*Wireless Sensor Network*, 2013, 5, 76-83
http://dx.doi.org/10.4236/wsn.2013.54010 Published Online April 2013 (http://www.scirp.org/journal/wsn)

# A Proposal for Mitigating Multiple Black-Hole Attack in Wireless Mesh Networks

**Om Shree, Francis J. Ogwu**
Computer Science Department, University of Botswana, Gaborone, Botswana
Email: Shree.om@mopipi.ub.bw, ogwufj@mopipi.ub.bw

Received February 4, 2013; revised March 5, 2013; accepted March 19, 2013

Copyright © 2013 Om Shree, Francis J. Ogwu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

## ABSTRACT

The Network Layer in wireless mesh networks is responsible for routing packets making it a prime target for intruders and hackers. Black-hole attack is a type of denial-of-service attack which when carried out can disrupt the services of this layer. This paper takes a look at some important detection and mitigation techniques and presents the drawbacks. After analysis of current mechanisms, the paper proposes RID-AODV, a security solution for multiple black-hole attack in wireless mesh networks. Based on the backbone of AODV, RID-AODV combines the ability of route skipping of IDSAODV and route failure correction using reverse route establishment of RAODV. The enhanced protocol RID-AODV, AODV, IDSAODV, and RAODV are implemented in a simulated environment using ns-2.35 simulator. The networks for each protocol are bombarded with up to ten black-hole nodes starting from zero. The results obtained are then analyzed and compared and a discussion is presented.

**Keywords:** Mobile Ad-Hoc Network; Wireless Mesh Networks; Ad-Hoc On-Demand Distance Vector; Black-Hole; RADOV; IDSAODV; RID-AODV

## 1. Introduction

Network security is a very important requirement in emerging networks. When developing a secure network, whether it is wired or wireless, the following five main attributes are considered authentication, confidentiality, integrity, access, and non-repudiation [1]. However, none of these properties have ever been ensured. Since the beginning of development of computer networks, malicious attacks have disrupted its functionality. [2] shows the number of incidents reported to Carnegie-Mellon Computer Emergency Response Team (CERT) from the year 1988 till 2003. At first hackers were more interested in showing their hacking skills whereas now the interest is more political, military and financial [3]. The mobile nodes which are usually cell phones, personal device assistants (PDAs) etc., have constraints due to securing WMNs are tough. The main four constraints are limited central processing unit (CPU) power, limited battery life, and limited bandwidth among nodes and node mobility which produces latency in convergence of the network. These constraints present the following security issues: signal jamming, denial-of-service, battery exhaustion, authenticity, integrity, and confidentiality [4]. These five attributes of network security along with the constraints of WMNs make it challenging to design a protocol that fulfills all the requirements. However, this is not the only attack against WMNs. Wireless Mesh networks are susceptible to routing protocol attacks and route disruption attacks. The threats that are unique to wireless mesh networks and are as follows: Worm-hole attack, Grey-hole attack, Sinkhole attack, and Sybil attack [5-7]. Black-hole attack is a type of **active** attack that exploits the RREP feature of AODV. These attacks involve some modification of the data stream or the creation of a false stream [5]. A malicious node sends RREP messages without checking its routing table for a fresh route to a destination. A RREP message from a malicious node is the first to arrive at a source node. Hence, a source node updates its routing table for the new route to the particular destination node and discards any other RREP messages from other neighboring nodes or even from the actual destination node. Once a source node saves a route, it starts sending buffered data packets to a malicious node hoping they will be forwarded to a destination node. Nevertheless, a malicious node (performing a black-hole attack) drops all data packets rather than forwarding them on. A detailed study of the various attacks can be seen in [4,5]. So far we know that black-hole attack is a

DoS attack that disrupts the services of routing layer by exploiting the route discovery process of AODV in WMNs. Over the past years, researches have been carried out to show the adverse effect of black-hole attack in WMN. In order to handle black-hole attacks, researches have been carried to develop methods or completely new protocols.

## 2. Related Works

[8] Provides a quantitative study of the performance impact of black-hole attacks in ad-hoc networks using DSR as the routing protocol. The authors used the following performance metrics to evaluate the impact of black-hole attack on network performance: System Fairness, Number of hops for received packets, Total system throughput, and Probability of interception [9]. The simulation results of impact of black-hole node on system fairness showed that with no black-hole node, the system has high fairness index. Another investigation of the effect of black-holes is carried out by [4]. Results obtained showed that almost 90% data packets were lost due to presence of black-hole nodes. [10] explored the effect of black-hole node on packet delivery ratio in an ad-hoc network. As evident from the results, there is a big drop in data packets delivery ratio with the presence of black-hole nodes. The results also show that as the number of black-hole nodes increases, the drop in data packets delivery ratio increases. The simulation results of [11], shows the effect of black-hole attack in mobile ad-hoc network. However, the results not only show the effect of the malicious node on packet delivery ratio for AODV protocol but also throughput, average end-to-end delay and jitter.

