Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-34

AODV vs. DSR: Simulation Based Comparison of Ad-hoc Network Reactive Protocols under Black Hole Attack

Lineo Mejaele and Elisha Oketch Ochola

***Abstract*— Mobile Ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of any fixed network infrastructure or centralized administration. Due to its fundamental characteristics such as open medium, dynamic topology and lack of central monitoring, MANET is vulnerable to security attacks. Black hole attack is one of the MANET attacks. In black hole attack, a malicious node attracts all packets to itself by falsely claiming a fresh route to destination and absorbs the packets without forwarding. Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) are popular MANET reactive routing protocols. This paper evaluates the performance of AODV and DSR under black hole attack. In our work, we simulated black hole attack in Network Simulator 2 (NS-2) and measured throughput, packet delivery ratio and end-to-end delay in a network with and without a black hole.**

***Keywords*— MANET, AODV, DSR, Black hole**

I. Introduction

MANET is a self-configuring network that is formed by a group of mobile devices via wireless communication channels. MANETs have no central administration or fixed network infrastructure and can therefore be constructed quickly and at a low cost [13]. The nodes move randomly in different directions and speeds in MANETs [2]. There are no dedicated routers, servers, access points and cables. Therefore, routing is done in mutual agreement and understanding between nodes. Mobile nodes within each other’s wireless transmission ranges can communicate directly; otherwise, intermediate nodes have to forward the packets to the destination node [24]. Every mobile node has to function as a router, to forward packets for others [19].

Mobile nodes in MANET can be of different types (PDAs, laptops, mobile phones, routers, printers, etc.) and are equipped with wireless transmitters and receivers [16, 24]. Since mobile nodes can move around; leave and join the network at any time, MANETs have a very dynamic network topology [20]. MANETs can find applications in areas where it is not possible to have a network infrastructure, but need temporary network connectivity. Typical applications include; military battlefield, disaster relief, temporary networks and vehicular networks [6].

- **Military Battlefield**: Military equipment now contains some sort of computation capabilities. MANETs help to overcome geographical barriers in a military operation by maintaining information network between the soldiers, vehicles, and military information headquarters [24].
- **Disaster Relief**: MANET can be used to replace damaged network infrastructure when temporary network is immediately needed. The possible causes of network infrastructure damage could be fire, earthquakes, and floods. Emergency rescue operations can take place through rapid redeployment of damaged communication network. Information is relayed from one rescue team member to another over a small hand held device [6].
- **Temporary Networks**: Today people attend meeting, conferences and classrooms with mobile devices such as laptops, notebooks and tablets. MANET can facilitate the formation of a temporary network so that participants can share information [21].
- **Vehicular networks:** MANET can be of importance in vehicular communications where vehicles would communicate collision warning to the drivers [17].

Routing is particularly challenging in MANET due to features such as dynamic network topology, lack of infrastructure, limited battery power, different devices, and open and bandwidth constraint channels [13]. Several MANET routing protocols have been defined to achieve an efficient routing mechanism. These are classified as proactive, reactive and hybrid protocols, depending on how nodes establish and maintain paths [5]. Proactive are table-driven routing protocols that attempt to maintain up-to-date routing information from each node to every other node in the network [6]. Reactive are on-demand routing protocols that find routes only when they need to send data to destination whose route is unknown [21]. Hybrid protocols combine the advantages of proactive and reactive protocols to get better results [18]. AODV and DSR are examples of reactive protocols.

Security is essential for both wired and wireless networks to provide protected communication. The success of MANET strongly depends on people’s confidence in its security. The

Lineo Mejaele
School of Computing, University of South Africa, Pretoria
South Africa

Elisha Oketch Ochola
School of Computing, University of South Africa, Pretoria
South Africa

Proc. of the Second Intl. Conf. on Advances in Computing, Electronics and Electrical Technology - CEET 2014.
Copyright © Institute of Research Engineers and Doctors, USA .All rights reserved.
ISBN: 978-1-63248-034-7 doi: 10.15224/ 978-1-63248-034-7-34

design of secure MANET routing protocols must fulfil five security requirements which are *confidentiality*, *integrity*, *availability*, *authentication* and *non-repudiation* for proper communication [23].

