Resisting blackhole attacks on MANETs

Abdelshafy, M. & King, P. J. B.

Original citation & hyperlink:
Abdelshafy, M & King, PJB 2016, Resisting blackhole attacks on MANETs. in 2016 13th IEEE Annual Consumer Communications & Networking Conference (CCNC) . IEEE, pp. 1048 - 1053, 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, United States, 9/01/16.
https://dx.doi.org/10.1109/CCNC.2016.7444935

DOI 10.1109/CCNC.2016.7444935
ISSN 2331-9860

Publisher: IEEE

Resisting Blackhole Attacks on MANETs

Mohamed A. Abdelshafy
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
Email: ma814@hw.ac.uk

Peter J. B. King
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
Email: P.J.B.King@hw.ac.uk

***Abstract*—MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the routing protocol. AODV is a reactive MANET routing protocol that is vulnerable to a dramatic collapse of network performance in the presence of blackhole attack. The paper introduces a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal protocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior. We present a Blackhole Resisting Mechanism (BRM) to resist such attacks that can be incorporated into any reactive routing protocol. It does not require expensive cryptography or authentication mechanisms, but relies on locally applied timers and thresholds to classify nodes as malicious. No modifications to the packet formats are needed, so the overhead is a small amount of calculation at nodes, and no extra communication. Using NS2 simulation, we compare the performance of networks using AODV under blackhole attacks with and without our mechanism to SAODV, showing that it significantly reduces the effect of a blackhole attack.**

***Keywords*—MANET, Routing, AODV, Security, Attack, Blackhole, Self-Protocol Trustiness**

I. Introduction

A Mobile Ad Hoc Network (MANET) is a decentralized infrastructureless network in which nodes cooperate to forward data from a source to a destination. Each node in a MANET acts both as a router and as a host. Several routing protocols have been designed for MANETs [3] to optimize network routing performance. The major issues involved in designing a routing protocol for MANET are node mobility, bandwidth constrained and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology [1].

MANET routing protocols can be classified as proactive or reactive routing protocols. In proactive (table-driven) routing protocols, each node maintains one or more tables containing routing information to every other node in the network. While in reactive (on-demand) routing protocols, routes are created whenever a source requires to send data to a destination node which means that these protocols are initiated by a source on-demand. In this paper, we focus on the AODV protocol [12] which is one of the extensively studied reactive protocols, considered by the IETF for standardization.

Conventional MANET routing protocols assume that all nodes cooperate without maliciously disrupting the operation of the protocol and do not provide defense against malicious attackers. However, the existence of malicious nodes cannot be ignored in computer networks, especially in MANETs because of the wireless nature of the network. MANET inherits security threats that are faced in wired as well as wireless networks and also introduces security attacks unique to itself [6] due its characteristics. Nodes in MANET have limited computation and power capabilities that make the network more vulnerable to Denial of Service (DoS) attacks. It is difficult to implement cryptography and key management algorithms which need substantial computations like public key algorithms. Node mobility introduces also a difficulty of distinguishing between stale routes and fake routes. A malicious node can attack the network layer in MANET either by not forwarding packets or by changing some parameters of routing messages such as sequence number and IP addresses, sending fake messages several times and sending fake routing information to disrupt routing operations. A large number of attacks on MANET [15] are known and many solutions have been proposed to resist them. Simulation studies have shown the impact of such attacks and the effectiveness of proposed defence mechanisms [11] [17].

Security mechanisms can be added to existing routing protocols to resist attacks. Cryptographic techniques are used to ensure the authenticity and integrity of routing messages [5]. A major concern is the trade off between security and performance, given the limited resources available at many MANET nodes. Both symmetric and asymmetric cryptography have been used as well as hash chaining. Examples of these security enhanced protocols are Authenticated Routing for Ad-hoc Networks (ARAN) [13], Secure Link State Routing Protocol (SLSP) [10], and Secure Ad-hoc On-demand Distance Vector routing (SAODV) [18]. In addition to the power and computation cost of using cryptographic techniques, the performance of secured mechanism is worse than non-secured in the presence of some attacks [2]. Securing the routing messages does not guarantee the detection of these malicious nodes.

