Intrusion Detection for Black Hole and Gray Hole in MANETs

Chundong She [1], Ping Yi [2], Junfeng Wang[3], Hongshen Yang[4]
[1] School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[e-mail: shurcd@vip.sina.com]
[2] School of Information Security Engineering, Shanghai Jiao Tong University, Shanghai, 200240, China
[e-mail: pyi_edu@yahoo.com.cn]
[3] College of Computer Science, Sichuan University, Chengdu 610064, P.R. China
[e-mail: wangjf@scu.edu.cn]
[4] Department of Electrical Engineering, Tongling University, Tongling 244000, P.R. China
[e-mail: yhs@tlu.edu.cn]
*Corresponding author: Junfeng Wang

Received October 5, 201X; revised November 10, 201X; accepted November 20, 201X; published December 25, 201X

Received March 25, 2013; revised May 30, 2013; accepted June 22, 2013; published July 30, 2013

Abstract

Black and gray hole attack is one kind of routing disturbing attacks and can bring great damage to the network. As a result, an efficient algorithm to detect black and gray attack is important. This paper demonstrate an adaptive approach to detecting black and gray hole attacks in ad hoc network based on a cross layer design. In network layer, we proposed a path-based method to overhear the next hop's action. This scheme does not send out extra control packets and saves the system resources of the detecting node. In MAC layer, a collision rate reporting system is established to estimate dynamic detecting threshold so as to lower the false positive rate under high network overload. We choose DSR protocol to test our algorithm and ns-2 as our simulation tool. Our experiment result verifies our theory: the average detection rate is above 90% and the false positive rate is below 10%. Moreover, the adaptive threshold strategy contributes to decrease the false positive rate.

Keywords: Mobile Ad Hoc Networks, Black Hole, Gray Hole, Cross Layer Design, Intrusion Detection

This work was supported by the Important National Science & Technology Specific Projects of China (2012ZX10004-901001); the National Natural Science Foundation of China (11102124), the Program for New Century Excellent Talents in University, Ministry of Education of China (NCET-10-0604), the Provincial Key Science and Technology Research and Development Program of Sichuan, China (2013SZ0002).
http://dx.doi.org/10.3837/tiis.2013.07.012

1. Introduction

Mobile Ad Hoc Networks (MANETs) [1] is one kind of new wireless network structures. Unlike traditional Wireless LAN solutions, all nodes are movable and the topology of the network is changing dynamically in an Ad Hoc Networks, which bring great challenges to the security of Ad Hoc Network. As a result, attackers can take advantage of flaws in routing protocols to carry out various attacks [2-3]. Black hole attack and gray hole attacks [4] are two class ical attacks under Ad Hoc networks, which could disturb routing protocol and bring about huge damage to the network's topology.

In this paper, we propose an innovative approach to detecting black hole and gray hole attacks by modifying the detecting threshold according to the network's overload. We manipulate a cross layer method to improve the performance of our detection. While the mechanism presented in this paper applies to any Ad Hoc protocol, we will focus our attention, without loss of generality, on DSR protocol [5] in network layer and IEEE 802.11 protocol in MAC layer.

The remainder of this paper is organized as follows: Section II presents the related researches. In Section III, a path based detecting algorithm over DSR protocol is proposed. We discussed its advantage and disadvantage. In Section IV, we present an enhanced method and explain the algorithm to estimate the detecting threshold. In Section V, some simulation results are given to characterize the performance of our proposed method. Finally, we draw our conclusions.

2. Related Work

2.1 Black and Gray Hole Attacks

Black hole attack disturbs the routing protocol by deceiving other nodes about the routing information. A black hole node works in the following scheme: once receiving RREQ and RREP messages, the attacker replies RREP messages directly and claims that it is the destination node. The source node is likely to receive a pseudo-RREP from the attacker before the real RREP returns. Under these circumstances, the source node sends data packets to the black hole instead of the destination node. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message. As for gray hole, its behavior is similar to a black hole. A gray hole does not drop all data packets but just part of packets. We define the *Gray Magnitude* as the percentage of the packets which are maliciously dropped by an attacker. For example, a gray hole is gray magnitude of 60% will drop a data packet with a probability of 60% and a classical black hole has a gray magnitude of 100%.

The black and gray hole attack will bring great harm to the performance of Ad Hoc network. In previous research, the authors have carried out experiment on black hole attacks [6]. In Section V of this paper, we first analyze the impact of gray hole under

different malicious drop rate. The malicious drop rate is defined by the ratio of dropped packet number and received packet number. Especially, the malicious drop rate of a black hole is 100%.