- **Confidentiality** ensures that information transmitted on the network is not accessible to unauthorized entities. Network transmission of sensitive information requires confidentiality. Leakage of such information to unauthorised parties could have upsetting consequences [25].
- **Integrity** guarantees that message received at the destination is exactly identical to the same message when it was sent at the source. Integrity can be compromised mainly in two ways:
    i. Malicious altering whereby a message can be removed, replayed or revised by an adversary with malicious goal.
    ii. Accidental altering in which the message is lost or its content is changed due to some transmission errors in communication or hardware errors [10].
- **Availability** means that a node should maintain its ability to provide all the designed services regardless of the security state. This attribute can be affected by Denial of Service (DoS) attack in which some selfish node can make some of the network services unavailable [10].
- **Authentication** is an assurance that participants in a communication are genuine and not impersonators. Each node must have identity of the peer nodes it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes [26].
- **Non-repudiation** ensures that the origin of a message cannot deny having sent the message. This is useful especially when it is needed to determine if a node with some abnormal behaviour is compromised or not. If a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message may have been compromised [10].

MANET is prone to many security attacks due to its characteristics. Black hole attack is one type of MANET routing attacks [9].

The rest of the paper is organized as follows: Section II describes an overview of AODV and DSR protocols. Section III discusses black hole attack. Section IV presents simulation environment. Section V discusses results obtained in simulations. Section VI presents the conclusion of the paper.

II. Overview of AODV and DSR Routing Protocols

This section gives the description of the two on-demand routing protocols AODV and DSR. It further illustrates the route discovery process using a flow diagram.

A. *Ad hoc On-demand Distance Vector Protocol*

AODV is an on-demand routing protocol that is used to find a route between the source and the destination node, and it is the most well-known MANET protocol [3]. Route finding is based on a route discovery cycle involving a broadcast network search and a unicast reply containing discovered paths [1]. Every node maintains a table containing information about a neighbour it intends to send packets to in order to reach destination. Each node broadcasts hello messages after a specific time interval to keep track of its neighbours [7].

The route discovery process is started by a source node that wants to communicate with a destination node for which there is no routing information in its routing table [7]. The source node performs route discovery by broadcasting route request (RREQ) packet [14]. Every node that receives the RREQ packet first checks if it is the destination for the packet, and if so, it sends back route reply (RREP) packet. If not, it checks with its routing table to determine if it has got route to destination. If not, it relays the RREQ packet by broadcasting to the neighbours.

If routing table does contain an entry to the destination, then the next step is the comparison of destination sequence number in its routing table to that present in RREQ packet, if destination sequence number is less than or equal to the one contained in RREQ packet, the node relays request further to its neighbours. If the destination sequence number in the routing table is higher than the one in RREQ packet, then it denotes that the route is a fresh route and packets can be sent through this route. The intermediate node then sends a unicast RREP packet to the source node through reverse route. The source node updates its routing table once it receives the RREP and starts utilizing the path for the transmission of data packets [7, 12]. For route maintenance, if any node identifies link failure during operation, it sends a route error (RERR) packet to all other nodes that use this link for their communication to other nodes [12].

B. *Dynamic Source Routing Protocol*

DSR [8] is an on-demand routing protocol that is based on the concept of source routing, that is the source node always knows the complete route from source to destination [7]. Mobile nodes are required to maintain route caches that contain the source routes, and entries in the route cache are continuously updated as new routes are learned [11]. DSR allows multiple routes to destination node and this makes routing to be loop-free.

When a node has a packet to send to some destination, it first consults its route cache to determine whether it already has a route to the destination. If it has an unexpired route to the destination, it will use this route to send the packet. On the other hand, if it does not have such a route, it initiates route discovery by broadcasting RREQ packet. To limit the number of RREQs, a node processes RREQ only if it has not already received it [11]. RREP packet is generated and sent to the source node when the RREQ packet reaches either the destination or an intermediate node which contains unexpired route to destination in its cache. Once the source node receives RREP packet, it starts transmitting data packets to the destination [5].