We introduce a new Blackhole Resisting Mechanism (BRM) that can be used for all on-demand routing protocols. Each node in this mechanism is responsible for monitoring the behaviour of its neighbors to detect malicious nodes and exclude them. We incorporate our proposed mechanism into AODV as an example of its use with on-demand routing protocols. This paper demonstrates a significant improvement in performance when using our mechanism.

The rest of the paper is organized as follows. In Section II, AODV and its behavior under blackhole attack is presented. Section III presents the related work. In Section IV, our proposed mechanism to detect the blackhole attack is intro-

duced. In Section V, the simulation approach and parameters is presented. In Section VI, simulation results are given. In Section VII, conclusions are drawn.

II. AODV under Blackhole Attack

AODV [12] is a reactive routing protocol. It uses destination sequence numbers to ensure the freshness of routes and guarantee loop freedom. To find a path to a destination, a node broadcasts a route request (RREQ) packet to its neighbors using a new sequence number. Each node that receives the broadcast sets up a reverse route towards the originator of the RREQ unless it has a fresher one. When the intended destination or an intermediate node that has a fresh route to the destination receives the RREQ, it unicasts a reply by sending a route reply (RREP) packet along the reverse path established at intermediate nodes during the route discovery process. Then the source node starts sending data packets to the destination node through the neighboring node that first responded with an RREP. When an intermediate node along the route moves, its upstream neighbor will notice route breakage due to the movement and propagate a route error (RERR) packet to each of its active upstream neighbors. Routing information is stored only in the source node, the destination node, and the intermediate nodes along the active route which deal with data transmission. This scenario decreases the memory overhead, minimizes the use of network resources, and runs well in high mobility situations.

In a blackhole attack [14], a malicious node absorbs the network traffic and drops all packets. Once a malicious node receives a RREQ packet from any other node, it immediately sends a false RREP; without checking its routing table; with a high sequence number and hop count equals 2 (i.e. one hop from the source and the destination) to spoof its neighbours that it has the best route to the destination. The malicious node reply will be received by the source node before any other replies. The high sequence number will cause the route including the malicious node to be selected. When the data packets routed by the source node reach the blackhole node, it drops the packets rather than forwarding them to the destination node. A malicious node initiating a blackhole attack generates a fake RREP for each RREQ it receives to incorporate itself in a route, therefore all packets are sent to a point where they are not forwarded anywhere which is a form of a denial of service (DoS) attack. A node has no way of detecting whether the neighbor that sent the RREP is malicious or not. A blackhole attack has a dramatic impact on the network performance [2].

III. Related Work

Since the on-demand routing protocols have been introduced, many significant algorithms have been proposed to secure MANET against blackhole attack. Some of these solutions use various cryptographic techniques to secure the routing packets. While these solutions introduce high immunity to the blackhole attack, network nodes suffer from the high computations required which does not suit the characteristics of MANET. Other solutions suggest modification to the routing protocols by adding some packets, modifying the existing packets or changing the procedure of these protocols.

Such solutions focus their suggested mechanisms on two characteristics of the RREP received from a blackhole node; the first is that this reply is usually received before any other replies as a result of blackhole node not needing to check its route table. The second is that this fake RREP usually contains a much higher sequence number relative to the RREQ because the blackhole node tries to convince its neighbours it has a fresh route to destination node. All these solutions make assumptions about blackhole behavior and cannot guarantee that excluded nodes are genuine blackholes. In this section we introduce some of the existing algorithms used to avoid the blackhole attack.