[12] not only present the effects of black-hole attack in mobile ad-hoc network using AODV routing protocol but also dynamic source routing (DSR) protocol. For the simulation, throughput was considered as the main measure. Though the simulation results showed a higher data packet loss when using DSR as compared to AODV, the dropped packet rate was still high for both protocols. DSR data loss was around 55 - 60 percent where as that of AODV was around 45 - 50 percent.

[13] presents a cross layer design to detect and mitigate multi-layer DoS attacks in WMNs.. However their simulation work was limited to injecting packet dropping attack, Grey-hole, into the network in order to measure the impact of DoS attacks [14]. Propose an attack detection system (ADS) called “Intelligent Secure Routing Model”. The ADS combines the properties of Secure Link state protocol (SLSP) and On-demand Secure Routing Protocol (OSRP) routing protocol to resist attacks such as black-hole and replay. To detect specifically black-hole attacks, the ADS employ the watchdog functionality on all the nodes participating in the ad-hoc network. [15] presents a solution to black-hole, neighbor, sequence number and packet forwarding attacks in MANETs. Their work introduces an enhanced intrusion detection system (EIDS) using AODV protocol that keeps record of all nodes present in the network and figure out malicious nodes based on trust level and complete data rate. In [16], a special case of DoS attack, known as selective forwarding (or Gray-hole) attack is investigated. The simulation results of CAD showed increased packet delivery ratio in presence of malicious node conducting selective-forwarding attack [17]. Present a solution to avoid black-hole attacks based on the authentication mechanism of Merkle tree. Their simulation results have shown positive results in the form of increased package delivery ration and low routing overhead in the presence of multiple black-hole attackers. [17,18] used a secret-key cryptographic mechanism to overcome the problem of black-hole attack in wireless ad-hoc networks. A major disadvantage of this encryption mechanism is the need to communicate the shared key. The exchange of the key between two nodes requires a high level of trust as the process of selecting, dispensing and storing keys is difficult to achieve in a trustworthy and confident modus and when you have a large number of keys they can become difficult to manage. Both [17,18] have not addressed this issue. [19] devised SAODV, an enhancement of AODV protocol which avoided black-hole attacks through the use of collective route reply table. The results show that in presence of black-hole nodes, SAODV does deliver more data messages than AODV but adds extra time to end-to-end delay. The drawback of this mechanism is the scalability. [20], also, call their method SAODV developed for protection of MANETs against black-hole attacks by using exchange of random numbers. However, [20] have not addressed the problem of path failure.

Authenticated Routing for Ad-hoc Networks, ARAN, is a protocol proposed by [12], developed to defend ad-hoc networks against modification, impersonation and fabrication exploits. However, a formal framework which can automatically verify hidden bugs in different wireless routing protocols against DoS attacks such as black-hole and wormhole has been developed by [15] using ARAN. The simulation results showed the weaknesses in ARAN whose cryptographic techniques were unsuccessful at defeating invisible node attacks, wormholes and black-hole attack. A black-hole detection scheme for Tactical MANETs using topology graphs is proposed in [21]. The developed schema is based on Optimized Link State Routing (OLSR) protocol. The method called TOGBAD consists of three parts. TOGBAD is developed for OLSR which is a pro-active routing protocol. The drawback in this mechanism is the availability of existing route in its routing table. How is it made sure that this route is still

Copyright © 2013 SciRes. 

available and the link is not broken is not explained by [22]. Another issue that needs addressing is mobility. Though the simulation results show positive results, the mechanism needs to be tested for more than single black-hole attacker [23]. Explore the use of intelligent agents called, Honeypots. The drawback of [23] is that it is developed from the point of view of static MRs of WMNs. The drawback can be found in [24]. [25] proposes a host-based intrusion detection system using anomaly detection to prevent black-hole attacks in MANETs. Hence, by identifying the anomalous activities of an adversary, it is possible to detect a possible intrusion and isolate the adversary. However, anomaly detection has at least three drawbacks as stated in [7]. We have seen that any modification to AODV increases the end-to-end delay. Also, if a solution has to be devised that would lengthen the route establishment process of a network where nodes are constantly moving in and out of transmission range, the issue of link failure must be addressed first. This led to the discovery of a reverse AODV (RAODV) routing protocol proposed by [3]. However, RAODV has been developed with the aim of solving path failure problem and has not been tested against black-hole attacks. Earlier, we showed the work of [4], IDSAODV, which uses route caching idea but does not cache all the routing replies and burden the routing table. Our proposed mechanism RID-AODV, as we have decided to call it, uses the advantages of RAODV and IDSAODV to withstand multiple black-hole attack in client-based WMNs. The architecture of RID-AODV is presented in the next section but before that we would like to show the working principle of RAODV and IDSAODV.