2.2 Detection Methods

Sun et al [7] presented a general approach for detecting the black hole attack. They devised a neighborhood-based method to detect the intruder and a routing recovery protocol to set up a correct path to the true destination. They first introduced the neighbor set of a node, which is all of the nodes that are within the radio transmission range of a node. Two types of control packets are introduced to share neighbor set between different nodes. If two neighbor sets received at the same time are different enough, it can be concluded that they are generated by two different nodes. One disadvantage of this scheme is that there must be a public key infrastructure or the detection is still vulnerable.

Patcha et al [8] proposed a collaborative method for black hole attack prevention. A watchdog method is introduced to incorporate a collaborative architecture to tackle collusion amongst nodes. In this algorithm, nodes in the network are classified into trusted, watchdog, and ordinary nodes. Every watchdog that is elected should observe its normal node neighbors to decide whether they can be treated as trusted or malicious.

Gao et al [9] proposed to use aggregate signature algorithm [10] to trace packet dropping nodes. The proposal was consisted of three related algorithms: 1) the creating proof algorithm. 2) The checkup algorithm. 3) The diagnosis algorithm. The strengths of this proposal are: 1) the reliability is satisfying, as evidence on forwarded packets is used; 2) the application scope is broad, as bi-directional communication links are not necessary; 3) the security is satisfying, as it is hard for malicious nodes to escape detection; 4) the bandwidth overhead is low, as nodes do not need to monitor each other.

Shila et al [11] presented a solution to defend selective forwarding attack (gray hole attack) in Wireless Mesh Networks [12]. The first phase of the algorithm is Counter-Threshold Based and uses the detection threshold and packet counter to identify the attacks. The second phase is Query-Based and uses acknowledgment from the intermediate nodes to localize the attacker. In the first phase, two types of packets, Control packet and Control ACK packet, are used to detect the attacker. Furthermore, they determine the appropriate value of detection threshold based on the routing metric ETX [13] to improve the performance under different network situation.

3. A Path-based Detecting Method

3.1 Detection Algorithm

Our proposal is based on a path based scheme. That is, a node does not watch every node in the neighbor, but only observes the next hop in current route path. For example, in **Fig. 1**, S is the source node; D is the destination node; and A is a black hole. Node S is sending data packets to node D through the path S, A, B, D. In our scheme, Node S only watches Node A, which is the next hop; but does not care Node 1 and Node 2.

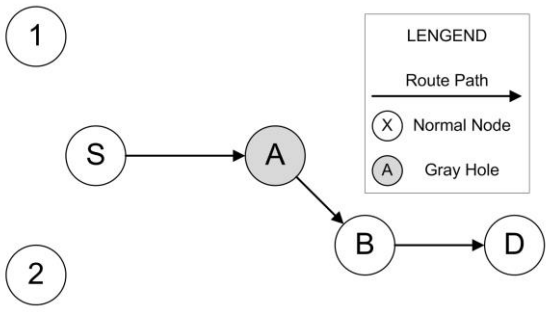

Fig. 1. A path based detection scheme

To implement the algorithm, every node should keep a FwdPktBuffer, which is a packet signature buffer. The algorithm is divided into three steps:

1) When a packet is forwarded out, its signature is added into the FwdPktBuffer and the detecting node overhears.
2) Once the action that the next hop forwards the packet is overheard, the signature will be released from the FwdPktBuffer.
3) In a fixed period of time, the detecting node should calculate the overhear rate of its next hop and compare it with a threshold. We define overhear rate in the Nth period of time as $OR(N)$.

$$OR(N) = \frac{\text{total overheard packer number}}{\text{total forwared packer number}} \tag{1}$$

If the forwarding rate is lower than the threshold, the detecting node will consider the next hop as a black or gray hole. Latter, the detecting node would avoid forwarding packets through this suspect node.

3.2 Advantage of the Algorithm

Our method has several advantages:

- In this scheme, each node only depends on itself to detect a black or gray hole. The algorithm does not send out extra control packets so that Routing Packet Overhead (the ratio of total number of routing related transmissions and the total number of packet transmissions) remains the same as the standard DSR routing protocol.
- Not like other collaborative detecting architectures, our proposal requires no encryption on the control packets to avoid further attacks on detection information sharing.
- There is no need to watch all neighbors' behavior. Only the next hop in the route path should be observed. As a result, the system performance waste on detection algorithm is lowered.