For maintenance of the routes, each node transmitting the packet is responsible for confirming that a packet has been received by next hop node along the source route. If there is no receipt confirmation received, then there is a link breakage and the source of the route will be notified with a RERR message, and it can send the packet using another existing route or perform a new route discovery [11, 26].

C. *Route Discovery Process Flow chart*

The flow chart (Fig. 1) below summarizes route discovery process in AODV and DSR as explained in section II.A and section II.B above. The source node (SN) starts the process by broadcasting RREQ, which is received by the intermediate node (IN). If the IN is not the destination node (DN), it checks if it has a route to destination in its routing table. If the route does exist, it compares the sequence number (seq.no) of route to sequence number in RREQ. If route's sequence number is higher, RREP is sent else IN further broadcasts RREQ.

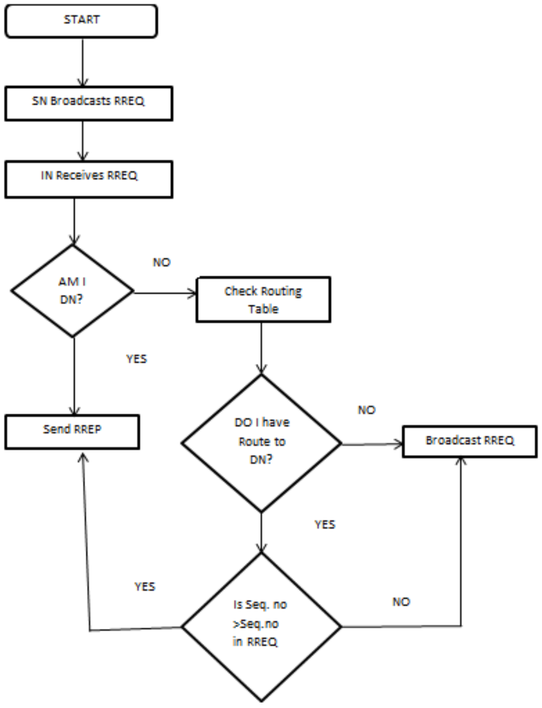

Figure 1. Route discovery process flow chart.

III. Black Hole Attack

Black hole attack is one of the security attacks that results from misbehaviour of a node. The misbehaving node acts as selfish or malicious node and is called a black hole [22]. This is a type of routing attack where a malicious node makes use of vulnerabilities of route discovery packets of routing protocols by advertising itself as having the shortest and freshest route to destination node. It achieves this by sending fake route replies and thereby attracting other 'good' nodes to send their data packets through it and drops them [15]. By doing this, the malicious node can deprive the traffic from the source node and disrupt communication among mobile nodes. After receiving the data packets, the black hole can be used as a denial-of-service attack where it can drop the packets or intercept the packets; hence confidentiality of the message is disclosed in the presence of black hole attack [22].

The figure (Fig. 2) below illustrates how the black hole attack can occur.

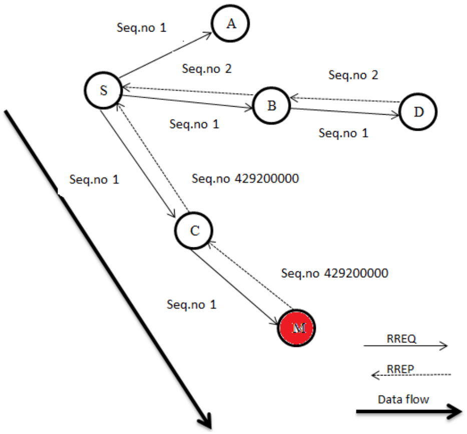

Figure 2. Black hole attack.

Suppose the source node S wants to send data packets to destination node D. It will initiate a route discovery process by broadcasting RREQ packet. If node M is malicious, it will claim to have a fresh enough route to D and will send RREP with highest sequence number as soon as it receives the RREQ packet. M will send RREP packet to S before any other node in the network because it is advantaged due to the fact that it does not have to search its routing table for route to destination. Node S will then think that the route discovery process is complete and will ignore all other replies and start forwarding data packets to malicious node M which will drop all the packets.

