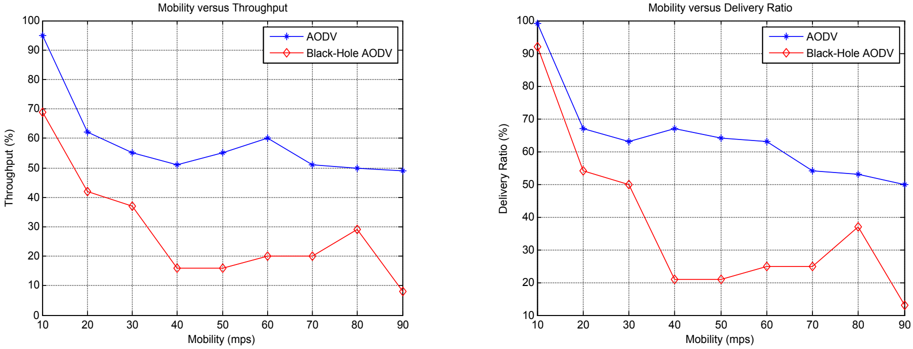
6. Simulation Performance Analysis

The simulation was done using OMNeT++ discrete events simulator, to analyse the AODV routing performance under the influence of a *Black Hole* attack, by varying the node mobility speed. Simulation setup illustrating the dynamic topology challenge in MANETs is shown in Figure 2.


Ochola_Ad_Hoc_Networks
Ochola_Ad_Hoc_Networks
OMNeT++/Tkenv - Ochola_Ad_Hoc_Networks
File Edit Simulate Trace Inspect View Options Help
STEP RUN FAST EXPRESS UNTIL STOP
Run #1: Ochola_Ad_Hoc_Netw Event #222206
T= 90.01 (1m 30s)
Next: Ochola

(a) Network topology at simulation time = 7200 sec. **(b) Network topology at simulation time = 90 sec.**

Figure 2: Simulation setup showing MANET dynamic topology



(a) Effect of Black Hole attack on the network throughput **(b) Effect of Black Hole attack on the network packet delivery ratio**

Figure 3: Effect of Black Hole Attack on the network performance

The metrics used to evaluate the routing performance are throughput and packet delivery ratio. The effect of a *Black Hole* attack on AODV routing protocol performance were evaluated as follows:

a) Throughput decreases in the presence of a *Black Hole* node in the network as shown in Figure 3 (a). The analysis shows that throughput is very high in AODV than *Black-Hole AODV* because of higher packet loss in the latter, as a result of packet dropping by the *Black Hole* node.
b) Packet delivery ratio decreases when there is a malicious (*Black Hole*) node in the network as shown in Figure 3 (b). This is because some of the packets are dropped by the *Black Hole* node and not received at the destinations.

7. Conclusion

Black Hole attack is one of the most serious security problems in MANET. It is an attack where a malicious (*Black Hole*) node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. The paper analyses secure routing in MANET against *Black Hole* attack. The existing solutions affect the AODV routing protocol performance negatively in terms of throughput, delay and overheads. Although these may not be avoided in totality, there is a need for trade-offs to achieve a secure optimal performances. The analyses necessitate that optimal threshold values should be determined for accurate anomaly detections, with trade-offs in delays and overheads, during characteristic changes detections.

8. References

Anjum, F., Ghosh, A.K., Golmie, N., Kolodzy, P., Poovendran, R., Shorey, R. and Lee, D. (2006), "Security in Wireless Ad hoc Networks", *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 217-220.

Cerri, D. and Ghioni, A. (2008), "Securing AODV: The A-SAODV Secure Routing Prototype", *IEEE Communications Magazine*, February 2008, pp. 120-125.

Deng, H., Li, W. and Agrawal, D.P. (2002), "Routing Security in Ad Hoc Networks", *IEEE Communications Magazine, Special Topics on Secuity in Telecommunication Networks*, vol. 40, no. 10, pp. 144-146.

Dokurer, S., Erten, Y.M. and Acar, C.E. (2007), "Performance Analysis of Ad-hoc Networks under Black Hole Attacks", *In Proceedings of the IEEE SoutheastCon*, 22-25 March 2007, Richmond, VA, pp. 148-153.

Huang, Y. and Lee, W. (2003), "A cooperative intrusion detection system for ad hoc networks", *In Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks (SASN '03)*, 27-30 October 2003, Washington, DC, USA, pp. 135-147.

Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A. and Nemoto, Y. (2007), "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", *International Journal of Network Security*, vol. 5, no. 3, pp 338-346.

Li, F., Wu, J. and Srinivasan, A. (2009), "Thwarting black hole attacks in distruption-tolerant networks using encounter tickets", *In Proceedings of the IEEE INFOCOM 2009*, 19-25 April 2009, Rio de Janeiro, pp. 2428-2436.

Liu, K., Deng, J., Varshney, P.K. and Balakrishnan, K. (2007), "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs", *IEEE Transaction on Mobile Computing*, vol. 6, no. 5, pp. 536-550.

Marti, S., Giuli, T.J., Lai, K. and Baker, M. (2000), "Mitigating routing misbehavior in mobile ad hoc networks", *In Proceedings of the 6th annual international conference on Mobile computing and networking (MobiCom '00)*, 6-11 August 2000, Boston, MA, USA, pp. 255-265.

Ning, P. and Sum, K. (2003), "How to misuse AODV: A case study of insider attack against mobile ad hoc routing protocol", *In Proceedings of the IEEE Systems, Man and Cybernetics Society Information Assurance Workshop*, 18-20 June 2003, United States Military Academy, West Point, NY, pp. 60-67.

Poongothai, T. and Jayarajan, K. (2008), "A non-cooperative game approach for intrusion detection in Mobile Adhoc networks", *In Proceedings of the International Conference on Computing, Communication and Networking (ICCCn 2008)*, 18-20 December 2008, St. Thomas, VI, pp 1-4.

Raj, P.N. and Swadas, P.B. (2009), "DPRAODV: A Dyanamic Learning System Against Blackhole Attack In Aodv Based Manet", *International Journal of Computer Science Issues (IJCSI)*, vol. 2, pp 54-59.

Ren, Y., Chuah, M.C., Yang, J. and Chen, Y. (2010), "Muton: Detecting malicious nodes in disruption-tolerant networks", *In Proceedings of WCNC'2010*, pp. 1-6.

Singh, K., Yadav, R.S. and Ranvijay (2010), "A Review Paper on Ad Hoc Network Security", *International Journal of Computer Science and Security*, vol. 1, no. 1, pp. 52-69.

Su, M.Y. (2011), "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", *Computer Communications*, vol. 34, no. 1, pp. 107-117.

Tamilselvan, L. and Sankaranarayanan, V. (2007), "Prevention of Impersonation Attack in Wireless Mobile Ad hoc Networks", *International Journal of Computer Science and Network Security (IJCSNS)*, vol. 7, no. 3, pp. 118-123.

Tamilselvan, L. and Sankaranarayanan, V. (2008), "Prevention of co-operative black hole attack in MANET", *Journal of Networks*, vol. 3, no. 5, pp.13-20.

Zapata, M.G. (2002), "Secure ad hoc on-demand distance vector routing", *Mobile Computing and Communications Review*, vol. 6, no.3, pp. 106-107.