3.3 Analysis of False Positive Probability

One problem of this detection method is that it suffers from a high false positive probability under high network overload if a constant threshold is used. The cause of high false positive probability is hidden node problem in carrier-sensing multiple-access with collision avoidance (CSMA/CA) protocol. A hidden node is a node which is beyond range of a packet sender (node S in **Fig. 2**) but in the range of a packet receiver (Node A in fig 2). In fig 2, Node B does not hear the data from Node S to Node A, and it is a hidden node. When Node B transmits to node C, the transmission collides with that from Node A to node B. Therefore, the hidden nodes lead to higher collision probability.

As for path based detection, black node problem will greatly increase the false positive probability. In fig 2, Node S is source node and Node C is destination node. Packet 1 is transmitted from Node B to Node C. At the same time, Packet 2 is transmitted from Node S to Node A. Consequently, Packet 1 and Packet 2 will collide at Node A. Then Node S will retransmit Packet 2; but Packet 1 will not be sent again because Packet 1 has been received by Node C successfully. As a result, Node A misses Packet 1 and treats it being dropped by Node B deliberately. In summary, a high network overload leads to a high collision rate caused by hidden node problem, so that the probability that a detecting node fails to overhear its next hop increases accordingly. Thus, the false positive probability rises in the end.

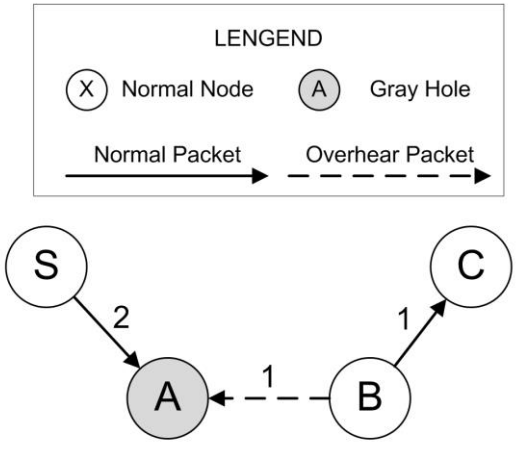

Fig. 2. A collision problem with the path based detection scheme

4. Dynamic Threshold and Adaptive Detection

4.1 MAC Layer Collision Report Mechanism

To avoid the problem caused by hidden node problem, we designed a cross-layer mechanism. Two counters, collisionPktNum and nonColPktNum, are added to standard

802.11 protocol. If a collision occurs, collisionPktNum increases 1; if a packet being received successfully, nonColPktNum increase 1. In a fixed period of time, the collision is defined as following:

$$RCN(N) = \frac{collisionPktNum}{collisionPktNum + nonColPktNum} \tag{2}$$

The collision rate is reported to network layer, and meanwhile, two counters are reset to zero.

In network layer (DSR protocol in this paper), accumulated collision rate is calculated. Let $ACR(N)$ be the accumulated collision rate in the Nth time period and $RCR(N)$ be the reported collision rate in the Nth time period. We fine $ACR(N)$ as:

$$ACR(N) = \begin{cases} 0, & for N = 0 \\ \frac{1}{2}(ACR(N) + RCR(N)), & for N \geq 1 \end{cases} \tag{3}$$

Equivalently, when $N \geq 1$:

$$ACR(N) = \sum_{i=1}^{N} (\frac{1}{2})^{N-i+1} RCR(N) \tag{4}$$

4.2 Threshold Calculation

Let $P_{collision}$ be the actual collision probability in the Nth time period; and $P_{forward}$ be the actual forward probability of a node; and $P_{overhear}$ be the probability of a node overhearing the next hop's forward action. So,

$$P_{overhear} = (1 - P_{collision}) \cdot P_{forward} \tag{5}$$

Our mechanism is able to measure $P_{overhear}$ using overhear rate, $OR(N)$, and $P_{collision}$ using accumulated collision rate $ACR(N)$. Substitute them into (5).

$$P_{forward} = \frac{OR(N)}{1 - ACR(N)} < (1 - T_f) \tag{6}$$

Let T_f be the fixed detection threshold. If a node drops packets in a probability higher than T_f, the detecting node can accuse it as a gray hole. Equivalently,

$$OR(N) < (1 - T_f) \cdot (1 - ACR(N)) \tag{7}$$

Finally, we define *dynamic detection threshold* as $T_d(N)$.

$$T_d(N) = 1 - (1 - T_f) \cdot (1 - ACR(N)) \tag{8}$$

Now, the detecting node can only accuse a gray hole, when it overhears the next hop "drops" packets in a probability higher than $T_d(N)$.

5. Simulation Environment

Our proposal is implemented in ns2 [14] and the performance is evaluated in terms of network throughput, false positive probability and false negative probability.

We use two simulations to evaluate our proposal.