SAODV [18] is an enhancement of AODV routing protocol to fulfil security feature. The protocol operates mainly by appending an extension message to each AODV message. The extension messages include a digital signature of the AODV packet using the private key of the original sender of the routing message and a hash value of the hop count. SAODV uses asymmetric cryptography to authenticate all non-mutable fields of routing messages as well as hash chain to authenticate the hop count (the only mutable) field. Since all fields except the hop count of routing messages are non-mutable they can be authenticated by verifying the signature using the public key of the message originator. So, when a routing message is received by a node, the node verifies the signature of the received packet. If the signature is verified, the node computes the hash value of the hop count; if the routing message is RREQ or RREP; and compares it with the corresponding value in the SAODV extension. If they match, the routing message is valid and will be forwarded with an incremented hop count and a new hash value or if the destination has been reached generate the RREP.

S. Lee [7] proposed a solution that modified the AODV routing protocol by introducing two new packets; the route confirmation request (CREQ) and route confirmation reply (CREP). An intermediate node has to send CREQ to its next-hop node toward the destination node in addition to RREP to the source node. Upon receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has a route, it sends the CREP to the source. After receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are coordinated, the source node judges that the route is appropriate. One drawback of this method is that it cannot avoid the cooperative blackhole attack if two consecutive nodes work together as the first node asked its next hop node to send CREP to the source.

L. Tamilselvan [16] proposed a solution that designed upon a Fidelity Table in which each participating node is assigned with a fidelity level that determines the node reliability. A default fidelity level is assigned to each node and this level is updated based on the behavior of the node. When a source node receives RREP, it waits to receive further route replies from its neighboring nodes and then selects a neighbor node with a highest fidelity level to forward data to the destination node. A destination node acknowledges receiving the data by sending ACK. Updating the fidelity level of node relies on trusted participation of the node in the network. The source node increments or decrements the fidelity level of the forwarding node upon receiving or missing the ACK respectively. Node is eliminated from the network if its fidelity level reaches zero and marked as a malicious node. The main

drawback of this solution is the high end-to-end delay specially when the malicious node is far away from the source node.

N. Mistry [8] introduced a solution that depends on analysing all received RREP. As source node receives first RREP, it waits MOS_WAIT_TIME seconds to receive multiple RREPs. During this time, the source node saves all the received RREPs in a table. Thereafter, the source node makes an analysis of all stored RREPs from the table, and rejects any having very high destination sequence number and considering its sender as malicious. The remaining entries in the table are arranged according to their destination sequence number and the node with the highest number is selected. This technique also records the identity of suspected malicious nodes to discard any upcoming control packets received and/or forwarded from/to that node and a routing entry for that node will not be maintained. The algorithm introduces high end-to-end delay as nodes have to wait for multiple RREPs.

N. Choudhary [4] introduced a solution that based on sensing the wireless channel. This approach assigns a max_trust value to all its neighboring nodes. A node will not do any further communication with a neighbor whose trust value is less than min_trust value. When a source node receives a RREP message, it updates its routing table, starts transmitting the data packets and inserts a unique sequence number with each transmitted data packet. When a node forwards a data packet, it sets a timer and listens to the wireless channel in promiscuous mode to ensure that this packet is forwarded by a next hop neighbor. When the timer expires without hearing the retransmission of this packet, the node reduces the trust value for its next hop node. Trust value information is updated and disseminated to other neighboring nodes. If the trust value of a node decreases below min_trust value, it will be isolated by all the nodes in the network.

IV. BRM-AODV Protocol

BRM-AODV is designed to mitigate the effect of the blackhole attack on the performance of AODV protocol by fast detection of blackhole neighbors. The mechanism introduces a new concept of Self-Protocol Trustiness (SPT) which clarifies that the detection of a malicious intruder is accomplished by complying with the normal protocol behavior and lures the malicious node to give an implicit avowal of its malicious behavior. The mechanism does not use cryptographic techniques which conserves the power and computation resources. Furthermore, the mechanism neither adds new routing packets nor modifies the existing ones. We introduce a small modification to the original AODV by storing the last three per hop times for a RREP received for a destination. The per hop time is calculated as the latency between sending a RREQ and receiving its corresponding RREP divided by the hop count value included in the RREP.