IV. Simulation Environment

Simulations have been carried out using Network Simulator 2 (NS-2) [4] to analyse AODV and DSR routing performance under black hole attack. The random waypoint model is selected as a mobility model. Random way point mobility specifies that at every instant, a node randomly chooses a destination and moves towards it with speed chosen randomly. After reaching the destination, the node stops for a duration defined by pause time parameter, chooses another random destination and it repeats the process until simulation ends.

The terrain area for simulation is 670m X 670m with the number of nodes varying from 20 to 100 with maximum speed of 20m/s. The simulation time is 500 seconds and the transmission rate is 4 packets/sec. At the physical and data link layer, IEEE 802.11 algorithm is used, and the channel used is wireless channel with two ray ground radio propagation model. At the network layer, AODV and DSR are used as routing algorithms. UDP is used at the transport layer, all data packets are constant bit rate (CBR) and the packet size is 512 bytes. The simulation parameters are given in Table 1 below.

TABLE I. SIMULATION PARAMETERS

Parameter	Values
Mobility Model	Random Waypoint
Traffic Type	CBR (UDP)
Number of nodes	20 to 100
Terrain Area	670m X 670m
Routing Protocols	AODV, DSR
Transmission Rate	4 packets/sec
Simulation Time	500 seconds
Maximum Speed	20m/s
Pause Time	0 seconds
Transmission Range	250 m
Number of malicious node	1
Packet Size	512 bytes

The figures (Fig. 3 and Fig. 4) below illustrate NS-2 simulation snapshot extracted from Network Animator (NAM). NAM is a NS-2 analysis report that shows the visual representation of the simulation.

The illustration shows simulations for wireless network with seven nodes. Node 0 (green) is the source, node 3 (blue) is the destination and node 5 (red) is the attacker. Fig. 3 illustrates a scenario where data packets sent by the source reach destination, while Fig. 4 illustrates a scenario where data packets from source are absorbed by attacker node.

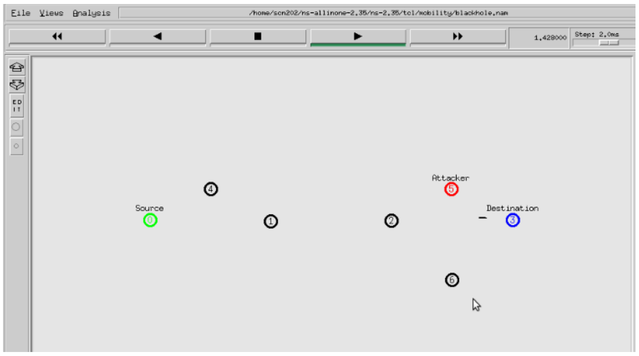

Figure 3. Packets reach destination.

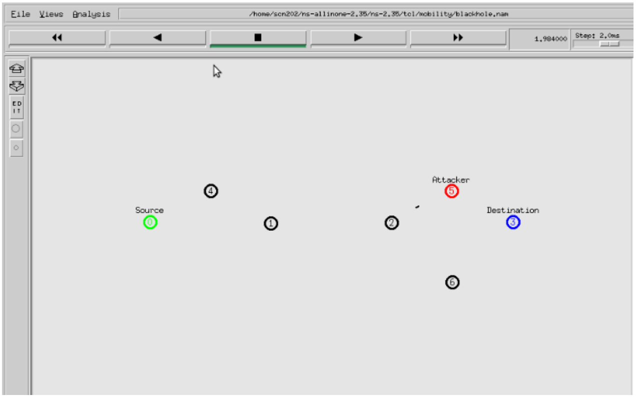

Figure 4. Packets absorbed by attacker.

V. Results and Discussions

The performance of AODV and DSR was measured by varying the number of mobile nodes in simulations based on the following performance metrics;

- Throughput: the average rate of successful message delivery over a communication channel.
- Packet Delivery Ratio: the ratio between the number of data packets that are sent by the source node and the number of packets that are received by the destination node.
- End-to-end Delay: the average time taken from generating the packet from source node till the reception of the packet by destination node.

