Journal of Computer Science 9 (12): 1722-1733, 2013
ISSN: 1549-3636

doi:10.3844/jcssp.2013.1722.1733 Published Online 9 (12) 2013 (http://www.thescipub.com/jcs.toc)

EFFECTIVE BLACK HOLE ATTACKS IN MANETS

[1]Raja Azlina Raja Mahmood, [1]Zurina Mohd Hanapi,
[1]Sazlinah Hasan and [2]AsadIqbal Khan

[1]Department of Communication Technology and Network,
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia
[2]Clayton School of Information Technology, Monash University, Melbourne, Australia

Received 2013-08-14, Revised 2013-09-30; Accepted 2013-10-29

ABSTRACT

Black hole or packet drop attack is a denial of service attack on routing protocols in which malicious nodes fabricate routing information, attract packets routed through them and then deliberately drop these packets. Most of the black hole attack simulations are performed by constantly fabricating routing information and thus consistently attracting packets to them, which can be easily detected by the intrusion detection system. In this study, a complicated and difficult to detect black hole attack is proposed. The malicious nodes only perform packet drop when they are in the advantageous positions or locations in the networks. This study investigates the impact of the proposed black hole attack performed by random as well as critical nodes, to the network performance. Critical nodes are nodes that reside along the most active traffic paths and results show that the attacks performed by these nodes cause significant damage to the networks or substantial reduction in packet delivery ratio in comparison to that of random nodes.

Keywords: Black Hole Attacks, Critical Nodes, Intrusion Detections Systems, MANETs

1. INTRODUCTION

Mobile ad hoc networks, also known as MANETs have been proven beneficial in many application areas. Due to their unique network characteristics, they have been deployed in many networks including the army tactical networks, battlefield surveillance networks, post-disaster emergency networks, environment and habitat monitoring networks and traffic control networks.

MANET consists of mobile, tiny, low-powered battery devices with limited processing and storage resources. Being an ad hoc network, MANET is an infrastructure-less network whereby the communication among the nodes is done through multi-hop that is the neighboring nodes forward the data for the sender if the destination is not within the sender's transmission range. In other words, each mobile node in the networks acts as both a router and a host. Communication of multi-hop wireless networks however has its own disadvantages, which includes being susceptible to many attacks. In particular, the networks can easily be crippled by the Denial of Service (DoS) attacks, such as the infamous black hole or packet drop attack.

Many researchers have simulated black hole attacks in their works and provided detection and/or prevention mechanisms as well (Yerneni and Sarje, 2012; Thachil and Shet, 2012; Osathanunkul and Zhang, 2011; Kurosawa *et al*., 2007). However, most of the black hole attacks simulations have been carried out by randomly assigned some nodes as the attackers. In addition, the attackers consistently fabricate routing information and thus attract all packets to them. Such behavior can be easily detected by the Intrusion Detection System (IDS). We propose a more complicated black hole attack. The attacks are only performed when the nodes are in the advantageous positions or locations within the networks. Thus, with such intermittent attacks, the traditional IDS may not be able to detect such behaviors easily. In this study, we simulate such attacks in two different scenarios, with randomly distributed

Corresponding Author: Raja Azlina Raja Mahmood, Department of Communication Technology and Network,
Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Malaysia

attackers as well as with selectively distributed attackers and study the impact of the attacks to the network performances. We define randomly distributed attackers as nodes that are randomly chosen to be attackers regardless of their positions or locations in the networks. Meanwhile, the selectively distributed attackers are nodes that reside along the most active traffic within the networks. Some packet loss activities are expected in both scenarios but major packet loss, thus significantly degrade the performance of the networks, can be anticipated from the selectively distributed attackers.

The rest of the study is organized as follows. In the following subsections, we discuss some of the attacks in MANETs with detailed explanation on the black hole attacks, some of the related works on simulating the black hole attacks and the implementation of the proposed black hole attacks. In section 2, we describe the parameters used in the experiments. In section 3, we present the simulation results of attack-free networks, as well as networks with effective black hole attacks by random nodes and critical nodes. Section 4 discusses the simulations findings and we conclude the work in section 5.

1.1. Attacks in MANETS

Table 1 shows some of the attacks in MANETs, based on protocol stacks. The attackers are known by few names, namely malicious, selfish and misbehaving nodes. The nodes that attack with the intention of bringing down the network, such as by performing Denial of Service (DoS) attack are called malicious nodes. Meanwhile selfish nodes are those that optimize their own gain and neglect the welfare of other nodes, such as by dropping other nodes' packets in order to conserve their own energy. These nodes are sometimes called misbehaving nodes, as they are not being cooperative or do not follow the protocols specifications.

Network layer or routing attacks are the current attack trends been heavily studied. Among ad hoc routing protocols, the reactive Ad Hoc On-Demand Distance Vector (AODV) (Perkins and Royer, 1999) and Dynamic Source Routing (DSR) (Johnson and Maltz, 1996) protocols are the most widely deployed. In response to any link breakage or changes in the network topology, the protocols perform route discovery to quickly find alternative routes. The source node floods the network with control messages known as Route Request (RREQ) and expects a Route Reply (RREP) packet in return. In AODV, the intermediate nodes with the best path value to the destination node will respond to the source node. Since our work will be focusing on AODV routing protocol, we will only include detailed explanation of its route discovery, as depicted in **Fig. 1**.