Each node in the network has to monitor the performance of its neighbors to detect if any misbehave as blackholes. BRM-AODV has no thresholds, such as RREP rate, that may be disseminated to malicious nodes and introduce a way for these malicious nodes to work under these thresholds. Instead of this, a node periodically sends a fake RREQ from a non-existant source node to a non-existant destination node. Only a malicious node will respond to this fake RREQ. If a node

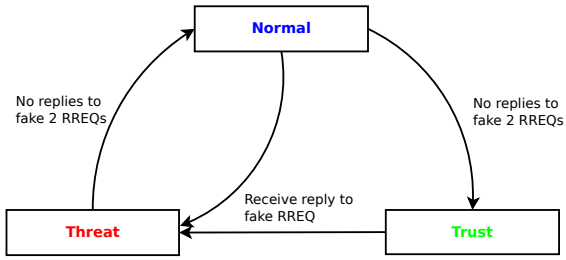

Fig. 1. FSM of Node Trust Level

receives a RREP to its fake RREQ from one of its neighbors, the node becomes sure that this neighbor is a blackhole node. The algorithm introduces two different variables; trust level and confidence level. Once a node joins a network, it sets its trust level to normal and it updates this trust level to either trust or threat upon reception of replies to its fake RREQs. Figure 1 shows the operation of trust levels as a finite state machine. A confidence level is a value assigned to each neighbor by a node. It is initialized to MAX_CONFIDENCE and decremented whenever that neighbor replies to a fake RREQ. Table 1 shows the values of parameters that were used in our simulations. A node implementing the Blackhole Resisting Mechanism behaves as follows:

- A node periodically sends a fake RREQ from a random non-existing source node to a random non-existing destination node. The node stores these fake source and destination addresses in a trustiness table for later examination. The node also sets an expiry time for this entry to avoid the table inflation.
- A node initialises its trust level to normal and sends fake RREQs at random time intervals between MIN_NORMAL and MAX_NORMAL. If a node receives a reply to one of its fake RREQs, it changes its trust level to threat and sends fake RREQs at random time intervals between MIN_THREAT and MAX_THREAT. The node upgrades it trust level from threat to normal or from normal to trust if it sends two successive fake RREQs without receiving a reply during RREP_VALIDATE period. A node that set its trust level to trust sends fake RREQs at random time intervals between MIN_TRUST and MAX_TRUST. The MIN_NORMAL and MAX_NORMAL interval, and their equivalents for thread and trust levels, are chosen to give a greater rate of testing of a neighbor when it is less trusted. These three intervals introduce more difficulty for a malicious node looking to subvert our proposed mechanism by tracing fake RREQs rate and differentiating it among valid RREQs.
- To solve the trade-off between flooding the network with fake RREQs which increases the routing overhead and detection of validity of the RREQ by a malicious node, it is suggested that the TTL value of this fake RREQ is set to a random number between TTL_MIN and TTL_MAX. We suggest values of 1 and 4 for these limits. This limit as well convinces any malicious neighbor that the node which sent the RREQ to it is a forwarding node and it did not originate it for testing the malicious trustiness.