A. *Results: Effect of Network Size*

The number of mobile nodes was varied from 20 to 100 nodes, keeping the maximum speed constant at 20m/s with maximum of 10 connections. The variations were done respectively, varying the routing protocol from AODV to DSR and introducing a black hole node in each of the protocols. The figures (Fig. 5, Fig. 6 and Fig. 7) below show the results taken from simulations, based on the performance metrics described in Section 5 above.

B. *Analysis*

As it can be seen from Fig. 5 and Fig. 6 that packet delivery ratio and throughput remain the same despite the increase in the number of nodes. DSR has a slightly more packet delivery ratio and throughput than AODV. This is because DSR always looks for the most fresh and reliable route when needed and does not look for it from the routing table like AODV.

Also from the Fig. 7, it is observed that end-to-end delay is higher in DSR than AODV. DSR is an on-demand source routing protocol and this is the major reason for it having a higher end- to-end delay. This means the route is looked only when needed and there is a route discovery mechanism happening every time and it also has to carry a large overhead each time, thus the higher delay. AODV on the other hand has only one route per destination in the routing table which is constantly updated based on the sequence number.

It is further observed that packet delivery ratio, throughput and end-to-end delay for both AODV and DSR decrease in the presence of black hole attack. DSR's performance is better than AODV's under black hole attack as it can be seen from the results that packet delivery ratio, throughput and end-to-end delay of AODV drops drastically to almost zero when the network is attacked by black hole.

Throughput and packet delivery ratio decrease when the network is under attack because of the packets discarded by malicious node during attack. End-to-end delay decreases when the network is under attack because of the immediate reply from a malicious node which would not check its routing table.

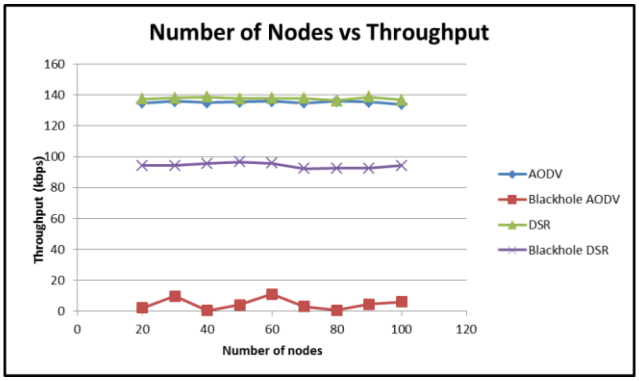

Figure 5. Throughput AODV vs. DSR.

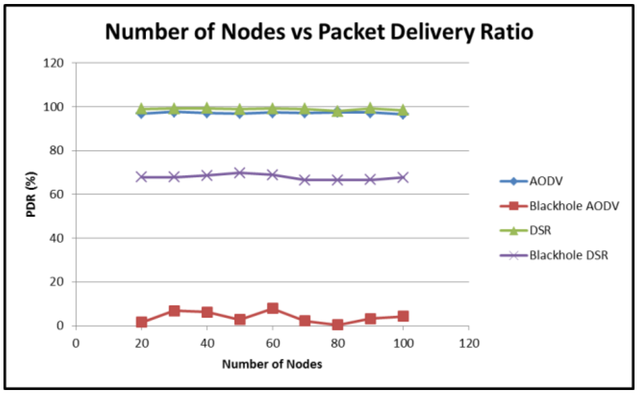

Figure 6. Packet Delivery Ratio AODV vs. DSR.

VI. Conclusions

MANETs can be deployed where the traditional network infrastructure is not feasible. Due to lack of infrastructure and other characteristics of MANETs security becomes an important issue in the deployment of MANETs. Black hole is one of the severe attacks that targets routing in MANETs. In this paper, the impact of black hole attack on performance of MANETs is analysed. Moreover, the performance of AODV and DSR under black hole attack is compared with the goal to find out which protocol shows less vulnerability in the case of black hole attack.