In order for node Src to send packets to node Dst, it has to generate a RREQ message and broadcast it to its neighbors, in this case, A, C and D. The RREQ contains the last known destination sequence number, in this case the Dst sequence number. The destination sequence number is an important attribute in RREQ that determines the freshness of a particular route. Thus, if any of the neighboring nodes has a fresh enough route to Dst, it will send a RREP message to Src. On the contrary, in case where it does not have a fresh enough route to Dst, it will forward the RREQ packet to its neighbours and this activity is repeated until the packet reaches Dst. When Dst receives the RREQ packet, it sends a RREP packet to Src. When node Src receives the RREP, a route is established. In case where Src receives multiple RREP messages, it will select the message with the largest destination sequence number value.

1.1.1. Black Hole Attacks

Black hole attack is also known as packet drop as well as sequence number attack. This attack is easily implemented in AODV during the route discovery process. In this attack, a malicious node advertises itself as having the shortest path to the destination node and thus will be selected against other nodes to forward the packets for the sender. In specific, the attacker forges its destination sequence number by having a relatively high destination sequence number, thus pretending to have the fresh enough route to destination. In general implementation, the legitimate node with the shortest path to the destination would increase its destination sequence number's value by 1, but the attacker would increase its destination sequence number's value by a large value, such as 10. Thus, this attacking node will then be in favored against others and once the forged route has been established, it becomes a member of the active route and intercepts the communicating packets. The attacker then drops all of the incoming packets routed through it and thus creates a black hole in the networks.

Alternatively, the attacker may choose to drop only selected incoming packets routed through it. In accomplishing the attack selectively, the malicious node only drop the packets based on certain criteria such as for a particular destination, at the certain time, a packet for every n packets or every t seconds, or randomly selected portion of the packets. Such attack is known as a gray hole attack and it is more difficult to detect in comparison to dropping all packets that come in. As mentioned earlier, the black hole attack is a type of DoS attack and thus, can be used as the first step to the man-in-middle attack, where the malicious node may monitor, delay, delete or manipulate the data packets.

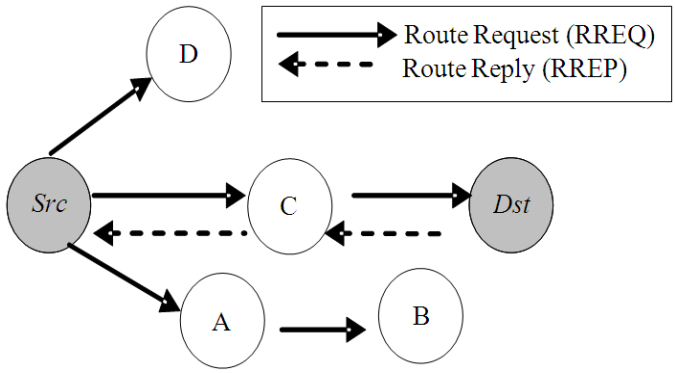

Fig. 1. An AODV discovery process

Table 1. Security attacks on MANET protocol stacks (Wu *et al*., 2010)

Layer	Attacks
Application layer	repudiation, data corruption
Transport layer	session hijacking, SYN flooding
Network layer	wormhole, black hole, Byzantine, flooding, resource consumption, location disclosure attacks
Link layer	traffic analysis, monitoring, disruption MAC, WEP weakness
Physical layer	jamming, interceptions, eavesdropping
Multi-layer	DoS, impersonation, replay, man-in-the-middle

1.1.2. Attack Detection Metric

The presence of the black hole or packet drop attacks in the networks is generally determined by the Packet Delivery Ratio (PDR) value. It is one of the most common metrics used to evaluate the performances of the routing protocols, among other metrics including throughput, end-to-end delay, overheads and jitter as reported by Broch *et al*. (1998). The PDR is calculated as follows Equation (1):

$$PDR = \frac{\sum \text{received packets at application layer}}{\sum \text{sent packets at application layer}} \quad (1)$$

Thus with the black hole or packet drop attacks in the networks, the PDR percentage should have been deteriorated. The decreasing of the percentage of PDR somehow varies due to different parameter settings, such as random node movements and different source-destination established connections. Next section discusses in details few of the black hole attacks implementations, detection methods as well as prevention methods using NS2.

1.2. Related Works

Yerneni and Sarje (2012) implemented a secure AODV, known as Opinion AODV (OAODV) and compared its PDR result against that of the traditional AODV within the under-attack networks. They simulated 20 to 50 mobile nodes under various speeds, from 5 to 40 m sec^{-1} for 50 sec. However no specific information on the black hole attack implementation has been provided, including number of attackers and how they have been selected. The results however shown that with black hole attacks within the normal AODV networks, the PDR has been significantly reduced to between 5 to 30% only. Meanwhile, the proposed method is able to thwart the attacks effectively with its high PDR resulting value ranging from 60 to 80%. With no details given on the number of attackers, we do not know the percentage of attackers within the networks. We could only assume that the attackers are randomly selected and the impact of the attacker or attackers to the networks is based on the PDR results given. With limited information, no correlation between the packet drop percentage and number of attackers in the networks can be made. In this study, the simulation was performed for the duration of 50 sec. The disadvantage of having a short simulation time however is that many source-to-destination connections may not get properly established when the simulation ends or in other words, the network has not reached its stable state. This could contribute to low PDR percentage within the network due to a number of data packets that

have not been received by the destination nodes when the 50 sec simulation time ends.

