Journal of Theoretical and Applied Information Technology
31st July 2014. Vol. 65 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MALICIOUSNESS IN MOBILE AD HOC NETWORKS: A PERFORMANCE EVALUATION

[1]K. TAMIZARASU, [2] A.M. KALPANA, [3] Dr. M. RAJARAM

[1]Global Institute of Engineering and Technology, Department of Computer Science and Engineering, Vellore, Tamil Nadu, INDIA
[2]Govt. College of Engineering, Department of Computer Science and Engineering, Dharmapuri, Tamil Nadu, INDIA
[2] Anna University, Department of Electrical and Electronics Engineering, Chennai, Tamil Nadu, INDIA
E-mail: [1] tamizarasu.aor@gmail.com

ABSTRACT

Mobile Ad hoc Networks (MANETs) combine wireless communication with high node mobility. Limited wireless communication range and node mobility ensure that nodes cooperate with each other to provide networking, with network dynamically changing to ensure needs are met continually. The protocols dynamic nature enables MANET operation as suited to deployment in extreme circumstances. Hence, MANETs are a popular research topic and are proposed for use in areas like rescue operations, tactical operations and environmental monitoring. This study evaluates impact of malicious node attack (Black Hole Attack) on Ad hoc On-demand Distance Vector (AODV) MANET routing. The experiment consists of 25 nodes distributed over 2 square kilometres. AODV routing protocol is resorted to. Three experiments were conducted, the first without malicious nodes and with 10% and 20% of malicious nodes.

Keywords: *Mobile Ad Hoc Networks (Manets), Routing In MANET, Ad Hoc On-Demand Distance Vector (AODV), And Black Hole Attack*

1. INTRODUCTION

A MANET is a self-configuring mobile router, and associated hosts network is connected by wireless links – whose union forms a random topology. Routers move randomly and organize themselves randomly; hence, network's wireless topology may also change rapidly and unpredictably [1]. Such networks operate in standalone fashion, or can be connected to a larger Internet. Minimal configuration and speedy deployment make ad hoc networks suit emergency situations like natural or human disasters, military engagements and emergency medical situations. Many MANET applications involve communication modes of one-to-many and many-to-many making group communication a most important communication way. Also, due to the projection of the opening MANET character the issue of providing safe communication is hot. Safe group communication is widely regarded and has progressed rapidly [2].

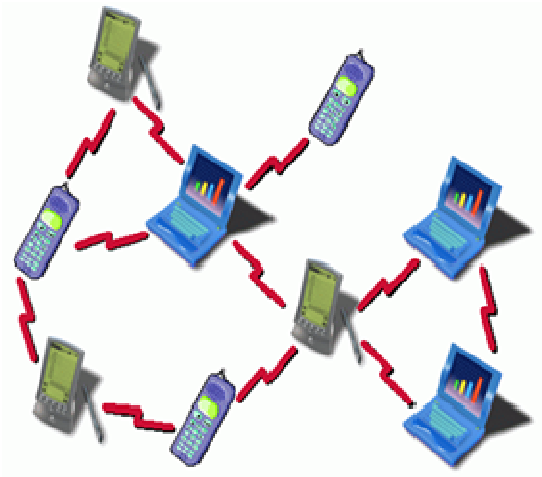

Figure 1: *Mobile Ad Hoc Network*

MANETs are a fast growing research area. They are attractive for many applications like rescue and tactical operations, due to their dynamic infrastructure's flexibility. This flexibility is at a price and introduces new security threats. Further, many conventional security solutions for wired networks are ineffectual and inefficient for highly

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

dynamic and resource-constrained environments where MANETs are used [3].

Nodes move freely from one location to another in ad hoc networks so node mobility on a path proven by source may not exist after a short time. Routing determines path from source to destination to enable nodes to communicate. Ad-hoc network's routing protocols are reactive, proactive and hybrid.

Reactive protocols are also called demand driven protocol as they locate a path only when necessary. They discover a new route by sending a route request and receiving a route reply. Only active routes are maintained by nodes. Delay is their major drawback due to route discovery.

Proactive protocols are also called table driven protocols and they regularly maintain network topology. In a network all nodes have information of neighbors in advance. Different tables are used to keep routing information and tables are updated according to network topology changes. Topology information is exchanged by nodes so that they have route information any time when needed.