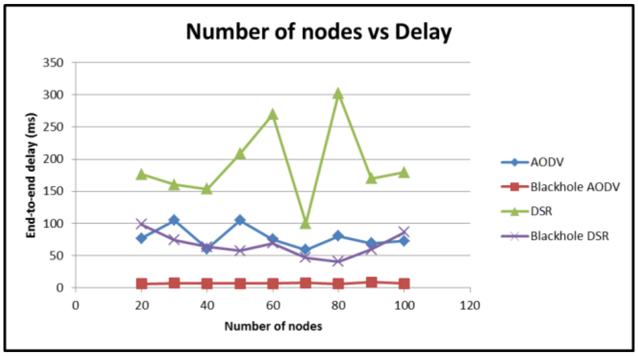

Figure 7. End-to-end Delay AODV vs. DSR.

In order to achieve the goal of the study, scenarios of AODV and DSR networks were simulated using NS-2. The first scenario for each of the protocol was simulated without attack and black hole attack was introduced in the second scenario for each of the protocols. Scenarios were simulated with respect to performance metrics of throughput, packet delivery ratio and end-to-end delay.

Having simulated the black hole attack, it was observed that MANET under regular operation outperforms MANET under black hole attack because the presence of black hole decreases throughput, packet delivery ratio and end-to-end delay.

Considering simulations for scenarios with 20 mobile nodes; for AODV network, when the black hole attack is launched, packet delivery ratio decreases by 95%, throughput decreases by 98% and end-to-end delay decreases by 92%. For DSR network, packet delivery ratio decreases by 31%, throughput decreases by 43% and end-to-end delay decreases by 43.9% when black hole attack is launched.

It can therefore be concluded from the above statistics that the impact of black hole is more severe in AODV than in DSR, and in comparison to AODV, DSR is the best routing protocol to be used in a networks that are frequently attacked by black hole.

Acknowledgment

This work is based on the research supported in part by University of South Africa (UNISA) and National University of Lesotho.

References

[1] AGRAWAL, R., TRIPATHI, R. AND TIWARI, S. 2011. Performance Evaluation and Comparison of AODV and DSR Under Adversarial Environment. In *Computational Intelligence and Communication Networks (CICN), 2011 International Conference on,* Anonymous IEEE, 596-600.

[2] DE OLIVEIRA SCHMIDT, R. AND TRENTIN, M.A.S. 2008. Manets routing protocols evaluation in a scenario with high mobility manet routing protocols performance and behavior. In *Network Operations and Management Symposium, 2008. NOMS 2008. IEEE,* Anonymous IEEE , 883-886.

[3] DOKURER, S., ERT, Y. AND ACAR, C.E. 2007. Performance analysis of ad-hoc networks under black hole attacks. In *SoutheastCon, 2007. Proceedings. IEEE,* Anonymous IEEE, 148-153.

[4] FALL, K. AND VARADHAN, K. 2005. The ns Manual (formerly ns Notes and Documentation). *The VINT project* 47.

[5] GIRUKA, V.C. AND SINGHAL, M. 2007. Secure Routing in Wireless Ad-Hoc Networks. *Wireless Network Security* 137-158.

[6] GOYAL, P., PARMAR, V. AND RISHI, R. 2011. Manet: vulnerabilities, challenges, attacks, application. *IJCEM International Journal of Computational Engineering & Management* 11, 32-37.

[7] JHAVERI, R.H., PATEL, A.D., PARMAR, J.D. AND SHAH, B.I. 2010. MANET routing protocols and wormhole attack against AODV. *International Journal of Computer Science and Network Security* 10, 12-18.

[8] JOHNSON, D.B. AND MALTZ, D.A. 1996. Dynamic source routing in ad hoc wireless networks. *Mobile computing* 153-181.

[9] KANNHAVONG, B., NAKAYAMA, H., NEMOTO, Y., KATO, N. AND JAMALIPOUR, A. 2007. A survey of routing attacks in mobile ad hoc networks. *Wireless Communications, IEEE* 14, 85-91.

[10] LI, W. AND JOSHI, A. 2008. Security issues in mobile ad hoc networks-a survey. Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County 1-23.

[11] MBARUSHIMANA, C. AND SHAHRABI, A. 2007. Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks. In *Advanced Information Networking and Applications Workshops, 2007, AINAW'07. 21st International Conference on,* Anonymous IEEE, 679-684.