Thachil and Shet (2012) proposed a trust based approach to mitigate black hole attack in MANETs. They simulated 50 mobile nodes with speed of 20 m sec^{-1} for 500 milliseconds and 1000 milliseconds. They deployed different number of malicious nodes, from 1 to 25 nodes or up to 50% of the network population. However, no detailed explanation is given on the attackers' selection and thus can be assumed randomly selected. As expected, with more attackers in the networks, the PDR value deteriorates even reaching 0% or collapsing the whole normal AODV network when there are 5 or more collaborative attackers in the networks. Their proposed method however is able to mitigate the attacks effectively and thus, causes minimal damage to the networks. The graph shows considerable reduction of PDR value when the proposed method was employed, that is the PDR value maintains at 80% when there are 5 malicious nodes and deteriorates afterwards to the lowest of 70% for 1000 milliseconds simulation time and to the lowest of 30% for network with simulation time of 500 milliseconds. Similar to Yerneni and Sarje (2012), this work has been simulated within a short span time, thus may have suffered from the abovementioned effect.

Osathanunkul and Zhang (2011) present a solution called Secure Expected Transmission Count (SETX) to counter black hole attack. They simulated 50 to 100 nodes with speed of 5 m sec^{-1} for 50 sec. They deployed 1 to 10 malicious nodes and studied the network PDR value respectively. As expected, the PDR steadily reaching 0% when there are 3 or more attackers in the traditional MANETs. Their method has significantly improved the network performance with the resulting PDR value ranges from 60 to 10% for the network of size 50. Meanwhile, in the network of bigger size, that is size 100 nodes, the PDR performance is better, ranges from 70% to the lowest of 25%. It can be concluded that with higher percentage of attackers within the network, the packet drop percentage increases. This explains why 10 attackers within network of 50 nodes are more harmful than having 10 attackers within network of 100 nodes, assuming that all the attackers are of the same capability. Similar to Yerneni and Sarje (2012) and Thachil and Shet (2012), the simulation time undertaken in this work is considerably short and thus also may have suffered from the abovementioned effect. It is worth to mention that the common simulation time used by the highly cited research works in studying the performances of MANETs with attacks presence, including Huang *et al*. (2003); Stamouli *et al*. (2005) and Kurosawa *et al*. (2007) is 900 sec or longer. All of the abovementioned highly cited works are following the work of the pioneers in MANETs (Broch *et al*., 1998).

The implementation of black hole attacks in these discussed works is performed in such a way that the malicious nodes always fabricate routing information and thus always attract packets to them. Thus, it explains the collapsed network even with the presence of only 5 attackers in a 50- node network as reported by Thachil and Shet (2012) and with the presence of 3 attackers in 50- and 100- node networks as reported by Osathanunkul and Zhang (2011) within a short period of time. However, we take a different approach. The next section discusses our implementation of the proposed black hole attack in details.

1.3. Effective Black Hole Attacks

We propose a more complicated and difficult to detect black hole attack. In particular, the fabrication of the routing information activity undertaken by the malicious nodes is intentionally made inconsistent, that is to avoid detection. Nodes that attract data packets all the time are easier to be detected by the IDS in comparison to nodes that attract packets intermittently. In our implementation, the nodes will only fabricate the routing information when they are at the appropriate or advantageous locations, such as they are legitimately within the paths of the forwarded packets. This is to prevent the nodes from being detected by intelligent agent or sensor that may have studied the location of the nodes that respond to have the shortest path to the destination. Similar detection method has been proposed earlier by Lee *et al*. (2008), but in the case of mitigating wormhole attack. They proposed each node gathers information of its neighbors within two hops. That is each newly joined node broadcasts an announcement, which is valid only within the next two hops. Although the method is capable of preventing the attacks, the requirement of maintaining two hops neighbors, keyed hash and TTL however limit the applicability of this method in a distributed system where there exists a wide variety of participants. Thus, similar detection technique may also be proposed to detect black hole attacks, in which the sensor is to gather information of the nodes within the destined traffic paths and thus the malicious nodes may be punished if they are not within these legitimate paths or in other words detected for fabricating the routing information.

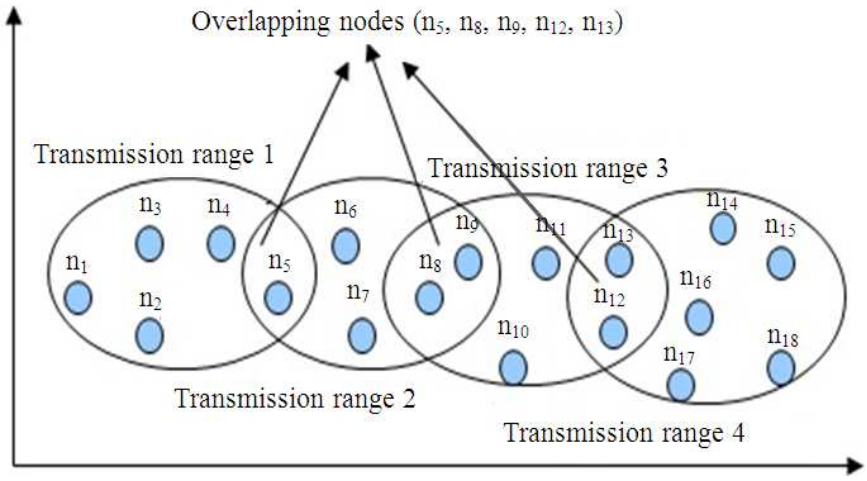

Fig. 2. MANET of 18 nodes with n_5, n_8, n_9, n_{12} and n_{13} overlapping nodes