Combining proactive and reactive protocols form hybrid protocols which use distance-vector for precise metrics to establish best path to destination networks. Routers alone maintain information about adjacent routers in hybrid protocols. Source initiates route establishment to a given destination on demand during reactive operation [4].

AODV is an on-demand, single path, loop-free distance vector protocol which combines on-demand route discovery mechanism in DSR with destination sequence numbers from DSDV. Unlike DSR which uses source routing, AODV resorts to hop-by-hop routing. AOMDV shares many characteristics with AODV. It is based on distance vector concept and uses hop-by-hop routing. Also, AOMDV locates routes on demand using route discovery. The difference lies in number of routes located in each route discovery. In AOMDV, RREQ propagation from source to destination establishes multiple reverse paths at intermediate nodes and the destination. Multiple RREPs traverse reverse paths to form multiple forward paths to destination at source and intermediate nodes. Note that AOMDV provides intermediate nodes with alternate paths as they reduce route discovery frequency.

The AOMDV protocol core ensures that discovered multiple paths are loop-free and disjoint, and efficiently finds such paths using a flood-based route discovery. AOMDV route update rules when applied locally at every node maintain loop-freedom and dis-jointness properties [5].

AOMDV calculates multiple paths during route discovery in highly dynamic ad hoc networks where link breakage is frequent due to vehicles high velocity. A route discovery procedure is needed after each link failure in AODV routing protocol. Performing this leads to high overhead and latency. So, this defect is overcome through multiple paths. Performing route discovery in AOMDV is done after paths to source or destination fail. In AOMDV routing protocol, it endeavors to utilize routing information available in underlying AODV protocol. But, little additional modification is required to calculate multiple paths. AOMDV protocol includes two sub-procedures:

- Calculating multiple loop-free paths at every node: In AODV protocol, route discovery defines an alternate path to source or destination potentially. Every RREQ packet copy received by a node, introduces an alternate path to source.

- Finding link-disjoint paths by using distributed protocols: Loop-free mechanism enables nodes to establish multiple paths to destinations that take it to the next stage i.e. dis-jointness process [6].

Securing wireless ad-hoc networks is highly challenging. Understanding the type of attack is the first step to developing security solutions. MANET communication security is important for secure information transmission. Absence of a central co-ordination tool and shared wireless medium make MANETs vulnerable to digital/cyber-attacks compared to wired networks. There are many attacks that affect MANETs and they are classified into two types:

- Passive attack
- Active attack

Passive attacks do not disrupt proper network operation. The attacker snoops on data exchanged in the network without touching it. Here, confidentiality can be violated if attacker interprets data gathered through snooping. Passive attacks detection is difficult as network operation itself is not affected. A way to prevent such problems is by using powerful encryption mechanisms to encrypt data being transmitted, making it impossible for eavesdroppers to get useful information from overheard data. E.g. Snooping: Snooping is unauthorized accessing of another person's data.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Active attacks try to alter/destroy data being exchanged in a network, disrupting normal network functioning. It is classified as external attacks and internal attacks. External attacks are carried out by nodes from without the network and they can be prevented by recourse to standard security mechanisms like encryption techniques and firewalls. Internal attacks are through compromised nodes which form part of the network [7-9].

Black hole attack is a possible attack on MANET where a malicious node sends a forged Route REPLY (RREP) packet to source node which initiates route discovery pretending to be a destination node. By comparing destination sequence number in RREP packets when a source node receives multiple RREPs, it judges the greatest as most recent routing information and selects route in that RREP packet. If sequence numbers are equal it selects a route with smallest hop count. If attacker spoofed the identity to be the destination node and sends RREP with destination sequence number higher than real destination node to source node, data traffic flows to the attacker. Hence, source and destination nodes are unable to communicate [10]. In flooding based protocols, when a malicious reply reaches requesting node before reply from actual node, a forged route is created. The malicious node then chooses whether to drop packets to perform a denial-of-service attack or use its place on route as first step in a man-in-the-middle attack [11].