### 2.1. Reverse Ad-Hoc On-Demand Distance Vector (RAODV)

The proposed RAODV discovers route using reverse route discovery procedure where the destination node DN sends reverse-route request (R-RREQ) messages to its neighbors to find a valid route to the source node SN after receiving RREQ from source node. Their simulation results show that RAODV does improve the performance of AODV in metrics such as packet deliver ratio (PDR), end-to-end delay, and energy consumption. The summarized communication process of RAODV can be found in [3]. The communication from here onward is same as AODV but from DN to SN. The original SN starts message transmission whenever it receives the first R-RREQ and saving late arrived R-RREQ for times when the primary path fails.

### 2.2. IDSAODV

IDSAODV is lightweight routing protocol proposed by [4] as a solution to black-hole attack problem in MANETs. The authors manually analyzed the output file obtained from simulation and found out very soon after the first RREP from DN, a second RREP arrived at the source node. Through simulation, they found out that the first RREP was from the black-hole node and the second RREP was from DN. At this point, for future simulations, they assumed that the first RREP would always be from black-hole node and modified the AODV protocol to ignore the first RREP and send using second RREP route. A RREP caching mechanism to count the second RREP message was added to aodv.cc file in NS-2 by [4]. The simulation results of [4] exhibit that IDSAODV improved the PDR in a MANET with a single black-hole node, thus proving the successful implementation of the route caching mechanism.

## 3. Design

The method proposed in this paper is based on RAODV by [3] and IDSAODV by [4]. RID-AODV implements the caching mechanism of IDSAODV into RAODV. The figure below shows a mesh network, consisting of some normal nodes and 2 black-hole nodes that are implementing RID-AODV. **Figure 1** shows route initiation process from SN looking for route to DN whereas **Figure 2** shows vice-versa. However, both figures are part of one communication process.

Communication starts with SN sending RREQ messages to its neighboring nodes in range to look for a route to DN because of absence of an active route in its routing table. The neighboring nodes, referred to as INs, record the address of SN, and check their routing table for an active route to DN. The IN forwards the RREQ to its neighboring nodes in range in the absence of an active route to the DN. If black-hole node, BN, receives RREQ, it sends a RREP message without checking for active routes in its routing table confirming of a fresh enough

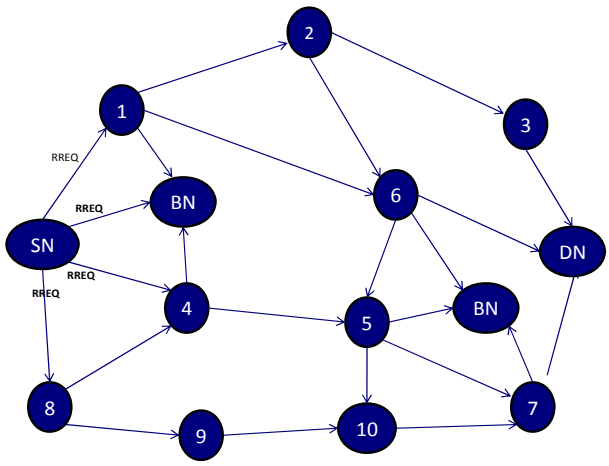


**Figure 1. RREQ process from SN to DN.**

Copyright © 2013 SciRes. 