In our implementation, malicious nodes only fabricate routing information when they are at appropriate locations, which are within the destined traffic paths. Intermittent attacks or sporadic packet loss is more difficult to detect than the consistent attacks. We simulate such effective attacks in two different scenarios, with attackers that are randomly distributed as well as with selectively distributed attackers. We define randomly distributed attackers as nodes that are randomly chosen to be attackers regardless of their positions or locations in the networks. Meanwhile, the selectively distributed attackers are nodes that are located along the most active traffics within the networks. The nodes that reside along the most active paths are called critical nodes, in which any disruption, in this case packet drop by these nodes may significantly degrade the performance of the networks. Thus black hole attacks by these critical nodes are expected to cause major damage to the networks, yet difficult to detect due to the intermittent attacks.

Overlapping nodes, as shown in **Fig. 2** are good candidates for critical nodes as they are responsible to forward packets from one cluster or one transmission range to another. Critical nodes have also been discussed by other researchers, especially in identifying critical nodes within the networks.

It is worth to mention that identifying critical nodes within MANETs is a highly challenging task. Given the time delays of the diagnostic packet, the mobility of the nodes and the limited processing resources makes determining the global network topology process seems impossible. Thus, many resort to approximating the network topology, which is also able to provide useful information such as the network density, network mobility, critical paths and thus, critical nodes in the networks. Karygiannis *et al.* (2006) approximate the global network topology by employing a graph theoretic approach as well as deploying network discovery algorithm. Meanwhile, Shivashankar and Varaprasad (2012) identified critical nodes in MANETs based on residual battery power, reliability, bandwidth, availability and service traffic type.

In this study, we simulate attack-free networks and then analyze the enormous traffic information to determine the network topology at certain given time. We then identify the critical nodes by focusing on the nodes that forward packets the most during the simulation period. This study aims to investigate the impact of the effective black hole attacks performed by randomly located nodes as well critical nodes to the network performances, in terms of PDR and packet drop percentage. Next section discusses the simulation works in details.

2. MATERIALS AND METHODS

We simulate a condense MANET with 50 nodes within a field size of 1500×300m using NS2. The parameters for the simulations are given in **Table 2**. The nodes will move within the network space according to the random waypoint mobility model, in which each node will move to a random location within the specified network area. Once the node arrived at the target location, it will remain in that position for a specified time, in this case the pause time, before moving to another random location. In our simulation, we have set multiple pause time, ranging from 0 s pause (high mobility) to 900 s pause (static), to study the nodes and networks behaviors under different stopping time.

Table 2. Simulation parameters

Parameters	Values
Simulation Time	900 sec
Number of mobile nodes	50
Topology	1500×300 m
Mobility Model	Random waypoint
Transmission Range	250 m
Routing Protocol	AODV
Maximum Bandwidth	2 Mbps
Traffic	Constant bit rate
Number of Traffic Sources	20
Packet size	64 bytes
Packet rate	4 packets sec^{-1}
Speeds	5, 15, 20 m sec^{-1}
Pause Times	900, 600, 300, 120, 60, 30, 0 s

The communication patterns deployed is the Constant Bit Rate (CBR) connection with a data rate of 4 packets per second with each packet of 64 bytes in size and 20 connections are established at random. We also set multiple movement speeds for the nodes, with the speed of 5 m sec^{-1} is to simulate people jog, 15 m sec^{-1} is to simulate a slow-speed moving car and 20 m sec^{-1} is to simulate a car of a high speed.

3. RESULTS

3.1. Attack-Free Networks

In the attack-free networks we discuss the performance of its PDR under different speed rates of different pause times. In general, as the speed of the node increases and with high mobility (pause 0, 30 and 60), the PDR percentage degrades as more path links break due to the node movement and finally lead to high packet drops. **Figure 3** shows the overall PDR performance for the attack-free networks, with all of the PDR percentage are above 95%, as AODV quickly finds alternative routes whenever there are broken paths. Within the attack-free networks, we have observed the packets drop percentage is very minimal, such that the percentage of packet delivery ranges from the lowest of 94.9% to the highest of 99.5% with the average percentage value of 96.8%. Many works have shown similar PDR results and thus we can safely assume that 95% is the PDR threshold value for MANETs with standard routing protocol implementation, that is without any packet dropping attacks (Yerneni and Sarje, 2012; Thachil and Shet, 2012; Osathanunkul and Zhang, 2011; Kurosawa *et al*., 2007; Stamouli *et al*., 2005). Thus, with packet drop attacks in the networks, we expect a significant performance degradation, that is much lower PDR percentage.

3.2. Networks with Random Attackers

In this study, we have selected 5 random nodes as the attackers, even before analyzing the forwarding table of the networks. These nodes will only perform the black hole attacks when they are within the destined traffics. We have chosen nodes 5, 10, 15, 25 and 35 to be the attackers. Due to the extensive processing resources required to analyze the huge trace files, we have limited the study to the following pause times only: pause 0 (high mobility), pause 60 and 120 (medium mobility), pause 300 (low mobility) and 900 (static). The results of the network performance with random node attackers are as shown in **Fig. 4**.