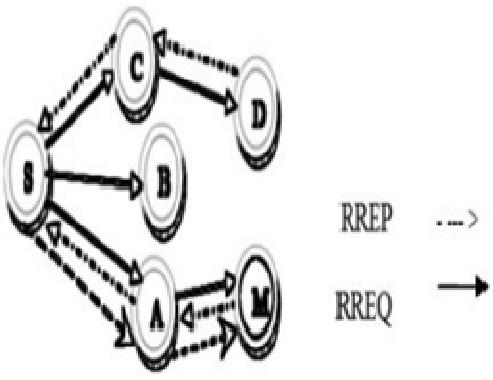

Figure 2: Black Hole Attack In MANET [12]

This study evaluates impact of malicious node attack (black hole attack) on AODV routing in MANETs. The experiment consists of 25 nodes distributed over 2 square kilometres. AODV routing protocol is used. The study is organized as follows: section 2 deals with reviews of some approaches for malicious node attack (black hole attack) on AODV routing in MANET available in literature. Section 3 discusses methodology used and section 4 reports results of experiments and section 5 concludes the paper.

2. LITERATURE REVIEW

Performance evaluation of energy consumption for DSR and AODV routing protocols in MANET was proposed by Barati, et al., [13] which discussed power consumption aspect of MANET routing protocols. Performance comparison of AODV and DSR routing protocols regarding average energy consumption and routing energy consumption were explained. An evaluation of how varying metrics in diverse scenarios affected power consumption in both protocols was discussed. Simulation model using Network Simulator with varied mobility and traffic models was used to study energy consumption. Finally, a routing protocols evaluation based on energy consumption was presented.

An efficient prevention of black hole problem in AODV routing protocol in MANET was proposed by Singh and Sharma [14], which suggested a solution to black hole attack in a prominent routing algorithm, AODV routing, for MANETs. The new method used promiscuous modes to detect malicious nodes and propagated this information to other network nodes. Simulation results showed the new method's efficacy as network throughput did not deteriorate in the presence of black holes.

Modified AODV routing protocol based on route stability in MANET was suggested by Mou and Meng [15], where the author suggested a new modified AODV routing protocol called MAODV which considered route stability to establish a stable path between source and destination. In MAODV some changes were made in Hello and RREQ message format to record sending time and route stability factors. Network simulator-2.30 simulated AODV and MAODV protocols in similar scenarios. Results comparison and analysis evaluated effectiveness of MAODV and it was found that it improved performance in some ways.

Combat with black hole attack in AODV MANET routing protocol was proposed by Medadian, et al., [16] which proposed combating black hole attack through negotiation with neighbours which claimed to have a destination route. Simulation results revealed that the new protocol provided better security and performance regarding packet delivery than conventional AODV in black holes with minimal additional delay and overhead.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MANET performance analysis under black hole attack was suggested by Bala, et al., [17], which simulated black hole attack, a possible attack on AODV routing protocol in MANETs with the help of network simulator (NS-2). Simulation results revealed packet loss, throughput, and end-to-end delay with and without black hole on AODV in MANETs. It also revealed that network packet loss increased with a black hole node. It was seen that throughput and end-to-end delay decreased with black hole node in the network.

Malicious AODV: implementation and analysis of routing attacks in MANETs was proposed by Ehsan and Khan [18], where author investigated some severe attacks against MANETs like black hole and sinkhole attacks, selfish node behaviour, RREQ and hello floods and selective forwarding attack. A detailed NS-2 implementation of such attacks being launched successfully using AODV routing protocol was presented and a comparative analysis of attacks was performed. The new method used routing overhead, packet efficiency and throughput as performance metrics. Simulation showed that flooding attacks like RREQ and hello floods drastically increased routing protocol overhead. Route modification attacks like sinkhole and black hole severely affected packet efficiency and lowered throughput to unacceptable ranges.

Detection and removal of co-operative black hole and Grayhole attacks in MANETs was proposed by Singh Bindra, et al., [19], where author proposed a mechanism to detect and remove black hole and Grayhole attacks. The solution proposed tackling such attacks by an EDRI Table at nodes in addition to AODV protocol routing table. The mechanism could detect a malicious node and maintained a history of a node's previous malicious instances to account for Gray behaviour. Refresh packet, renew packet, BHID packet, further request and further reply packets were used along with existing packets (RREQ and RREP). The technique found a chain of cooperating malicious nodes dropping a major fraction of packets.

Secure route discovery to prevent black hole attacks on AODV-based MANETs proposed by Tan and Kim [20] suggested a mechanism which provided secure route discovery needing both source and destination nodes to verify RREQ and RREP message sequence numbers based on defined thresholds before establishing a connection with destination nodes to send data. Simulation results using Network Simulator 2 showed improvement in packet delivery ratio for three different environments using this, compared to standard AODV protocol.