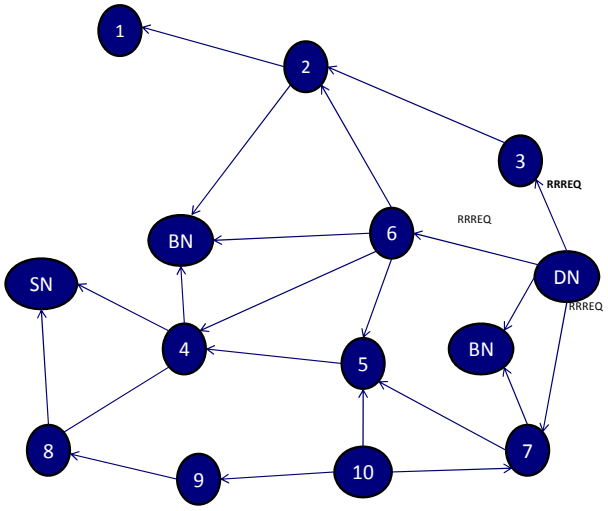


**Figure 2. R-RREQ process from DN to SN.**

routes to DN. Unlike AODV, in RID-AODV, no action is taken by the SN upon reception of RREP message from BN because it is waiting to receive R-RREQ message. Hence the RREP message is discarded. Since the RREQ is broadcasted throughout the network, an IN may receive copies of RREQ with the same broadcast id and source address. In such a case, the IN checks the routing table for redundancy and drops the RREQ message if a similar broadcast id and source address already exist in the routing table. As we can see in **Figure 1**, nodes 4-7 receive more than one RREQ messages. When the first RREQ message is received by the DN, instead of unicasting RREP back to SN, it generates R-RREQ message and broadcasts it to neighboring nodes within range to find SN. This is a similar route request process as that of SN but with DN sending route request message to establish a route to SN as shown in **Figure 2**. When BN receives R-RREQ, posing as a legitimate node, immediately sends a RREP message to the node it received R-RREQ from. This is where the route caching mechanism comes in to effect. The RREP from BN is cached in the routing table of the legitimate node. However, there are no data messages to be sent so the path building to SN continues through other INs. The BN keeps waiting on data messages. So at this point the black-hole attacker finds out that a modified protocol is in work because the R-RREQ contains the DN ip address and sequence number which are also part of RREP message. We assume that the black-hole attacker starts sending R-RREQ message to SN. The SN adds the first R-RREQ message in the routing table but does not forward data packets assuming the first reply are from BN. The SN waits for the arrival of second R-RREQ. After the routing table updates process, SN starts transmission of data packets along the second route in the routing table.

If we look at **Figures 1** and **2**, we see that at the time when SN initiates communication, there is possibility of a route SN > 1 > 2 > 3 > DN besides other routes. However, by the time the RREQ message arrives at DN and it broadcasts R-RREQ messages, node 1 has moved out of transmission range due to which a reverse path along this route could not be established. In AODV, this could lead to packet loss and overhead as SN will wait on RREP from node 1. Since RID-AODV is modified version of RAODV; it establishes a reverse route and overcomes this scenario of path failure. The method proposed in this paper was simulated in a personal computer with an Intel Pentium 4, 3.0 GHz microprocessor and 3 gigabytes (GB) of random access memory. The operating system is Redhat Fedora 17.0. The experiments are implemented and run in the network simulator ns-2. The experiments use the Carnegie Mellon University AODV package, which comes along the ns-2 bundle. The implementation modifies the AODV source code to add the defense system features. The "setdest" application of ns-2.35 is used to generate random node positions, their moving speed, and moving directions. Simulation has been carried out for surface sizes of 750 × 750 meters and 1500 × 1500 meters. Node group (NG) of 20 and 30 nodes is simulated within 750 × 750 meter surface space and NG of 40 and 50 nodes within 1500 × 1500 meter surface space. Each NG is simulated with black-hole nodes ranging from 0 up to 10. Each simulation is run for 500 seconds and stops at 490 seconds so that enough time is given to fully terminate all communications.

## 4. Results

The results of AODV, RID-AODV, IDSAODV, RAODV for the following scenarios: average packet delivery ratio (APDR) under normal operation, and 2, 4, 6, 8, and 10 black-hole nodes (BN) and average routing overhead (ARO) under normal operation, and 2, 4, 6, 8, and 10 black-hole nodes (BN). The results are presented for 20, 30, 40, and 50 node capacity networks. This detailed results obtained for the experiments which consists of total control packets sent and received, total data packets sent and received, PDR, and RO as presented.

### 4.1. APDR vs. BN for AODV, RID-AODV, IDSAODV, and RAODV

The APDR of a 20 node network for the following scenarios: Normal operation and black-hole attack with increasing number of malicious nodes are shown in the **Figure 3**. The rate of normal AODV is represented by red line, RID-AODV using blue, IDSAODV using green and RAODV using purple lines. This color scheme is maintained for all the other scenarios as well.

The rates at the beginning of experiments with no BN present in the network for AODV and RID-AODV in

Copyright © 2013 SciRes. 