5.1 A Grid Simulation Environment:

The first one is network with 1200m*1200m space and 25 fixed nodes as **Fig. 3**. Every node is settled in a fixed location. We set the maximum transmission range as 250m and the distance between two neighbors is 200m so that a node can only have 4 neighbors. The simulation span is 300 seconds. We implement this scenario to evaluate the collision rate of each node in different location under different CBR rate. The communication patterns we use are 8 constant bit rate (CBR) connections with a size of 512 byte, but the interval between two packets (CBR rate) remain variable.

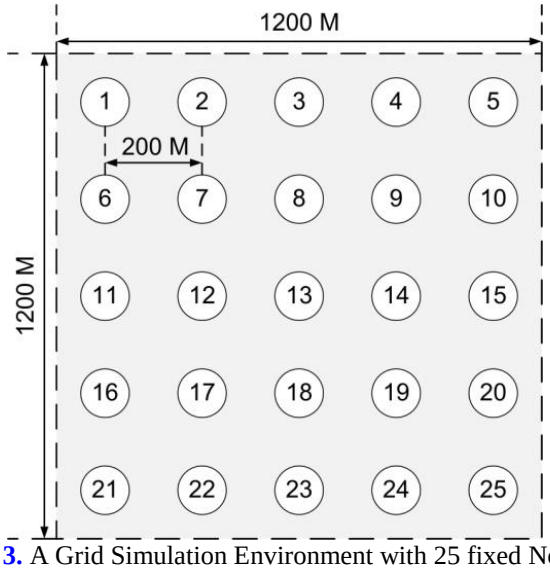

Fig. 3. A Grid Simulation Environment with 25 fixed Nodes

5.2 A Random Simulation Environment:

We simulate a network with 670m*670m space and 50 mobile nodes. The simulation span is 100 seconds. The mobile nodes move within the network space according to the random waypoint mobility model [15] with a maximum speed of 20m/s. The pause time is 50 seconds. The communication patterns we use are 10 constant bit rate (CBR) connections with a size of 512 byte. In the following simulation, the time period for collision report is one second.

5.3 Metrics

1) *Overall Packet Delivery Rate*: the percentage of the data packets which are actually received by the destination. We measure the overall throughput to analyze how gray hole attack impacts the performance of the entire network under different number of attackers and different gray magnitude.
2) *Accumulated Collision Rate:* designed to calculate dynamic threshold. Before we can confidently use the formula in Section IV, we must evaluate whether accumulated collision rate actually reflects a node's network overload.
3) *Detection Probability:* the ratio of the number of detected malicious nodes and the total number of malicious nodes. This metric directly reflects the performance of our detection algorithm.
4) *False Positive Probability:* the ratio of number of honest nodes mistakenly detected as malicious and the total number of honest nodes. Theoretically, our adaptive detection method should have a better performance on false positive probability than the fixed-threshold solution. We verify this inference by comparing false positive probability between different solutions.

6. Simulation Results and Discussion

6.1 Gray Hole Attack's Impact on Network Performance

The first task is to determine the impact of gray hole attack. We focus on the number of attackers and the gray magnitude of gray hole. In this experiment, we use the random simulation environment

We randomly choose 0, 3, 6, 9, 12, and 15 malicious nodes in each of the simulation test. Furthermore, different gray magnitude (GM) - 0.2, 0.4, 0.6, 0.8, and 1.0- are tested. Here, packet delivery rate is used to reflect the performance of network. We repeat every single experiment for 10 times and then calculate the average value and the standard error.

The simulation result is presented in **Fig. 4**. In case the network is free from gray hole attack, packet delivery rate is close to 1.0, which is the best status of the test network. When the number of gray hole increases, packet delivery rate decreases accordingly. Especially, if there are 15 black holes (gray holes with gray magnitude of 1.0), more than 40% packets will be lost in the half way. On the other hand, a higher gray magnitude leads to a more server impact. While over 40% packets lost under the situation of 15 black holes, less than

20% packets are dropped maliciously when the gray magnitude is lower than 0.6.

Based on this result, we will only focus on gray hole with gray magnitude of 0.6 or above, because a lower gray magnitude cannot bring about great damage to the network.