A mechanism to detect cooperative black hole attack in MANET was proposed Sen, et al., [21] where a defence mechanism was presented against coordinated attacks by multiple black hole nodes in MANETs. Simulation on proposed scheme produced results demonstrating effectiveness of the mechanism in attack detection while maintaining a reasonable network throughput.

A trust based approach for AODV protocol to mitigate black hole attack in MANET was proposed by Thachil and Shet [22], in which nodes monitored neighbouring nodes and calculated trust value on neighbouring nodes dynamically. If a monitored node's trust value was below a predefined threshold, then monitoring node assumed it as malicious and avoided it from route path. Experiments revealed that the new scheme secures AODV MANET routing protocol by mitigating/avoiding black hole nodes.

Prevention of black hole attack in MANET was proposed by Tamilselvan and Sankaranarayanan [23]. AODV protocol security was compromised by black hole attack where a malicious node advertised itself as having shortest path to node whose packets it wanted to intercept. To reduce probability it was proposed to wait and check replies from neighbouring nodes to find safe routes. Computer simulation using glomosim showed that the protocol showed improved performance than conventional AODV in black holes with minimal additional delay and overhead.

Malicious nodes deliberately disrupt routing protocol operations. Performance of a defenceless AODV was evaluated by Abdallah, et al., [24] when many network's nodes misbehaved. Ns-2 simulated various routing disruption attack's scenarios. Performance impact on defenceless AODV was evaluated and compared to performance of regular AODV. Results indicated that malicious nodes presence was a major problem for defenceless AODV protocol.

3. METHODOLOGY

This study evaluated impact of malicious node attack (black hole attack) on AODV routing in MANET. The experiment consists of 25 nodes distributed over 2 square kilometres.

3.1 Throughput

It is a network dimensional parameter which gives a fraction of channel capacity for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

transmission selects a destination when simulation starts i.e., information whether data packets were delivered to destinations correctly.

Mathematically, it is defined as:

Throughput= N/1000 (1)

where N is number of bits received successfully by destinations [25].

3.2 Routing Overhead

Nodes often change location within a network in wireless Ad-hoc networks. So, some stale routes are generated in routing table leading to unnecessary routing overhead. Generally it is packets number generated by routing protocol during simulation which is defined as [26]:

$$Routing\ overhead = \sum_{t}^{n} OVERHEAD \quad (2)$$

where overhead i is control packet number generated by node i. Generation of an important overhead decreases protocol performance.

3.3 Cache

A cache scheme is characterized by following set of design choices which specify cache management regarding space (cache structure) and time (when to read/add/delete cache entry):

- store policy, rules to decide cached information structure,
- read policy, rules to decide when to read (use) an entry from cache,
- writing policy, rules to decide when to write an entry into cache,
- Deletion policy, rules to decide when to remove an entry from cache [27].

4. RESULTS AND DISCUSSION

In this study the impact of malicious node attack (black hole attack) on AODV routing in MANET is evaluated. The experimental setup consists of 25 nodes distributed over two square kilometres. AODV routing protocol is used. Three experiments were conducted, the first without malicious nodes and the next two with 10% and 20% of the nodes being malicious respectively. The results are as tabulated from figure 3-5.

