[[1]](#footnote-1)

Improvements on a Path-Based Adaptive Detection Algorithm for Black Holes in MANETs

Eileen Hindmon, Charisse Scott, and Christopher Zingraf

*Abstract*— Mobile Ad-Hoc Networks have increased with the growing use of mobile wireless devices. The topologies of these networks are unique due to the fact the networks must be dynamic in nature and are constrained to their environment. The open medium of the nodes requires distributed cooperation. Each node must act as a host and a router communicating without a traditional network infrastructure or centralized administration. The most obvious security vulnerability within a mobile ad hoc network can be found within the routing protocol. This paper focuses on an attack delivered at such level; the attack, or problem, is coined black hole.

*Index Terms*—**Black hole, MANET, mobile ad hoc network, secure routing, security**.

# INTRODUCTION

A

 MOBILE AD-HOC NETWORK (MANET) is a collection of wireless mobile nodes that communicate without a pre-defined network infrastructure or centralized administration. The mobile ad-hoc network offers unrestricted mobility and connectivity through each node acting as a host and router. In addition to mobility and connectivity, the MANET must also provide the CIA of security to its services: confidentiality, integrity, and authentication. However, this can be challenging with the dynamic nature of the topology. Since each node operates as a host and a router, this means the wireless channel is accessible to both legitimate users and malicious attackers. The topology lacks a clear line of defense between each of the nodes. Two approaches to defending the mobile ad hoc network have been researched: proactive and reactive. The proactive approach is a preventative methodology that attempts to prevent the attacker from launching attacks through various cryptology techniques. The reactive methodology seeks to detect threats and then act accordingly. Attacks on the mobile ad-hoc network can be classified into two categories, passive and active. Passive attacks are difficult to detect because they do not disrupt the flow of data; their only objective is to discover valuable data without notice. However, an active attack has very different goals. This attack focuses on modifying data, gaining authentication, or securing authorization by inserting false packets into the line of communication between the nodes. An active attack can also be divided into two additional categories: external and internal attacks. Nodes that do not belong on the network cause an external attack. A compromised or hijacked node that has already been authorized on the network defines an internal attack. Because this node has been previously authorized, this attack proposes the highest security risk.*.*

# Literature Survey

Chundong She *et al.* [1] presented a path-based algorithm (PBA) for detecting black and gray holes. They used ns2 to simulate a network and observe the effects of their algorithm on detecting black and gray holes. After testing their algorithm in the simulation, they compared the performance of theirs with another algorithm. The PBA solution proved to detect more black and gray holes than the other comparable solutions. Although the PBA solution is able to detect more black holes and provide a low false positive rate, its performance suffers under heavy load. This can cause problems as network traffic fluctuates and performance can suffer greatly under this solution and a heavy network load.

Hizbullah Khattak *et al*. [2] proposed a simple solution to avoid black holes. This solution simply discards the shortest path in favor of the second shortest path. This solution relies on a black hole’s inability to monitor the entire network. The black hole would say it is the shortest path, and thus the second path would in fact be the shortest and most secure path. This is a very effective solution to use if there are black or gray holes in the network. This solution does fall short when there is an absence of black or gray holes. By always choosing the second shortest path to the destination, transmissions would take longer to reach the destination. Combine this with multiple hops across multiple nodes and the transmission time for packets increases drastically.

 Medadian *et al.* [3] proposed a solution to minimize the effects of black holes by waiting and checking every node’s reply before making the path selection. They ran simulations on this new solution and found that it does perform better than the conventional ad hoc on-demand distance vector routing schemes. Even though it proved to be more secure, this solution suffers from a high delay. This is because the node has to wait for every response from the neighbors before making the selection. This is reasonable when there are few neighbors, but as the network grows the delay also grows.

 Deng *et al.* [4] created a protocol that solves the black hole problem by requiring the intermediate nodes to send information on the next hop in the path. This helps defend against black holes by letting the source node know whether the path is actually a valid path. The source node is given the choice to accept the path or choose a different one. This works out well, as paths are validated by all intermediate nodes, but this solution suffers from an increase in routing overhead and causes more end-to-end delay.