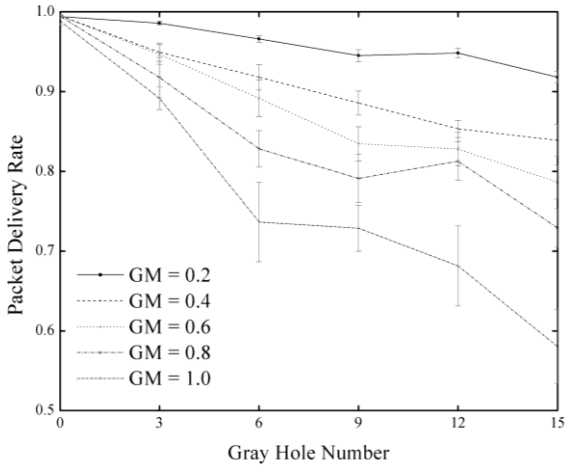

Fig. 4. Packet Delivery Rate vs. Gray Hole Number under Different Gray Magnitude from 0.2 to 1.0

6.2 Analysis of Collision Rate

It is reasonable to estimate that the collision rate should be high in two cases: 1) where number of CBR stream is large, 2) where CBR rate is high. To verify this hypothesis, we designed an experiment under the grid simulation environment.

Table 1. Classification of node in the grid environment

Node Class	Member of This Class
Node I	Node 13[a]
Node II	Node 8, Node 12, Node 14, Node 18
Node III	Node 7, Node 9, Node 17, Node 19
Node IV	Node 3, Node 11, Node 15, Node 23
Node V	Node 2, Node 4, Node 6, Node 10, Node 16, Node 20, Node 22, Node 24
Node VI	Node 1, Node 5, Node 21, Node 25

a. The node number is based on Fig. 3

We set up 8 CBR streams: from Node 1 to Node 25, from Node 2 to Node 24, from Node 3 to Node 23, from Node 4 to Node 22, from Node 5 to Node 21, from Node 10 to Node 16, from Node 15 to Node 11, and from Node 20 to Node 6. These 8 CBR streams are symmetrical to the center node (Node 13), so that a node which is closer to the center has a higher probability to be engaged into more CBR streams. We classified all 25 nodes into 6

class listed in **Table 1**. In each class, every node is located to the center in the same distance. For example, the distance between nodes in Class II and the center is 200m; in Class VI is approximately 566m. Especially Node Class I only contains the center node. We compare the reported collision rate between different node classes to evaluate the number of CBR stream's effect on collision probability.

In addition to location, we also consider the impact brought by different CBR rate. We carry out the experiment under different CBR rate and compare the reported collision as well.

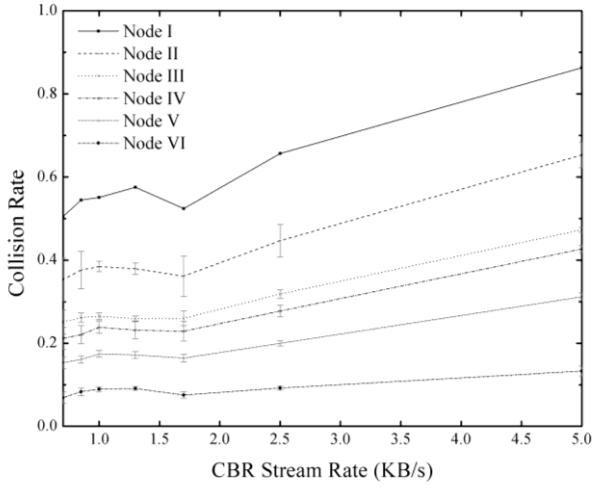

Fig. 5. Reported Collision Rate vs. CBR stream rate with different distance to the topology center of the test network

Fig. 5 shows the experiment result. The average collision rate is used to represent a node class's performance, and standard error is also given. 6 lines indicate collision rate of different node class. The center node suffers a high collision rate and collision happens less likely in those remote node classes. On the other hand, when CBR Stream Rate increases from 0.4KB/s to 5.0KB/s, reported collision rate has an obvious trend to rise. For those nodes that are close to the center, collision rate rises more rapidly.

These results confirm our previous inference that there are more collisions in the aera where network is crowded. Based on this result, we are confident to carry out further experiments.

6.3 The Performance of Our Detection Method

In the third experiment, our detection algorithm is tested. We use the random simulation environment in this part. Because attackers with a gray magnitude below 60% only have slight impact on network's performance, in this experiment, only those attackers with gray magnitude above 60% are added into the network. We randomly choose 0, 3, 5, 8, 10, 13, and 15 malicious nodes in each of the simulation test. We choose attackers' gray magnitude

100%. To get more accurate results, every single experiment is repeated for 10 times; average value and standard error of the experiment results are calculated and presented. Our detection threshold is dynamically calculated by Formula (8) in Section IV, and the parameter T_f is set to 0.6.

Furthermore, we compare our solution with the DSR_Probe [16]. **Fig. 6** and **Fig. 7** present the experiment result.