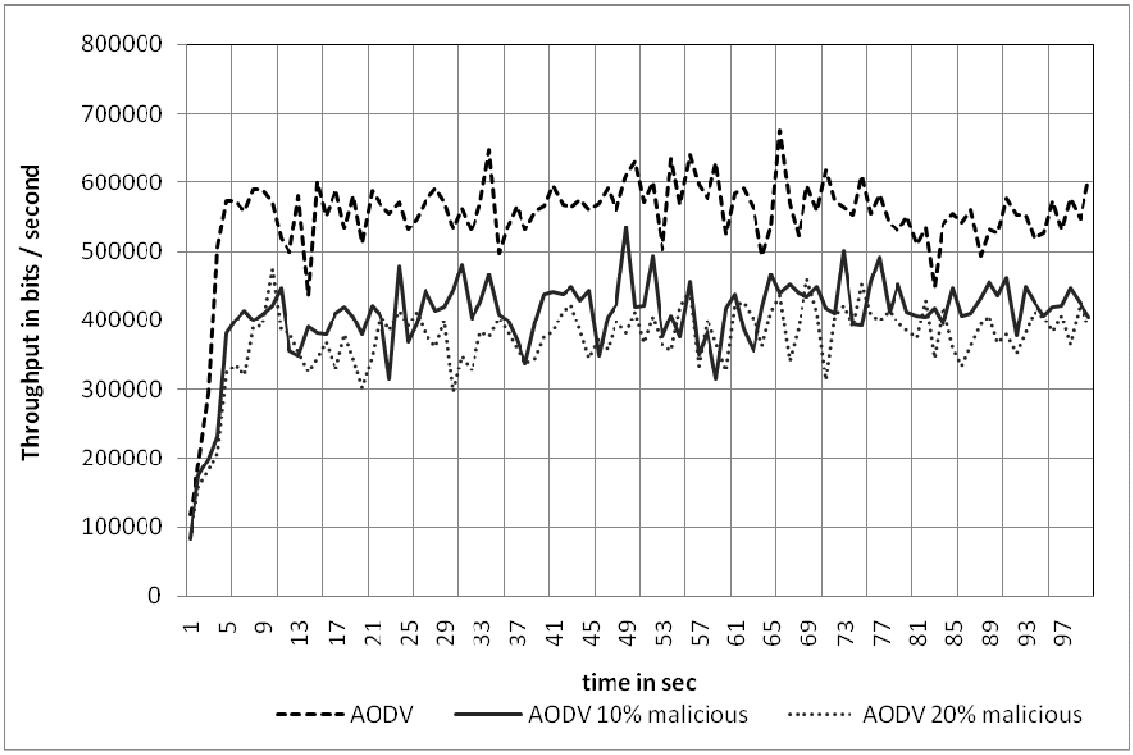

Figure 3: Throughput

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From figure 3 it is defined that the AODV without malicious has throughput degradation of 26.12% and 32.43% compared to 10% malicious and 20% malicious AODV respectively.

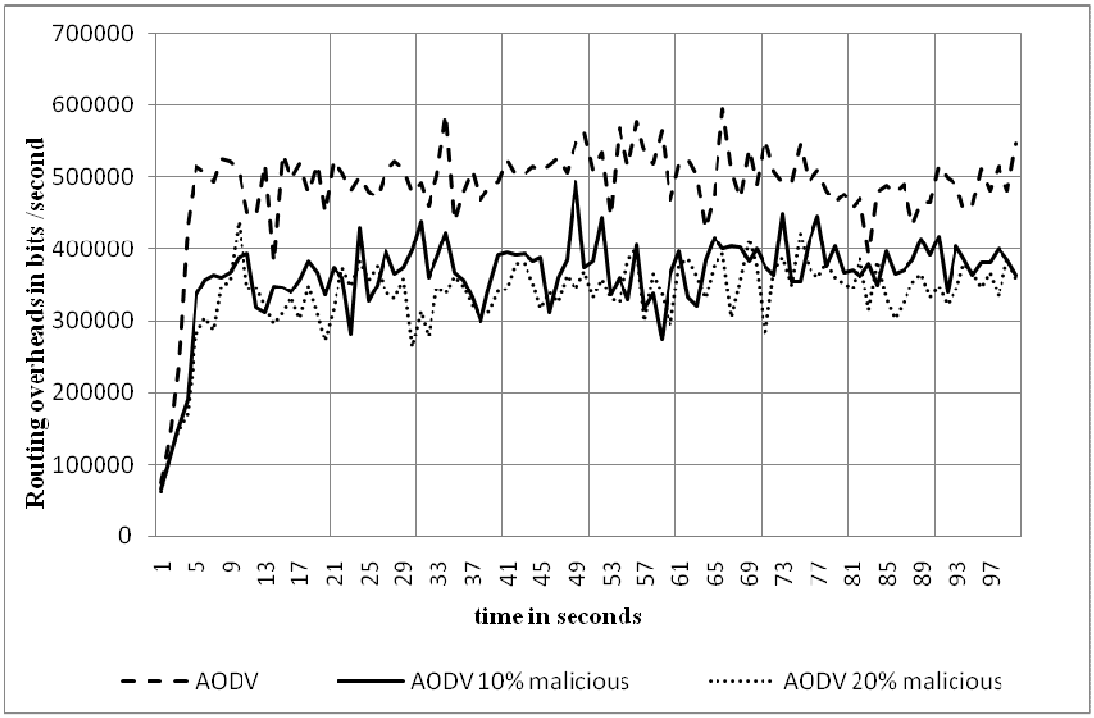

Figure 4: Routing Overhead

From figure 4 it is defined that the AODV without malicious has routing overhead degradation of 25.64% and 30.93% compared to 10% malicious and 20% malicious AODV respectively.