# Problem Statement

In this paper, we further examine the Path-Based Adaptive (PBA) method for black and gray hole detection proposed in [1]. Here, the authors propose a scheme which uses a dynamically-calculated packet-forwarding rate threshold to detect black and gray holes in the network. This method offers many resource-conservative benefits over other approaches:

* Unlike collaborative schemes, no extra control packets need to be sent.
* No encryption on control packets is required.
* Each node only need be concerned with the behavior of its immediate neighbors.

There are, however, some problems inherent in this scheme. The first problem is related to the proposed algorithm for detecting a black hole. In [1], this algorithm is described as follows:

1. For each packet that is forwarded out from a node, that packet's signature is stored in a buffer on the node.
2. The node listens to hear the packet being forwarded from the next hop. When it does, that packet's signature is removed from the buffer.
3. After a certain time interval, the node calculates the next hop node's ratio of packets overheard to total packets sent to that node.

$$R= \frac{packets overheard from next hop}{total packets forwarded to next hop}$$

The next hop is considered to be a black hole if *R* is lower than the threshold.

The problem with this scheme is that, at a high network load, the probability for false positive detection increases. That is because, under CSMA/CA protocol in 802.11 networks, packet collisions can often occur among hidden nodes. A high rate of traffic causes a higher rate of collisions, and these collisions can lead to a node's inability to overhear the forwarding of packets from its next hop nodes. Thus, even though a particular node might be “normal”, it might be detected as a black hole because its forwarding rate is lower than the threshold.

She *et al.* address this problem in their paper with dynamic threshold calculation, based on the *current probabilities* of a collision occurring and a packet being forwarded. These values are recalculated on regular time intervals to adapt the detection threshold to the current network performance.

The authors found the dynamic threshold method to be successful in lowering the rate of false positive detection, especially at high levels of traffic (CBR stream rate). However, using this method, the detection rate becomes much less competitive at CBR stream rates higher than 1.5 KB/s.

This happens because, as traffic rate rises, collision rate rises. As collision rate rises, the value of the dynamic threshold also rises to compensate. Thus, the detection algorithm becomes more permissive, and fewer black/gray holes are detected. The authors present this as an unsolved problem in their approach.

We believe that the PBA scheme proposed by She *et al.* is a useful one because of its low overhead and resource conservation. It is possible that this scheme could be adapted to remove the problem described above while still maintaining the simplicity and low cost of the original scheme. One such adaptation may be to “roll over” to another detection method at high network loads. This second method should have the same qualities of low cost as PBA, but should not be reliant on network loads. The Optimal Path & Hash Based (OPH) Scheme described in [2] is one such method, because it uses a very simple algorithm: discard the first RREP message in order to select the second-shortest path to the destination [5],[2]. Our goal in this paper is to determine whether rolling over to OPH at a high network load would be an improvement over the method proposed in [1].

# Approach to Solve the Problem

In order to determine whether including OPH would be an improvement over PBA alone, we must answer the following questions:

1. We must determine the “weak point” in PBA. At what network load (CBR stream rate) does it fail? This is the point where we should switch to OPH scheme.
2. How should we measure the increase (if any) in performance that our proposed method achieves?

After establishing the answers to these questions, we should carry out a study using the ns2 network simulation program. We should replicate the simulations carried out in [1], but implementing the OPH scheme at the appropriate CBR stream rate. This way, we can be sure that any changes in performance are due to the introduction of the OPH scheme. Then, we can measure any potential increase in detection performance using the metric(s) determined in response to question (2) above.

# Results

To determine at what CBR stream rate we should try implementing the OPH scheme, we must examine the data from [1]. Figure 1 shows the difference in detection rate between using an adaptive threshold and a static threshold.

##

 Fig. 1. Detection rate vs. CBR stream rate for the adaptive threshold and static threshold solutions [1].

It can be seen that the largest disparity between the two schemes begins at 1.5 KB/s. If the OPH scheme were implemented at CBR stream rates greater than or equal to 1.5 KB/s, it could potentially narrow this disparity.

In [1], overall performance of the PBA scheme is measured using detection rate. Since there is no active detection of black/gray holes in the OPH scheme, we would need to determine another metric to use to compare our proposed method with PBA. The metrics used in [1] are as follows:

1. Overall packet delivery rate
2. Accumulated collision rate
3. Detection probability
4. False positive probability

It would be most practical to use overall packet delivery rate as our determining metric. However, this measurement is not recorded in [1] for the implementation of the dynamic threshold solution. Thus, before simulating our own proposed scheme, we would need to replicate the simulations for the dynamic threshold solution carried out in [1] to record a baseline measurement for overall packet delivery. If our proposed method is an improvement over PBA alone, it should be shown in a higher overall packet delivery rate under the same conditions.