As expected, **Fig. 4** shows network performance degradation, with significant degradation in some cases, in comparison to those in the attack-free MANETs due to the deliberate dropping activity by the attacking nodes. With the presence of black hole attacks, the PDR value has dropped, even significantly reduced to 47% for traffic of speed 20 m sec^{-1}, with pause at 900 sec. Based on the results obtained from the attack-free MANETs (**Fig. 3**), it can be concluded that "unjustifiable" packet dropping activity has occurred whenever the PDR value is below the 95% threshold value. With random nodes been chosen as the attackers, we have seen that the percentage of packet delivery ranges from 46.9 to 93.2% with average value of 77.2%. We expect even lower percentage of PDR in the networks with critical nodes are chosen to be the attackers.

3.3. Networks with Critical Nodes as Attackers

In this section, we study the network performances when critical nodes are selected as the attackers. In order to identify the critical nodes, we studied the network topology of various speeds and various pause times. In particular, we identified 5 nodes that forwarded the most packets in the networks in every network scenario. These nodes will only perform the black hole attacks when they are within the destined traffics and since they are at the advantageous positions most of the time, they will perform frequent packet drop. **Table 3** shows the critical nodes of different speed and of different pause time in our experiments. It also shows the total percentage of networks forwarded by these critical nodes. The PDR value would have significantly reduced if all packets forwarded to these critical nodes are deliberately dropped. In specific, the network would have been collapsed when more than half of the network traffics have been dropped by these nodes at speed 5 m sec^{-1} and pause time of 900 sec.

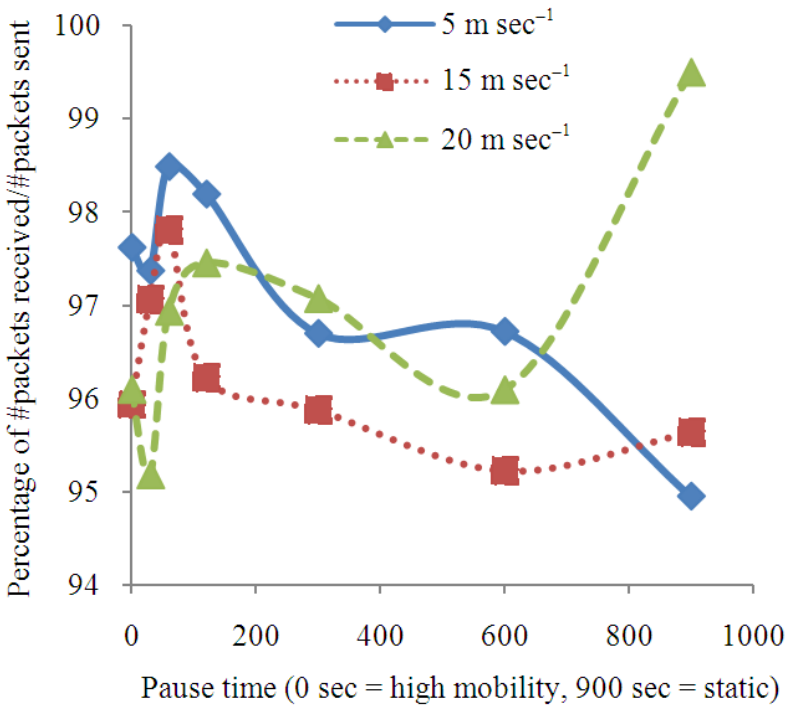

Fig. 3. Packet delivery ratio of attack-free MANETs

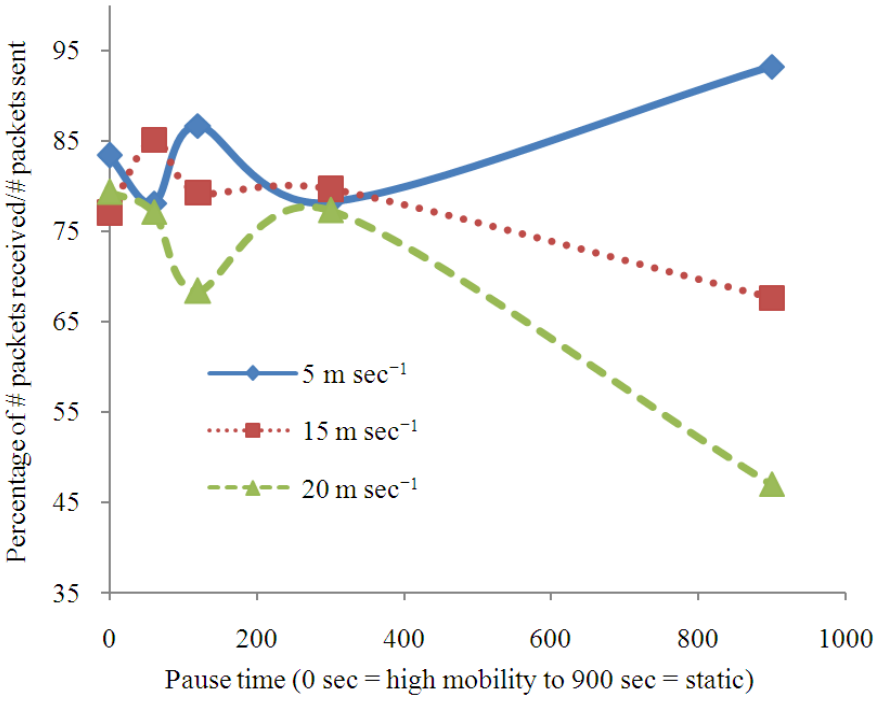

Fig. 4. Packet delivery ratio of MANETs with random attackers, node 5, 10, 15, 25 and 35