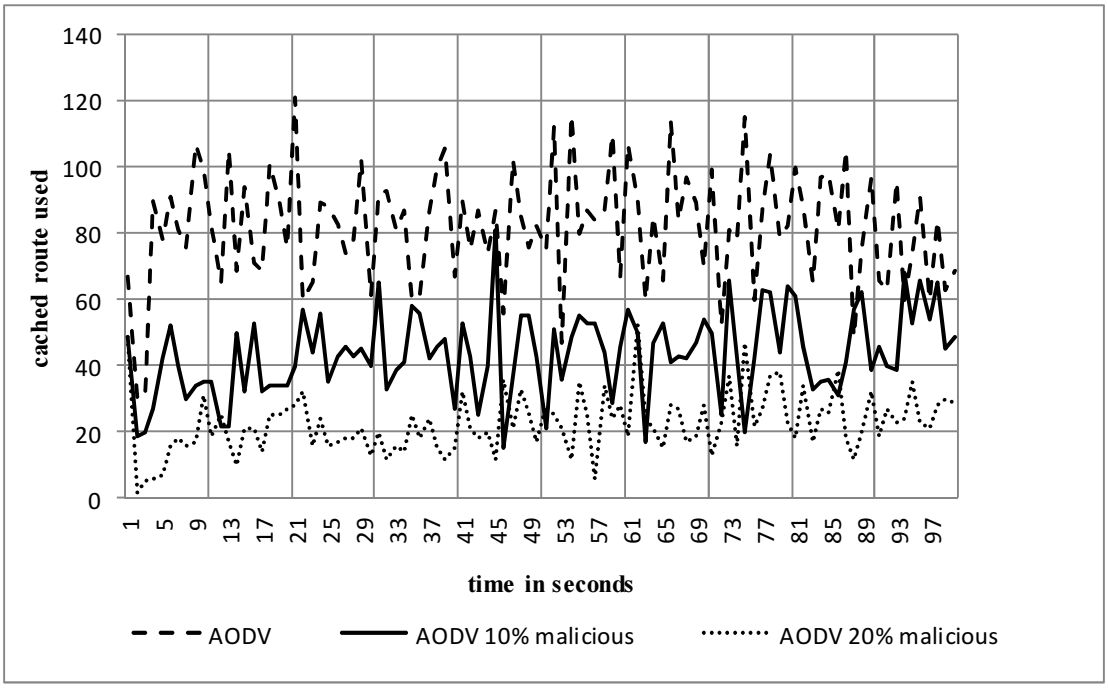

Figure 5: Cache Route

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

From figure 5 it is defined that the AODV without malicious has Cache route degradation of 46.5 % and 72.46% compared to 10% malicious and 20% malicious respectively.

5. CONCLUSION

MANET networks are presented dynamically and self-organized in temporary topologies. Internal attacks are very severe as malicious insider nodes already belong to network as authorized parties and hence are protected by network security. This study evaluates impact of malicious node attack (black hole attack) on MANET AODV routing. Experiment consists of 25 nodes distributed over 2 square kilometres. AODV routing protocol is used. Three experiments were conducted, the first without malicious nodes and the next two with 10% and 20% of nodes being malicious. The results show that AODV without malicious nodes has throughput degradation of 26.12% and 32.43%, routing overhead degradation of 25.64% and 30.93%, Cache route degradation of 46.5 % and 72.46% compared to 10% malicious nodes and 20% malicious nodes in AODV respectively.

REFRENCES

[1] DonatasSumyla 2006 'Mobile Ad-hoc Networks'

[2] Du, X., & Zhao, Z. (2010). A Group Key Agree Management Scheme for MANET. International Journal of Nonlinear Science, 10(1), 77-81.

[3] Vimala, N., &Balasubramaniam, D. R. (2010). Distributed Key Management Scheme for Mobile Ad-Hoc Network-A Survey. Global Journal of Computer Science and Technology, 10(3)

[4] Singh, H., & Singh, M. Securing MANETs Routing Protocol under Black Hole Attack

[5] Marina, M. K., & Das, S. R. (2002). Ad hoc on-demand multipath distance vector routing. ACM SIGMOBILE Mobile Computing and Communications Review, 6(3), 92-93.