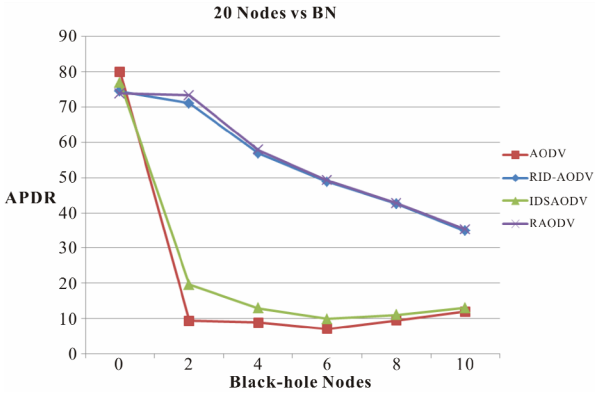


**Figure 3. Average packet delivery percentage rate vs. black-hole nodes for 20 nodes.**

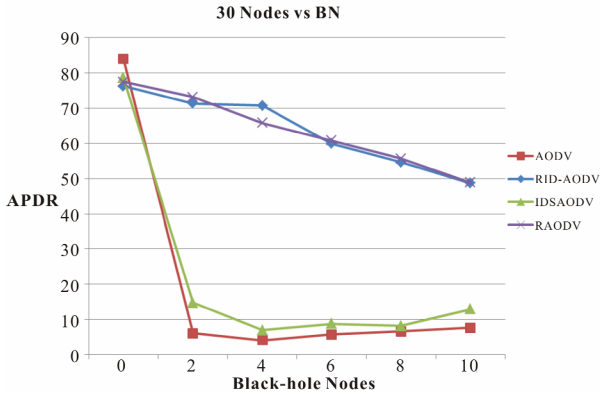


**Figure 4. Average packet delivery percentage rate vs. black-hole nodes for 30 nodes.**

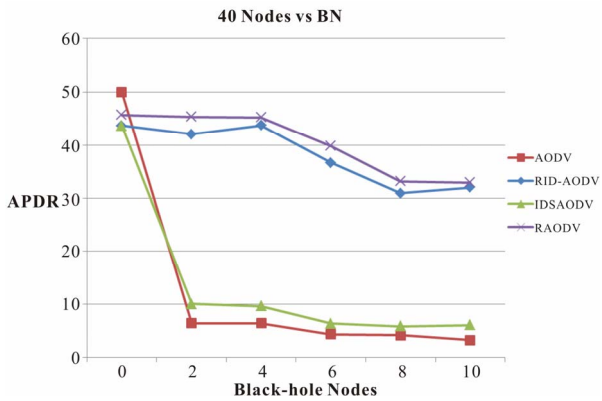


**Figure 5. Average packet delivery percentage rate vs. black-hole nodes for 40 nodes.**

**Figure 3** are at 80% and 74% respectively. As BN are introduced in the network, we notice a sharp drop in the APDR of AODV. From 80% under normal operation, the APDR of AODV drops approximately by 88% with 2 BN in the network, by 89% with 4 BN, by 91% with 6 BN, by 88% with 8 BN and by 85% with 10 BN. From 74%, the APDR of RID-AODV dips by approximately 5% with 2 BN, 23% with 4 BN, 34% with 6 BN, 43% with 8 BN and 53% with 10 BN. The APDR of a 30 node network for the following scenarios: Normal operation and black-hole attack with increasing number of malicious nodes are shown in **Figure 4**.

The rates at the beginning of experiments with no BN present in the network for AODV and RID-AODV in figure 4 are at 84% and 76% respectively. As BN are introduced in the network, we notice a sharp drop in the APDR of AODV. From 84% under normal operation, the APDR of AODV drops approximately by 93% with 2 BN in the network, by 95% with 4 BN, by 93% with 6 BN, with 92% with 8 BN and by 91% with 10 BN. From 76%, the APDR of RID-AODV dips by approximately 6% with 2 BN, 7% with 4 BN, 21% with 6 BN, 28% with 8 BN and 36% with 10 BN. The APDR of a 40 node network for the following scenarios: normal operation, and black-hole attack with increasing number of malicious nodes is shown in **Figure 5**. However from this point the experiments are carried out for surface space of 1500 × 1500 meters. Every other parameter remains the same.

The rates at the beginning of experiments with no BN present in the network for AODV and RID-AODV in **Figure 5** are at 50% and 44% respectively. As BN are introduced in the network, we notice a sharp drop in the APDR of AODV. From 50% under normal operation, the APDR of AODV drops approximately by 87% with 2 and 4 BN in the network, by 91% with 6 BN, by 92% with 8 BN and by 93% with 10 BN. From 44%, the APDR of RID-AODV dips by approximately 4% with 2 BN, 16% with 6 BN, 29% with 8 BN and 27% with 10 BN. With 4 BN, experiments showed an increase in APDR by 0.1% which is possibly due to the node positioning of the black-hole nodes. As we know, APDR is calculation of PDR of 5 simulations. The APDR of a 50 node network for the following scenarios: Normal operation and black-hole attack with increasing number of malicious nodes are shown in **Figure 6**.