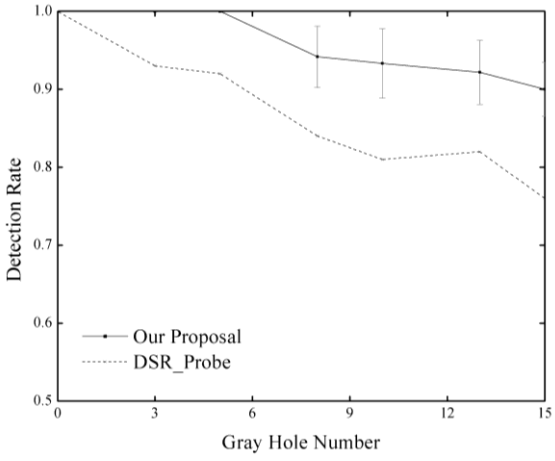

Fig. 6. Detection Rate vs. Gray Hole Number: Detection threshold is set to 0.6, and the attacker is black hole

In **Fig. 6**, detection rate is compared. Our proposal accomplishes higher detection rate compared with DSR_Probe scheme. In DSR_Probe scheme, detection rate drops rapidly while gray hole number continues to increase; however, over method provided detection rate not less than 0.9 under call circumstance.

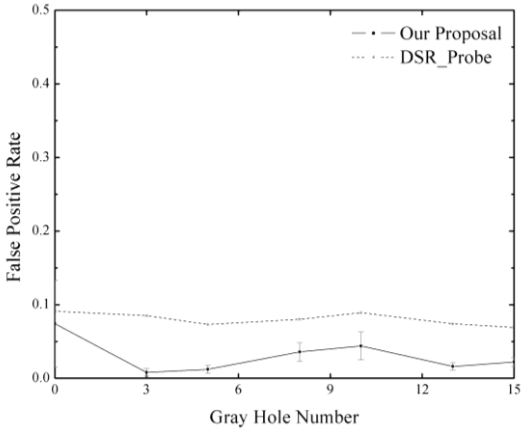

Fig. 7. False Positive Rate vs. Gray Hole Number: Detection threshold is set to 0.6, and the attacker is black hole

Fig. 7 shows that our proposal gains relatively lower false positive rate. False Positive Rate vs. Gray Hole Number: Detection threshold is set to 0.6, and the attacker is black hole

Actually, T_f being set to 0.6 is a conservative strategy. If T_f is modified to a higher value, false positive rate would decrease. However, we recommend 0.6 because under this setting, the algorithm can safely detect nearly all kinds of gray hole which gray magnitude is larger than 0.6. The following is a validation test.

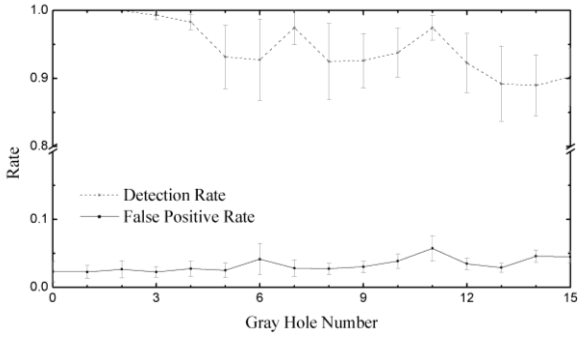

Fig. 8. Detection Rate & False Positive Rate vs. Gray Hole Number: Detection threshold is set to 0.6, and the attackers' gray magnitude is between 60% to 100%

We randomly choose 0 to 15 malicious nodes and 60% to 100% gray magnitude for every attacker in each of the simulation test. We still run every single test for 10 times. Test results are showed in **Fig. 8**.

Approximately, detection rate still keeps above 90%, and false positive rate is lower than 5%. This result reflects that our detection scheme is valid for attackers with gray magnitude between 60% and 100%.

6.4 Analysis of Dynamic Threshold

Last but not least, the dynamic threshold's contribution on detection performance must be evaluated, so we designed the following experiment.

Detection rate and false positive rate are compared between fixed threshold strategy and dynamic strategy. The gray hole number is set to 10 and the gray magnitude is set to 60%. CBR stream rate keeps changing from 0.5KB/s to 2.5KB/s. As same as previous tests, we run every single test for 10 times.

It is presented in **Fig. 9** that adaptive threshold method really decreases the false positive rate. Especially, when CBR stream rate reaches a high level, false positive rate rises sharply. However, in adaptive scheme, false positive rate remains in a relative low level.