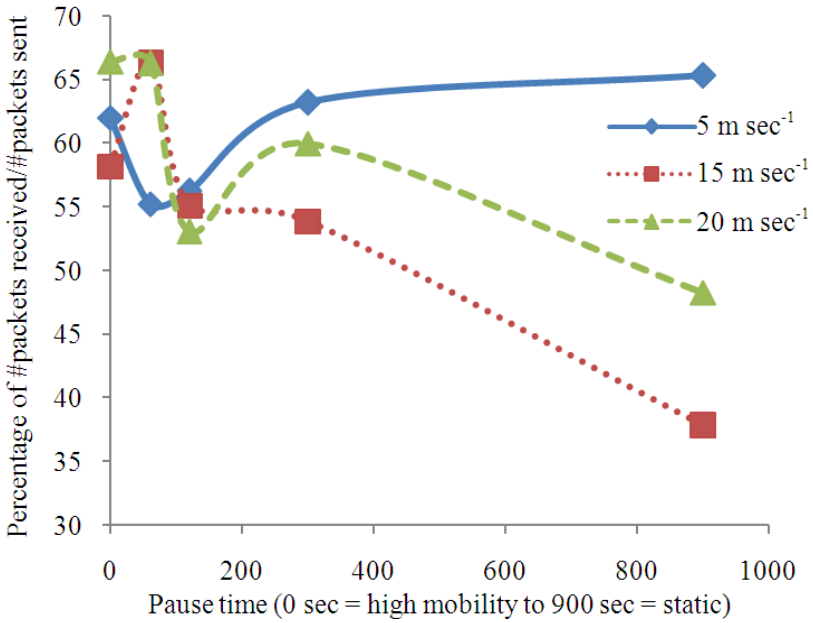

Fig. 5. Packet delivery ratio of MANETs with critical nodes as attackers

Table 3. Critical nodes of different network scenarios

Speed (m/s)	Pause time	Critical Nodes (descending order)	Total percentage of forwarded packets in the networks (%)
5	0	45, 31, 28, 42, 17	21.20
	60	29, 32, 19, 27, 9	21.23
	120	34, 16, 45, 3, 9	23.95
	600	30, 3, 24, 14, 12	31.61
	900	3, 19, 45, 48, 21	51.81
15	0	17, 27, 10, 29, 16	19.89
	60	4, 40, 17, 48, 19	18.93
	120	36, 0, 4, 20, 10	20.27
	600	2, 32, 4, 35, 16	31.96
	900	31, 16, 18, 48, 10	48.29
20	0	30, 34, 45, 25, 32	17.12
	60	10, 19, 23, 45, 38	17.93
	120	16, 36, 10, 9, 2	24.49
	600	41, 15, 1, 42, 49	30.36
	900	42, 29, 35, 34, 10	47.10

From **Table 3**, we can conclude that the critical nodes vary from one network scenario to another. The mobility of the nodes, which act as routers at the same time to forward neighboring packets, has made determining "universal" critical nodes impossible. Suffice to mention that from observation, some nodes appear few times in different scenarios such as nodes 3 and 9 in networks of speed 5 m sec^{-1}, nodes 4 and 10 in networks of speed 15 m sec^{-1} and nodes10, 42 and 45 in networks of 20 m sec^{-1}. This could only mean that these nodes are within the active paths numerous times, thus part of critical nodes for different network scenarios. However, it is worth to mention that the reason for high packet drop percentage in the network with random attackers of speed 20 m sec^{-1}, with pause at 900 sec is because one of the random attackers, namely node 10 is part of the critical nodes (**Table 3**). **Figure 5** shows the damage that these attackers have caused to the networks.

With critical nodes been chosen as the attackers, the percentage of packet drop in the networks has increased significantly, ranges from the lowest of 33.6% to the highest of 62.1%, with average of 42.1% packet dropping. Such high percentage of packet drop could definitely bring down the whole networks. Thus, the PDR value is significantly lower than those of random attackers, in which the percentage of packet delivery ranges only from 37.9 to 66.4% with average value of only 57.9%. The most devastating impact was at speed 15 m sec^{-1} with pause time of 900 sec, whereby 62.15% of the packets supposedly to be forwarded have been dropped deliberately. This result shows that by choosing the attackers carefully, the impact can be overwhelmingly dangerous to the networks, even though the attackers just made up 10% of the network population. Thus, the result has demonstrated that an effective black hole attack performed by the critical nodes causes significant damage in comparison to the damage by the randomly assigned attackers. More importantly, due to the intermittent packet drop activity within the networks, it is more difficult to be detected by the IDS.

4. DISCUSSION

Based on the PDR results shown in **Fig. 4 and 5**, we can conclude that having the critical nodes as attackers cause a devastating impact to the network performance, even catastrophic at times. On the contrary, the attacks by the random nodes have less devastating impacts to the networks, although at speed of 20 m sec^{-1}, with pause at 900 sec, the PDR value has significantly dropped to only 47%. This proves that the random nodes are part of the active paths for that particular network scenario. However, if the randomly chosen attackers are somehow not part of the active paths, the packet drop activity may only occur few times or even not taking place at all. **Figure 6** shows the packet drop percentage by random attackers on various network scenarios. In particular, within the speed 5 m sec^{-1} network scenarios, the packet drop rate ranges from 6.8 to 21.9%, with average value of 16.1%. For network scenarios of speed 15 m sec^{-1}, the rate ranges from 14.9 to 32.4.9%, with average packet drop values of 22.3%. Finally, for network scenarios of speed 20 m sec^{-1}, the rate ranges from 20.7 to 32.4%, with average packet drop values of 26%. In general, on average, the packet drop rate is about 21.47% for each network scenario which can still be considered as having less devastating effects to the networks.