The rates at the beginning of experiments with no BN present in the network for AODV and RID-AODV in **Figure 6** are at 58% and 44% respectively. As BN are introduced in the network, we notice a sharp drop in the APDR of AODV. From 58% under normal operation, the APDR of AODV drops approximately by 91% with 2 BN in the network, by 93% with 4 BN, by 94% with 6 BN, with 96% with 8 BN and by 93% with 10 BN. From 44%, the APDR of RID-AODV dips by approximately 12% with 2 BN, 8% with 4 BN, 9% with 6 BN, 20% with 8 BN and 16% with 10 BN.

## 4.2. ARO vs. BN

The normalized average routing overhead (ARO) of RID-AODV over AODV for 20 nodes with increasing number of BN is presented in **Figure 7**. The ARO of normal AODV is represented by red line, RID-AODV using

Copyright © 2013 SciRes. 

blue, IDSAODV using green and RAODV using purple lines. This color scheme is maintained for all the other scenarios as well. When the network is under black-hole attack, the new protocol's retransmission attempts of control packets increase the network workload. The normalized average routing overhead (ARO) of RID-AODV over AODV for 30 nodes with increasing number of BN is presented in **Figure 8**. When the network is under black-hole attack, the new protocol's retransmission attempts of control packets increase the network workload. The normalized average routing overhead (ARO) of RID-AODV over AODV for 40 nodes with increasing number of BN is presented in **Figure 9**.

When the network is under black-hole attack, the new protocol's retransmission attempts of control packets increase the network workload. The normalized average routing overhead (ARO) of RID-AODV over AODV for 50 nodes with increasing number of BN is presented in **Figure 10**.

When the network is under black-hole attack, the new protocol's retransmission attempts of control packets increase the network workload.