TABLE I. BRM-AODV PARAMETERS

MAX_CONFIDENCE	7
RREP_VALIDATE	5 s
TRAFFIC_TIME	10 s
MIN_THREAT	5 s
MAX_THREAT	30 s
MIN_NORMAL	30 s
MAX_NORMAL	90 s
MIN_TRUST	90 s
MAX_TRUST	150 s

- If a RREP is received from a neighbor for this fake RREQ and both fake source and destination addresses are found in the trustiness table and either the source address of this reply or the number of hops identifies that RREP originator is the neighbor (i.e. number of hops is 2), the node identifies the originator as a blackhole node by setting its black_list value to 1 and removes it from its routing table and drops any upcoming RREPs received from this neighbor without processing. This check forces a malicious node looking to launch a blackhole attack to impersonate as other node has originated this RREP and guarantees that malicious neighbor will stop claiming it has best route to a destination by setting its reply hop count to 2.
- If a RREP is received from a neighbor for this fake RREQ and both fake source and destination addresses are found in the trustiness table and the source address of this reply is not identical to the forwarding neighbor and the number of hops is greater than 2 which implies that this neighbor may be a victim used to forward this RREP or a malicious node that tries to subvert our algorithm. The node drops this RREP and computes the latency between sending the corresponding RREQ and this RREP and then divided this value by the hop count received in this RREP to calculate the per hop time for the received RREP. Then, the node compares this value to the average hop time of all routes included in the routing table taking into account that each route has three previously stored per hop time values. If the per hop time of the received RREP is less than the average per hop time of all stored routes in the routing table, the node decrements this neighbor confidence level for each received RREP of a fake RREQ. The node clarifies that this neighbor trying to use the blackhole feature of replying without checking its RREP which is a reason of receiving the RREP faster than those from other normal nodes.
- If a neighbor confidence level becomes zero, the node identifies this neighbor as a blackhole node or a colluding node. If this neighbor is not malicious, it might be a colluding node as it should detect its malicious neighbor that uses it as victim node to forward RREPs. Decrementing a confidence level for a neighbor ensures that the node gives plenty of time for it neighbor to discover its malicious neighbor which is implicating it in misbehaving. So, the node sets the neighbor's black_list value to 1 and removes it from its routing table and ignores any RREPs received from this neighbor.

V. SIMULATION APPROACH

NS-2 simulator [9] is used to simulate AODV, SAODV and our new BRM-AODV routing protocols under blackhole attack. The parameters used are shown in Table 2. Node mobility was modelled with the random waypoint method. In all cases, the 90% confidence interval was small compared with the values being reported. While we examined our proposed mechanism on both UDP and TCP traffic and the mechanism succeeded in detecting blackhole neighbors and enhancing the network performance for both, this paper is focused on the results of the proposed mechanism on the TCP traffic only. We examined our proposed mechanism for different number of nodes (25, 50, 75 and 100) and different node speeds (0, 5, 10, 15, 20 and 25 m/s). The highest negative impact of malicious nodes usually appears on static networks and this effect decreases as nodes mobility increases [1], so we report here the case of static networks. Finally, we compare the performance of networks using AODV under blackhole attacks with and without our mechanism. We also compare the results to SAODV as it is a well-known fully secured MANET reactive protocol chosen by IETF for standardization.

Our blackhole attack model assumes that once a malicious node receives a RREQ packet from any other node, it immediately constructs a fake RREP that includes a randomly generated hop count between 2 and 4 to spoof other nodes about best route (i.e. 1 to 3 hop counts only from the RREQ source). The attacker assigns the destination sequence number value of this fake RREP as equal to the received one in the RREQ plus randomly generated number between 10 and 30 to spoof other nodes about the freshness of this RREP. Then, the attacker unicasts this fake RREP toward the RREQ source.

TABLE II. SIMULATION PARAMETERS

Simulation Time	600 s
Simulation Area	1000 m x 1000 m
Number of Nodes	100
Number of Connections	150
Number of Malicious Nodes	0 - 10
Node Speed	0 - 25 m/s
Pause Time	10 s
Traffic Type	TCP

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.
Throughput: The number of data bits delivered to the application layer of destination node in unit time measured in bps.
End-to-End Delay (EED): The average time taken for a packet to be transmitted across the network from source to destination.
Routing Overhead: The number of routing packets for route discovery and route maintenance required to deliver the data packets from sources to destinations.