# Conclusion

In this paper, we discussed Mobile Ad-hoc Networks and the various security risks found in them. Our main focus was on black holes and gray holes as those active attacks pose a serious threat not only to data integrity but also network performance.

We examined the Path-Based Adaptive (PBA) method to detect black and gray holes in a MANET proposed by Chundong She *et al.* in [1]. This method is more resource conscious when compared to other methods of detecting and preventing black and gray holes. The PBA method is conservative when it comes to resource use because it doesn’t need extra control packets to be sent into the network. Also, there is no need to encrypt the control packets that are sent out. To further conserve resources this method requires each node to only take into consideration the behavior of immediate neighbors.

Even with these resource saving characteristics, the PBA method does have some drawbacks. One problem is with the algorithm used to detect black holes. Because of the way networks work there can be a lot of false positives when the network is under a heavy load. This is because of collisions within the network. Under heavy load there is a higher rate of collisions causing nodes to think that the dropped packets are due to a black hole when in fact they are simply colliding with other packets in the network.

To combat this, She *et al.* propose a calculation based on current statistics about network collision rates. This calculation must happen on regular timed intervals to be effective. Although this does help lower false positives, the detection rate is affected, especially under heavy loads. This is due to the fact that at higher loads, the collision rate will be higher. To accommodate this, the threshold is adjusted. It must be more permissive to more accurately calculate, but in making it more permissive can allow more black holes to remain undetected.
 We proposed a solution to combat this heavy load problem. Our solution is to switch detection methods when the network is under a heavy load. Once the network reaches a certain load, the detection algorithm could switch over to one such as The Optimal Path and Hash Based (OPH) Scheme [2]. We wanted to determine if switching to OPH under heavy load would improve the network performance when under heavy load.

 To determine whether switching to OPH while under heavy load would improve performance over sticking to the PBA method, we needed to answer a few questions. First, we needed to find the “weak point” in PBA, that is, when to switch over to OPH. We also needed to figure out how to measure the performance increase if any exists in our proposed method. The next step in the process is actually testing the method out using the ns2 network simulation program. This way, we could see and record how our method performed in comparison to the PBA model. We determined that we would set up the network environment exactly as She *et al.* did in their simulation. This way, we could compare the results we got with their results. This would determine the effectiveness of our solution.

 The future work that must be performed is running the simulation in ns2. Once we set up the simulation environment, we could run the original simulation that She *et al.* ran to get the readings needed to compare our method to theirs. Once we run the PBA simulation and gather the results, we would be able to then run our proposed solution and compare the results.

References

1. She, Yi, Wang, Yang, “Intrusion detection for black hole and gray hole in MANETs,” *KSII Transactions on Internet and Information Systems*, vol. 7, no. 7, Jul. 2013.
2. H. Khattak, N. Nizamuddin, F. Khurshid, N. ul Amin, “Preventing black and gray hole attacks in AODV using optimal path routing and hash,” in *10th IEEE International Conference on Networking, Sensing and Control (ICNSC)*, 2013.
3. M. Medadian, M. H. Yektaie, A. M. Rahmani, “Combat with black hole attack in AODV routing protocol in MANET,” in *First Asian Himalayas International Conference*, 3-5 Nov. 2009.
4. H. Deng, W. Li, and D. P. Agrawal, "Routing security in wireless ad hoc networks," *Communications Magazine*, IEEE, vol.40, no.10, pp. 70- 75, October 2002.
5. F. Pardhi, “Detection & prevention techniques to black & gray hole attacks in MANET: a survey,” *International Journal of Advanced Research in Computer and Communication Engineering*, Vol. 2, Issue 10, October 2013.
1. Manuscript received May 4, 2014.

E. Hindmon is with the College of Science and Technology, Radford University, Radford, VA 24141 USA (e-mail: ehindmon@radford.edu).

C. Scott is with the College of Science and Technology, Radford University, Radford, VA 24141 USA (e-mail: cscott6@radford.edu).

C. Zingraf is with the College of Science and Technology, Radford University, Radford, VA 24141 USA (e-mail: czingraf@radford.edu). [↑](#footnote-ref-1)