## 5. Discussion and Conclusions

The paper proposes a modified version of AODV called

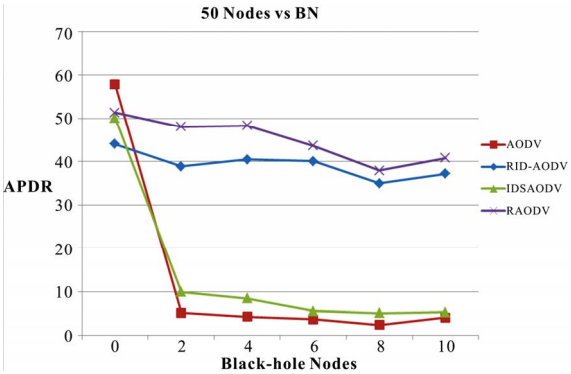


**Figure 6. Average packet delivery percentage rate vs. black-hole nodes for 50 nodes.**

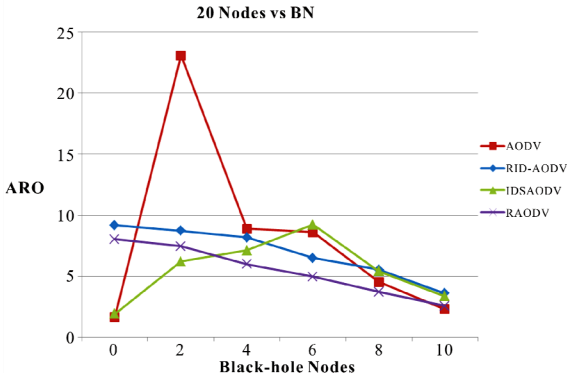


**Figure 7. Average routing overhead vs. black-hole nodes for 20 nodes.**

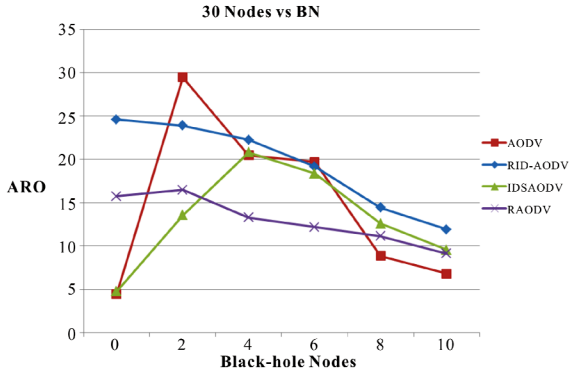


**Figure 8. Average routing overhead vs. Black-hole nodes for 30 nodes.**

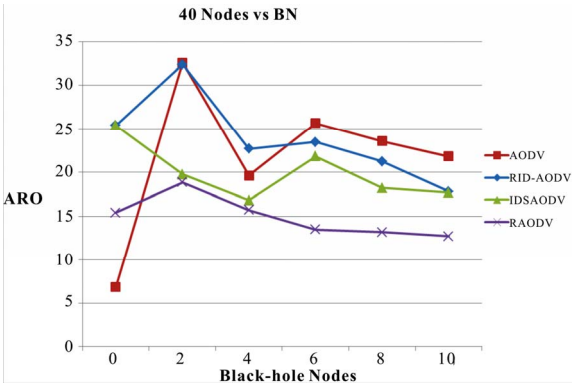


**Figure 9. Average routing overhead vs. black-hole nodes for 40 nodes.**

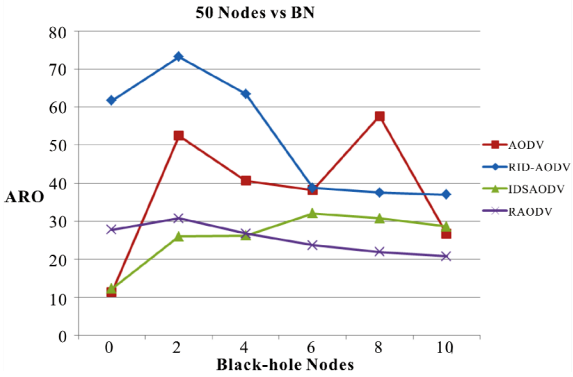


**Figure 10. Average routing overhead vs. black-hole nodes for 50 nodes.**

RID-AODV, which is a combination of reverse routing and route caching technique, to reduce the negative effects of black-hole attack. RID-AODV routing messages use standard AODV messages and data packets for communication between network nodes, hence, no system-wide upgrade or modification is needed. By caching the reply from black-hole node during forward and reverse route request, the network gains a capacity to bypass the attacking nodes and reduce the damage to the network, hence increasing packet delivery ratio. However, it is a more secure protocol than RAODV because

Copyright © 2013 SciRes. 

when the black-hole attacker learns of the operation of RAODV, it will also start sending R-RREQ messages. RAODV has no protection for this threat. However, RID-AODV will cache the first R-RREQ message which is assumed to be from the black-hole attacker hence reducing the risk of black-hole attack success.

The experiment results show that it is very easy to modify the AODV protocol and deploy black-hole attack resulting in tremendous damage to the network. Results of RID-AODV on the other hand show a better network packet delivery rate proving that it is able to withstand the attack. However, RID-AODV does burden the network with increased overhead due to increased transmission rate of control messages. From the ARO results we conclude that the increase in number of control messages transmission also increases the rate of successful data message transmission because the higher number of control messages transmitted raises the chances of more routes being discovered. Thus, there is always a positive result of RID-AODV in a multiple black-hole attack scenario than AODV.

## REFERENCES


[1] W. Stallings, "Network Security Essentials: Applications and Standards," 2nd Edition, Prentice Hall, Upper Saddle River, 2003.

[2] CERT Statistics (Historical). http://www.cert.org/historical/

[3] C. Kim, E. Talipov and B. Ahn, "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks," *Proceeding from EUC*'06: *The* 2006 *International Conference on Emerging Directions in Embedded and Ubiquitous Computing*, Seoul, 1-4 August 2006, pp. 522-531.

[4] S. Dokurer, Y. M. Erten and E. A. Can, "Performance Analysis of Ad-Hoc Networks under Black Hole Attacks," *Proceeding from SECON*'07: *IEEE Southeast Conference*, Richmond, 22-25 March 2007, pp. 148-153.

[5] M. Imani, M. E. Rajabi, M. Taheri and M. Naderi, "Vulnerabilities in Network Layer at Wireless Mesh Network (WMNs)," *Proceeding from ICENT*'10: 2010 *International Conference on Educational and Network Technology*, Qinhuangdao, 25-27 June 2010, pp. 487-492. doi:10.1109/ICENT.2010.5532257

[6] F. Nait-Abdesselam, B. Bensaou and T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad-Hoc Networks," *IEEE Communication Magazine*, Vol. 46, No. 4, 2008, pp. 127-133. doi:10.1109/MCOM.2008.4481351

[7] V. Zhang, J. Zheng and H. Hu, "Security in Wireless Mesh Networks," Auerbach Publications Taylor & Francis Group, London, 2009.