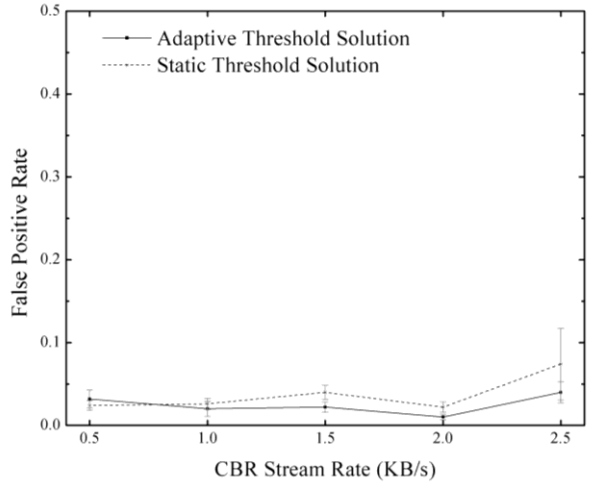

Fig. 9. False Positive Rate vs. CBR Stream Rate: comparison between adaptive sulotion and static solution, attackers' gray magnitude is set to 60%

As for detection rate, the adaptive threshold sulotion is not as competetive as the static threshold sulotion under a high CBR stream rate as shown in **Fig. 10**. This result is predictable because a high CBR stream rate leads to a high collision rate. According to Formula (8) in Section IV, when collision rate rises, $T_d(N)$ increases as well, so that some gray hole will not be detected. This is an unsolved problem in the adaptive threshold strategy.

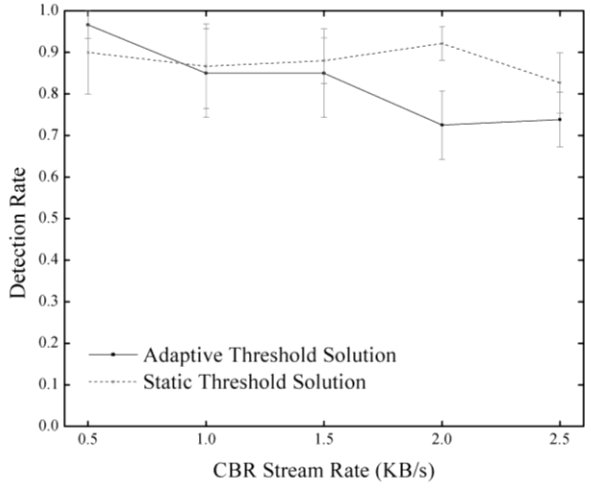

Fig. 10. Detection Rate vs. CBR Stream Rate: comparison between adaptive sulotion and static solution, attackers' gray magnitude is set to 60%

7. Conclusion

Wireless Ad Hoc network is likely to be attacked by the black and gray hole attack. To solve this problem, we presented a path based method to detect black and gray hole attack. After theoretically analyzing advantages and disadvantages of this method, we proposed an adaptive algorithm to enhance the detection performance. The simulation results reveal that attacks with gray magnitude above 60% would bring about magnificent damage to the network. We compare our method to other strategy, and confirm our proposal as successful to provide better detection. Finally, we evaluate the positive and negative impacts brought by adaptive detection scheme, which provide a better false positive rate, but a less competitive detection rate as well.

References

[1] H.Nishiyama, T.Ngo, N. Ansari, N.Kato, "On Minimizing the Impact of Mobility on Topology Control in Mobile Ad Hoc Networks," *IEEE Transactions on Wireless Communications*, Vol.11, No.3, pp. 1158 – 1166, 2012. Article (CrossRef Link).

[2] Yingbin Liang, Poor, H.V., Lei Ying, "Secrecy Throughput of MANETs Under Passive and Active Attacks," *IEEE Transactions on Information Theory*, Vol.57, No.10, pp. 6692 – 6702, 2011. Article (CrossRef Link).

[3] Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, Ruoyu Wu, "Risk-Aware Mitigation for MANET Routing Attacks," *IEEE Transactions on Dependable and Secure Computing*, Vol.9, No.2, pp. 250 – 260, 2012. Article (CrossRef Link).

[4] Deng, H., Li, W., & Agrawal, D., "Routing Security in Wireless Ah Hoc Networks," *IEEE Communications Magazine*, Vol.40, No.10, pp.70 – 75, 2002. Article (CrossRef Link).

[5] Johnson DB, Maltz DA, Broch J., "DSR: The dynamic source routing protocol for multiple wireless ad hoc networks," *Ad Hoc Networking.* Addison-Wesley, pp.139-172, 2001.

[6] Cai, J.W., Yi, P., Tian, Y., Zhou Y.K., Liu N., "The Simulation and Comparison of Routing Attacks on DSR Protocol," in *Proc. of 5th International Conference on Wireless Communications, Networking and Mobile Computing, 2009 (WiCom '09)*, Beijing, China, September, 2009. Article (CrossRef Link).