VI. SIMULATION RESULTS

The effect of blackhole attack on the packet delivery ratio is shown in Figure 2. While the blackhole attack has severe impact on the PDR of AODV specially for large number of malicious nodes, BRM-AODV achieves an approximately

constant PDF regardless the number of malicious nodes. On the other hand, while SAODV has a constant PDR regardless the number of malicious nodes such as our algorithm; our algorithm achieves a better PDR value than SAODV.

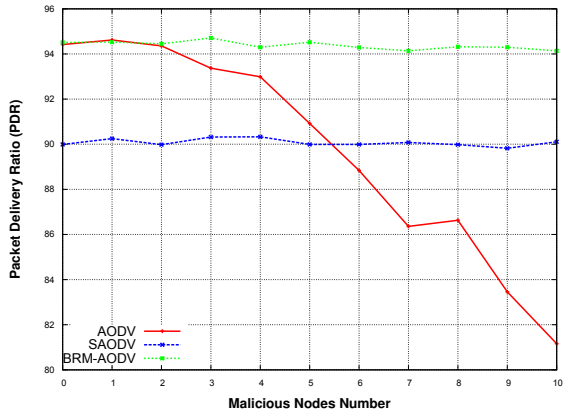

Fig. 2. Packet Delivery Ratio

Figure 3 shows the effect of blackhole attack on the network throughput. Throughput of BRM-AODV is better than AODV by approximately 25% for each malicious node and the enhancement becomes huge for high malicious number. While the throughput of AODV dramatically decreases as the number of malicious nodes increases, BRM-AODV slightly decreases for the high number of malicious nodes. The mechanism introduces a negligible degradation of throughput in the absence of malicious nodes. In addition, our algorithm achieves a better throughput than SAODV by approximately 100%.

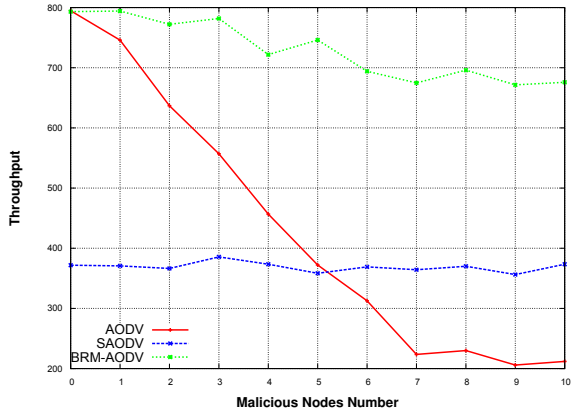

Fig. 3. Network Throughput

The effect of blackhole attack on the end-end-delay is shown in Figure 4. An expected logical result has to be increasing the end-end-delay as the number of malicious nodes increases and this delay should be at least equal the delay of the network in the absence of malicious nodes. On the other hand, the results show that the delay of the original AODV protocol is reduced as the number of malicious nodes increases which is slightly paradoxical as the attack improves the delay. This is a misleading result because the delay is only measured on packets that reach their destinations and since the blackhole nodes drop all received data routed through them, the number of packets that will be considered in calculating the delay decreases as the number of malicious nodes increases. So, the routes that avoid blackhole nodes suffer less competition, and hence reduced delay. As our proposed mechanism succeeded in receiving many data packets relative to AODV, the number of packets that will be considered in calculating the delay increases approaching the logical level that is the delay of network in the absence of malicious nodes. While delay does not affect too much in SAODV regardless the number of malicious nodes, our algorithm decreases it slightly compared to SAODV.