[8] I. Aad, P. J. Hubaux and W. E. Knightly, "Impact of Denial-of-Service Attacks on Ad-Hoc Networks," *IEEE-ACM Transactions on Networking*, Vol. 16, No. 4, 2008, pp. 791-802. doi:10.1109/TNET.2007.904002

[9] R. Jain, "The Art of Computer System Performance Analysis," John Wiley and Sons, Inc., Hoboken, 1991.

[10] E. Cayirci and C. Rong, "Security in Wireless Ad Hoc and Sensor Networks," John Wiley & Sons Publications, 1st Edition, Hoboken, 2009.

[11] CERT Statistics (Historical). http://www.cert.org/historical/

[12] D. Mishra, K. Y. Jain and S. Agarwal, "Behavior Analysis of Malicious Node in the Different Routing Algorithms in Mobile Ad Hoc Network (MANET)," *Proceeding from ACT*'09: *Advances in Computing, Control and Telecommunication Technologies*, Trivandrum, 28-29 December 2009, pp. 621-623.

[13] D. Bansal and S. Soffat, "Use of Cross Layer Interactions for Denial of Service Attacks in WMN," *Proceeding from NETWORKS*'10: *The* 14*th international Telecommunications, Network Strategy and Planning Symposium*, Warsaw, 27-30 September 2010, pp. 1-6.

[14] R. Rangara, R. Jaipuria, G. Yenugwar and P. Jawandhiya, "Intelligent Secure Routing Model for MANET," *Proceeding from ICCSIT*'10: *3*rd *International Conference on Computer Science and Information Technology*, Chengdu, 2010, p. 452.

[15] S. Umang, B. V. R. Reddy and M. N. Hoda, "Enhanced Intrusion Detection System for Malicious Node Detection in Ad Hoc Routing Protocols Using Minimal Energy Consumption," *IET Communications*, Vol. 4, No. 17, 2010, pp. 2084-2094. doi:10.1049/iet-com.2009.0616

[16] M. D. Shila, Y. Cheng and T. Anjali, "Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs," *IEEE Transactions on Wireless Communication*, Vol. 9, No. 5, 2010, pp. 1661-1675. doi:10.1109/TWC.2010.05.090700

[17] S. Hashmi and J. Brooke, "Towards Sybil Resistant Authentication in Mobile Ad Hoc Networks," *Proceeding from SECURWARE*'10: 4*th International Conference on Emerging Security Information Systems and Technologies*, Venice, 18-28 July 2010, pp. 17-24.

[18] L. Hong, W. Chen, L. Gao, G. Zhang and C. Fu, "Grey Theory Based Reputation System for Secure Neighbor Discovery in Wireless Ad Hoc Networks," *Proceeding from ICFCC*'10: 2*nd International Conference on Future Computer and Communication*, Wuhan, 21-24 May 2010, pp. V2-V749.

[19] L. Tamilselvan and V. Sankarnarayanan, "Prevention of Blackhole Attack in MANET," *Proceeding from AUS-WIRELESS*'07: 2*nd International Conference on Wireless Broadband and Ultraband Communications*, Sydney, 27-30 August 2007, p. 21.

[20] S. Lu, L. Li, K. Lam and L. Jiya, "SAODV: A MANET Routing Protocol That Can Withstand Black Hole Attack," *Proceeding from CIS*'06: *International Conference on Computational Intelligence and Security*, Beijing, 11-14 December 2009, pp. 421-425.

[21] E. Gerhards-Padilla, N. Aschenbruck, P. Martini, M. Jahnke and J. Tolle, "Detecting Black Hole Attacks in Tactical MANETs Using Topology Graphs," *Proceeding from LCN*'07: 32*nd IEEE Conference on Local Computer Networks*, Dublin, 15-18 October 2007, pp. 1043-1052.


Copyright © 2013 SciRes. 

[22] A. Prathapani, L. Santhanam and P. D. Agarwal, "Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks," *Proceeding from MASS*'09: *IEEE* 6*th International Conference on Mobile Adhoc and Sensor Systems*, Macau, 12-15 October 2009, pp. 753-758.

[23] L. Coleman, M. Martin, T. Meurer and K. Plauche, "Honeypot Technology," 2009. http://students.kennesaw.edu/~lec6557/Formal%20Report.htm

[24] F. Y. Alem and C. Z. Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection," *Proceeding from ICFCC*'10: *International Conference on Future Computer and Communication*, Wuhan, 21-24 May 2010, pp. V3-V672.

[25] T. Krone, "Hacking Motives [PDF Document]". http://www.aic.gov.au/publications/current%20series/htcb/1-20/htcb006.aspx

Copyright © 2013 SciRes. 