As mentioned earlier, attacks by critical nodes can be catastrophic. The total network could collapse if cooperative attacks are launched by the attackers such as the case of network with speed 15 m sec^{-1} and pause 900 sec with 62.15% packet drop rate as well as network with speed 20 m sec^{-1} and pause 900 sec with 51.72% packet drop rate (**Fig. 7**), in which huge proportion of network traffics are within the attackers' influence.

Figure 7 shows high percentage of packet drop by the critical nodes on various network scenarios. In general, on average, the packet drop rate is about 42.14% for each network scenario, which is double the rate of that of random nodes. In particular, within the speed 5 m sec^{-1} network scenarios, the packet drop rate ranges from 34.7 to 44.7%, with average value of 39.6%. For network scenarios of speed 15 m sec^{-1}, the rate ranges from 33.6 to 62.19%, with average packet drop values of 45.7%. Finally, for network scenarios of speed 20 m sec^{-1}, the rate ranges from 33.6 to 51.7%, with average packet drop values of 41.2%. In summary, the packet drop percentages by the critical nodes are about double the drop percentages by the random nodes and thus have more devastating impacts.

In summary, we can conclude that the packet drop percentage shown by both random and critical attackers are between 5 and 62%. Unlike other works reported earlier, the packet drop percentage has never reached 100% even after the 900 sec simulation time ends. Yerneni and Sarje (2012) reported their PDR has been significantly reduced to only 5%, which means 95% of packets have been dropped within that small span of time or 50 sec simulation time. Meanwhile as reported by Thachil and Shet (2012), their resulting PDR is reduced to 0% or in other words 100% of packets have been dropped, when there were 5 attackers in the networks within the short 500 milliseconds and 1000 milliseconds of simulation time. Osathanunkul and Zhang (2011) reported their PDR reached 0% when 3 malicious nodes performed black hole attacks within the 50 sec simulation time. This shows that consistent packet drop activity within the network by the traditional black hole attacks could collapse the whole networks in short time. However, at the same time, such consistent packet drop behavior can be easily detected by IDS.