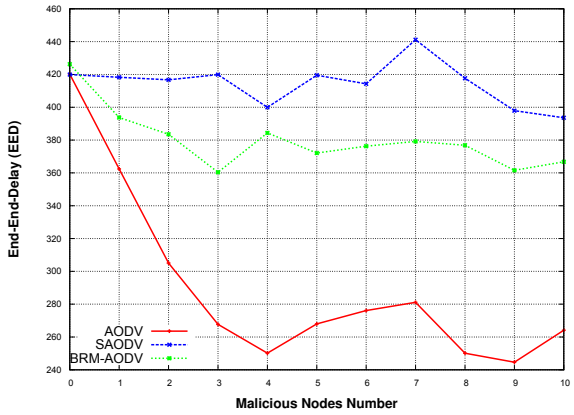

Fig. 4. End-to-End Delay

Figure 5 shows the effect of blackhole attack on the routing overhead. The result shows that the routing overhead of AODV decreases as a result of malicious nodes increases which is slightly confusing as the blackhole attack improves the routing overhead. This is because the blackhole nodes stop rebroadcasting the RREQ which decreases the number of RREQ packets, one of the factors used to measure the routing overhead. The routing overhead of BRM-AODV slowly decreases as the number of malicious nodes increases and approaches to the routing overhead value of network in the absence of malicious nodes as a result of continuous detection of blackhole nodes. On the other hand, while routing overhead in SAODV is constant regardless the number of malicious nodes, our algorithm reduces the routing overhead compared to SAODV. Although the figure shows that the number of routing packets of our algorithm is less than its value of SAODV by approximately 5%, this enhancement increases up to approximately 400% if we consider the difference between AODV and SAODV packet sizes.

Our simulation shows that regardless of the number of nodes and the number of malicious nodes in the network, a node will detect a malicious neighbor within a short time. Figure 6 shows the proportion of malicious nodes that have been detected as time progresses. For clarity, we only show the results for 1, 4, 7 and 10 malicious nodes. The figure shows that as the simulation time increases the mechanism succeeded in detecting and excluding malicious nodes up to more than

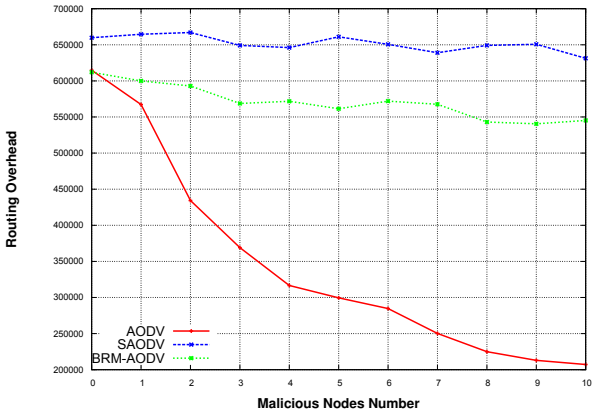

Fig. 5. Routing Overhead

75% of blackhole neighbors if the time is 600 seconds. The mechanism succeeded in excluding high percentage of the blackhole neighbors after 120 seconds from the beginning of the simulation because most of the genuine RREQs and RREPs are sent during this period. The mechanism continues to exclude more blackhole neighbors after that with low rate as a result of small number of RREQs and blackhole replies to these requests.