[7] Bo Sun; Yong Guan, Jian Chen, Pooch U.W., "Detecting Black-hole Attack in Mobile Ad Hoc Networks," in *Proc. of 5th European Personal Mobile Communications Conference,* pp.490-495, 2003. Article (CrossRef Link).

[8] Patcha, A., Mishra, A., "Collaborative security architecture for black hole attack prevention in mobile ad hoc networks," *Radio and Wireless Conference*, pp.75-78, 2003. Article (CrossRef Link).

[9] Gao Xiaopeng, Chen Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks," in *Proc. of IFIP International Conference on Network and Parallel Computing Workshops*, pp.209-214, 2007.Article (CrossRef Link).

[10] D. Boneh, C. Gentry, B. Lynn, H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," *Advances in Cryptology-EUROCRYPT'03: LNCS 2656*. Berlin: Springer-Veralg, pp.416-432, 2003. Article (CrossRef Link).

[11] Shila, D.M., Anjali, T., "Defending selective forwarding attacks in WMNs," in *Proc. of IEEE International Conference on Electro/Information Technology*, pp.96-101, 2008. Article (CrossRef Link).

[12] Akyildiz, I. F., & Wang, X., "A Survey on Wireless Mesh Networks," *IEEE Communications Magazine*, Vol.43, No. 9, pp.23-30, 2005. Article (CrossRef Link).

[13] D.S J De Couto, D.Aguayo, J.Bicket, and R.Morris, "A High-Throughput Path Metric for Multi-Hop Wireless routing," in *Proc. of ACM International Conference on Mobile Computing and Networking (ACM Mobicom2003)*, 2003. Article (CrossRef Link).

[14] Kevin Fall and Kannan Varadhan, *NS notes and documentation*, The VINT Project, UC Berkely, LBL, USC/ISI, and Xerox PARC, 1997.

[15] J. Broch, D. A. Maltz, D. B. Johnson, Y. C. Hu, and J. Jetcheva, "A performance comparison of multi-hop wireless ad hoc network routing protocols," in *Proc. of ACM International Conference on Mobile Computing and Networking (ACM Mobicom1998)*, 1998. Article (CrossRef Link).

[16] M. Just, E. Kranakis, and T. Wan, "Resisting Malicious Packet Dropping In Wireless Ad Hoc Networks," *International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW2003)*, Oct. 2003. Article (CrossRef Link).

Chundong She was born in 1971. Currently he is Professor at School of Electronic Engineering, the Beijing University of Posts and Telecommunications in China. He received the BSc degree in department of computer science and engineering from the PLA University of Science and Technology, Nanjing, in 1991. He received the MSc degree in computer science from the Nanjing University of Aeronautics and Astronautics, Nanjing, in 1997. He received the Ph.D degree at the school of computer science and engineering, from the University of Electronic Science and Technology of China, in 2004. His research interests include sensor networks system and networks security. Email:shurcd@vip.sina.com

Ping Yi was born in 1969. Currently he is Associate Professor at School of Information Security Engineering, Shanghai Jiao Tong University in China. He received the BSc degree in department of computer science and engineering from the PLA University of Science and Technology, Nanjing, in 1991. He received the MSc degree in computer science from the Tongji University, Shanghai, in 2003. He received the Ph.D degree at the department of Computing and Information Technology, Fudan University, China. His research interests include mobile computing and ad hoc networks security. He is a member of IEEE Communications and Information Security Technical Committee, Associate Editor for Wiley's Security and Communication Networks (SCN) Journal, Editor for Journal of Security and Telecommunications, Technical Program Committee (TPC) for the ICC'12 CISS (ICC 2012 Communication and Information Systems Security Symposium), the GC'12 CCNS (IEEE Globecom 2012 Computer and Communications Network Security Symposium) .

Junfeng Wang was born in 1976. He received the M.S. degree in Computer Application Technology from Chongqing University of Posts and Telecommunications, Chongqing in 2001 and Ph.D. degree in Computer Science from University of Electronic Science and Technology of China, Chengdu in 2004. From July 2004 to August 2006, he held a postdoctoral position in Institute of Software, Chinese Academy of Sciences. From August 2006, Dr Wang is with the College of Computer Science, Sichuan University as a professor. His recent research interests include spatial information networks, network and information security, and intelligent transportation system.

Hongshen Yang was born in 1968. Currently he is Lecturer at College of Electrical Engineering, Tongling University in China. He received the M.S. degree of Engineering from Hefei University of Technology of China. His research interests include sensor networks system and networks security.