[12] MEDADIAN, M., MEBADI, A. AND SHAHRI, E. 2009. Combat with Black Hole attack in AODV routing protocol. In *Communications (MICC), 2009 IEEE 9th Malaysia International Conference on,* Anonymous IEEE , 530-535.

[13] OSATHANUNKUL, K. AND ZHANG, N. 2011. A countermeasure to black hole attacks in mobile ad hoc networks. In *Networking, Sensing and Control (ICNSC), 2011 IEEE International Conference on,* Anonymous IEEE, 508-513.

[14] PUROHIT, N., SINHA, R. AND MAURYA, K. 2011. Simulation study of Black hole and Jellyfish attack on MANET using NS3. In *Engineering (NUiCONE), 2011 Nirma University International Conference on,* Anonymous IEEE, 1-5.

[15] RAJ, P.N. AND SWADAS, P.B. 2009. Dpraodv: A dyanamic learning system against blackhole attack in aodv based manet. *arXiv preprint arXiv:0909.2371* .

[16] RAJABHUSHANAM, C. AND KATHIRVEL, A. 2011. Survey of wireless MANET application in battlefield operations. *IJACSA) International Journal of Advanced Computer Science and Applications* 2.

[17] RAJESH, Y. AND ANIL K, S. 2012. Secure AODV protocol to mitigate Black hole attack in Mobile Ad hoc Networks .

[18] SINGH, P.K. AND SHARMA, G. 2012. An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on,* Anonymous IEEE, 902-906.

[19] STOJANOVIC, M., ACIMOVIC-RASPOPOVIC, V. AND TIMCENKO, V. 2012. The Impact of Mobility Patterns on MANET Vulnerability to DDoSAttacks. 3, 1392 – 1215.

[20] THACHIL, F. AND SHET, K. 2012. A trust based approach for AODV protocol to mitigate black hole attack in MANET. In *Computing Sciences (ICCS), 2012 International Conference on,* Anonymous IEEE, 281-285.

[21] THAKARE, A.N. AND JOSHI, M. 2010. Performance Analysis of AODV & DSR Routing Protocol in Mobile Ad hoc Networks. *IJCA Special issue on "Mobile Adhoc Networks", MANETs* 211-218.

[22] VANI, A. AND RAO, D.S. 2011. Removal of black hole attack in ad hoc wireless networks to provide confidentiality security service. *International Journal of Engineering Science* 3.

[23] WU, B., CHEN, J., WU, J. AND CARDEI, M. 2007. A survey of attacks and countermeasures in mobile ad hoc networks. *Wireless Network Security* 103-135.

[24] WU, B., CHEN, J., WU, J. AND CARDEI, M. 2007. A survey of attacks and countermeasures in mobile ad hoc networks. In *Wireless Network Security,* Anonymous Springer, 103-135.

[25] ZAIBA, I. 2011. Security issues, challenges and solution in MANET. 2, 108-109-112.

[26] ZHOU, H. 2003. A survey on routing protocols in MANETs. *Department of Computer Science and Engineering, Michigan State University, East Lansing, MI* 48824-41027.

About Authors:

Lineo Mejaele received her BSc. (Hons.) in Computer Science degree from University of Lesotho, Lesotho. She is a Demonstrator at the National University of Lesotho and pursuing her MSc. Computer Science at University of South Africa (UNISA), South Africa. Her research interests include security in Mobile Ad-hoc Networks (MANETs)

Elisha Oketch Ochola received his BSc. (Hons.) in Computer Science degree from Egerton University, Kenya, in 2004. He received double masters' degrees in Electronic Engineering (MSc. in Electronic Engineering) and Electrical Engineering (MTech. Telecommunication Technology) from *Ecole Supérieure d'Ingénieurs en Electronique et Electrotechnique (ESIEE)*, France, and Tshwane University of Technology (TUT), South Africa, respectively in 2008. He is a senior lecturer and advancing a PhD in Computer Science at University of South Africa (UNISA), South Africa. His research interests include routing protocol development, power consumption management, and security in Mobile Ad-hoc Networks (MANETs)