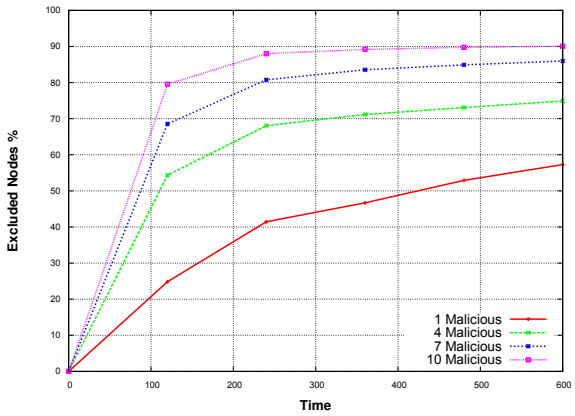

Fig. 6. Malicious Exclusion Percentage

VII. Conclusion

The paper introduced a new concept of Self-Protocol Trustiness (SPT) in which detecting a malicious intruder is accomplished by complying with the normal protocol behavior and luring the malicious node to give an implicit avowal of its malicious behavior. We introduced a new Blackhole Resisting Mechanism (BRM) that can be incorporated into any reactive routing protocol in MANET. The proposed mechanism did not use cryptographic techniques which conserves the power and computation resources. Furthermore, the mechanism did not require any additional packets and hence does not incur any additional overhead. As an example, we incorporated our Blackhole Resisting Mechanism into AODV to study the performance of the network under the presence and absence of the mechanism. Simulation results showed that BRM-AODV gives a huge improvement of the network performance in all network metrics over both AODV and SAODV. The proposed mechanism succeeded in detecting blackhole nodes within a short time regardless the number of malicious nodes and the time they are participating in the network. Future work includes extending this idea to other reactive protocols, and confirming its general applicability.

References

[1] M. A. Abdelshafy and P. J. King. Analysis of security attacks on AODV routing. In *8th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 290–295, London, UK, Dec 2013.

[2] M. A. Abdelshafy and P. J. King. AODV & SAODV under attack:performance comparison. In *ADHOC-NOW 2014, LNCS 8487*, pages 318–331, Benidorm, Spain, Jun 2014.

[3] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Bölöni, and D. Turgut. Routing protocols in ad hoc networks: a survey. *Computer Networks*, 55(13):3032–3080, September 2011.

[4] N. Choudhary and L. Tharani. Preventing black hole attack in AODV using timer-based detection mechanism. In *International Conference on Signal Processing And Communication Engineering Systems (SPACES)*, pages 1–4, Jan 2015.

[5] P. Joshi. Security issues in routing protocols in MANETs at network layer. *Procedia Computer Science*, 3:954–960, 2011.

[6] A. Kumar. Security attacks in MANET - a review. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, RTMC(11), May 2012.

[7] S. Lee, B. Han, and M. Shin. Robust routing in wireless ad hoc networks. In *International Conference on Parallel Processing Workshops*, pages 73–78, 2002.

[8] N. Mistry, D. C. Jinwala, and M. Zaveri. Improving AODV protocol against blackhole attacks. In *International MultiConference of Engineers and Computer Scientists (IMECS)*, pages 1–5, Hong Kong, China, March 2010.

[9] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.

[10] P. Papadimitratos and Z. J. Haas. Secure link state routing for mobile ad hoc networks. In *Symposium on Applications and the Internet Workshops*, pages 379–383. IEEE Computer Society, 2003.

[11] M. Patel and S. Sharma. Detection of malicious attack in MANET a behavioral approach. In *IEEE 3rd International on Advance Computing Conference (IACC)*, pages 388–393, 2013.

[12] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1997.

[13] K. Sanzgiri and et al. Authenticated routing for ad hoc networks. *IEEE Journal On Selected Areas In Communications*, 23:598–610, 2005.

[14] N. Sharma and A. Sharma. The black-hole node attack in MANET. In *Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies*, ACCT '12, pages 546–550, Washington, DC, USA, 2012. IEEE Computer Society.

[15] M. Singh, A. Singh, R. Tanwar, and R. Chauhan. Security attacks in mobile adhoc networks. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, RTMC(11), May 2012.

[16] L. Tamilselvan and V. Sankaranarayanan. Prevention of blackhole attack in MANET. In *2nd International Conference on Wireless Broadband and Ultra Wideband Communications*, pages 21–21, Aug 2007.

[17] G. Usha and S. Bose. Impact of gray hole attack on adhoc networks. In *International Conference on Information Communication and Embedded Systems (ICICES)*, pages 404–409, 2013.

[18] M. G. Zapata. Secure ad hoc on-demand distance vector routing. *SIGMOBILE Mob. Comput. Commun. Rev.*, 6(3):106–107, jun 2002.