[6] Moravejosharieh, A., Modares, H., Salleh, R., &Mostajeran, E. Performance Analysis of AODV, AOMDV, DSR, DSDV Routing Protocols in Vehicular Ad Hoc Network. Research Journal of Recent Sciences ISSN, 2277, 2502

[7] Rai, A. K., Tewari, R. R., &Upadhyay, S. K. (2010). Different types of attacks on integrated MANET-Internet communication. International Journal of Computer Science and Security, 4(3), 265-274.

[8] Nandy, R., & Roy, D. B. (2011). Study of Various Attacks in MANET and Elaborative Discussion of Rushing Attack on DSR with clustering scheme. Int. J. Advanced Networking and Applications, 3(01), 1035-1043.

[9] Goyal, P., Parmar, V., & Rishi, R. (2011). Manet: vulnerabilities, challenges, attacks, application. IJCEM International Journal of Computational Engineering & Management, 11, 32-37.

[10] Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., &Nemoto, Y. (2007). Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. IJ Network Security, 5(3), 338-346.

[11] Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97). ACM.

[12] Ghonge, M., &Nimbhorkar, S. U. (2012). Simulation of AODV under Blackhole Attack in MANET. International Journal, 2(2).

[13] Barati, M., Atefi, K., Khosravi, F., &Daftari, Y. A. (2012, June). Performance evaluation of energy consumption for AODV and DSR routing protocols in MANET. In Computer & Information Science (ICCIS), 2012 International Conference on(Vol. 2, pp. 636-642). IEEE.

[14] Singh, P. K., & Sharma, G. (2012, June). 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 (pp. 902-906). IEEE.

[15] Mou, Z., &Meng, X. (2011, November). A modified AODV routing protocol based on route stability in MANET. In Wireless, Mobile & Multimedia Networks (ICWMMN 2011), 4th IET International Conference on (pp. 63-67). IET.

[16] Medadian, M., Mebadi, A., &Shahri, E. (2009, December). Combat with Black Hole attack in AODV routing protocol. In Communications (MICC), 2009 IEEE 9th Malaysia International Conference on (pp. 530-535). IEEE.

[17] Bala, A., Bansal, M., & Singh, J. (2009, December). Performance analysis of MANET under blackhole attack. In Networks and Communications, 2009. NETCOM'09. First

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

International Conference on (pp. 141-145). IEEE.

[18] Ehsan, H., & Khan, F. A. (2012, June). Malicious AODV: Implementation and Analysis of Routing Attacks in MANETs. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on (pp. 1181-1187). IEEE.

[19] Singh Bindra, G., Kapoor, A., Narang, A., & Agrawal, A. (2012, September). Detection and removal of co-operative blackhole and grayhole attacks in MANETs. In System Engineering and Technology (ICSET), 2012 International Conference on (pp. 1-5). IEEE.

[20] Tan, S., & Kim, K. (2013, October). Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In ICT Convergence (ICTC), 2013 International Conference on (pp. 1027-1032). IEEE.

[21] Sen, J., Koilakonda, S., &Ukil, A. (2011, January). A mechanism for detection of cooperative black hole attack in mobile ad hoc networks. In Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on (pp. 338-343). IEEE.

[22] Thachil, F., &Shet, K. C. (2012, September). A trust based approach for AODV protocol to mitigate black hole attack in MANET. In Computing Sciences (ICCS), 2012 International Conference on (pp. 281-285). IEEE.

[23] Tamilselvan, L., &Sankaranarayanan, V. (2008). Prevention of co-operative black hole attack in MANET. Journal of networks, 3(5), 13-20.

[24] Abdallah, A.M.; Nassef, L.; Saroit, I.A., "Analysis of a defenseless ad hoc on demand Distance Vector routing protocol under routing disruption attacks," Informatics and Systems (INFOS), 2010 The 7th International Conference on , vol., no., pp.1,5, 28-30 March 2010

[25] Malany, A. B., Dhulipala, V. S., &Chandrasekaran, R. M. (2009). Throughput and Delay Comparison of MANET Routing Protocols. Int. J. Open Problems Compt. Math, 2(3), 462-468.

[26] Yadav, A., & Joshi, P. (2012). Performance of Flat Routing Protocols in MANET. International Journal of Electronics and Computer Science Engineering (IJECSE, ISSN: 2277-1956), 1(04), 2035-2041.

[27] Beraldi, R., &Baldoni, R. (2003). A caching scheme for routing in mobile ad hoc networks and its application to ZRP. Computers, IEEE Transactions on,52(8), 1051-1062.