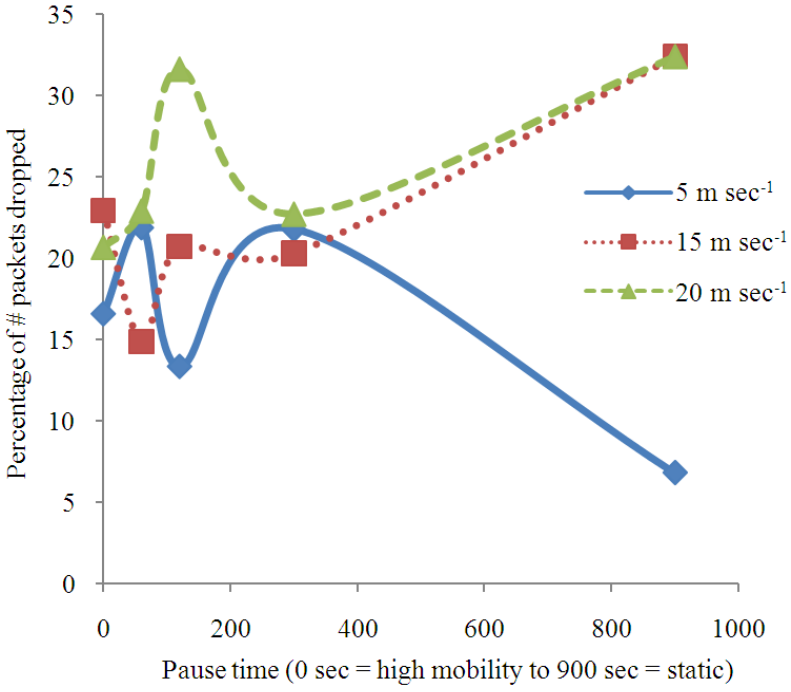

Fig. 6. Packet drop percentage by random attackers

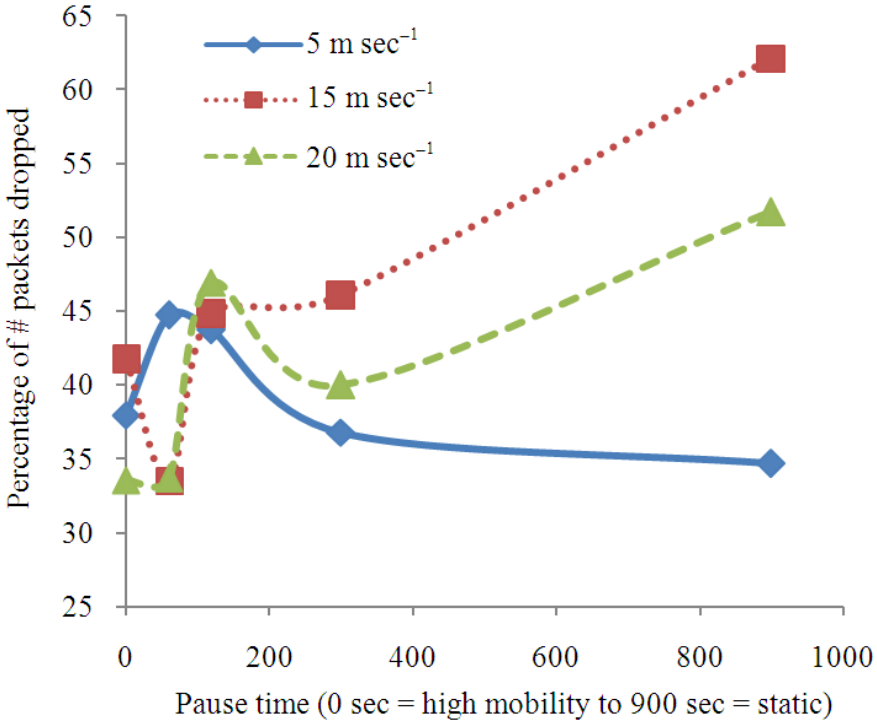

Fig. 7. Packet drop percentage by critical nodes

In this preliminary study, we only consider the non-real time network traffic information in MANETs. We investigate the damage done to the networks when the critical nodes are chosen as the attackers, in comparison to the randomly chosen attackers. In identifying the critical nodes, we analyzed the network traffic information from the enormous NS2 trace files and chose 5 nodes that forwarded packets the most in various network scenarios. The forwarding table of each network scenario is huge and thus requires extensive resources to compute the packet drop percentage of different attackers. For instance, in analyzing the network topology of speed 20 m sec^{-1} with pause 0sec, we have to deal with a 1977 MB size of trace file and have to traverse through 122,062 forwarding activities within the 61,525 source-to-destination paths to determine if the attackers are within the paths and thus to calculate the packet drop. In average, it takes about 6 to 8 h to generate the packet drop percentage results for one network scenario on a 2.3 Ghz Intel Core i5 processor with 4GB RAM machine. Thus, identifying the critical nodes in real-time is even more challenging. Due to the time delays of the diagnostic packets, the mobility of the nodes and the limited processing resources of nodes in MANETs, such attempts can be considered futile. We hope the investigation of the network topology using the non-real time traffic information provides some basis of understanding of the difficulties in dealing with extensive and highly dynamic traffic data within resource-scarce wireless networks.

5. CONCLUSION

In this work, we implemented effective black hole attacks using random nodes as well as critical nodes. We have shown that by choosing random nodes as attackers, the damage may be mild or less significant if the attackers are not within the paths of most of the network traffics. On the contrary, selecting critical nodes as the attackers would significantly degrade the whole network performance and sometimes catastrophic. However, the packets drop percentage shown in this study is considerably low in comparison to that of discussed works that performed traditional black hole attacks. Our proposed attack is more complicated and difficult to detect due to the intermittent attacks behaviors. By studying more complicated attacks behaviors, it would help in devising more robust and effective IDS. In addition, understanding the significant of critical nodes in the networks would help not only in launching damaging attacks but also in the efforts to thwart such malicious attacks efficiently. For instance, implementing attacks prevention and detection mechanisms on critical nodes and not on all of the nodes in the networks may be cost effective, such that it reduces the computational costs of these resource scarce networks. In future work, we plan to employ few detection algorithms on critical nodes and study their effectiveness in detecting our proposed black hole attacks in MANETs.

6. REFERENCES

Broch, J., D.A. Maltz, D.B. Johnson, Y.C. Hu and J. Jetcheva, 1998. A performance comparison of multi-hop wireless ad hoc network routing protocols. Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, Oct. 25-30, ACM Press, New York, USA., pp: 85-97. DOI: 10.1145/288235.288256

Huang, Y.A., W. Fan, W. Lee and P.S. Yu, 2003. Cross-feature analysis for detecting ad-hoc routing anomalies. Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, May 19-22, IEEE Xplore Press, pp: 478-487. DOI: 10.1109/ICDCS.2003.1203498

Johnson, D.B. and D.A. Maltz, 1996. Dynamic Source Routing in Ad Hoc Wireless Networks. In: Mobile Computing, Imielinski, T. and H. Korth (Eds.), Springer, ISBN-10: 0792396979, pp: 153-179.

Karygiannis, A., E. Antonakakis and A. Apostolopoulos, 2006. Detecting critical nodes for MANET intrusion detection systems. Proceedings of the 2nd International Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing, Jun. 2-29, IEEE Xplore Press, Lyon, pp: 7-15. DOI: 10.1109/SECPERU.2006.8

Kurosawa, S., H. Nakayama, N. Kato, A. Jamalipour and Y. Nemoto, 2007. Detecting blackhole attack on AODV-based mobile ad hoc networks by dynamic learning method. Int. J. Netw. Security, 5: 338-346.

Lee, G., J. Seo and D. Kim, 2008. An approach to mitigate wormhole attack in wireless ad hoc networks. Proceedings of the International Conference on Information Security and Assurance, Apr. 24-26, IEEE Xplore Press, Busan, pp: 220-225. DOI: 10.1109/ISA.2008.44

Osathanunkul, K. and N. Zhang, 2011. A countermeasure to black hole attacks in mobile ad hoc networks. Proceedings of the IEEE International Conference on Networking, Sensing and Control, Apr. 11-13, IEEE Xplore Press, Delft, pp: 508-513. DOI: 10.1109/ICNSC.2011.5874910

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, Feb. 25-26, IEEE Xpore Press, New Orleans, LA., pp: 90-100. DOI: 10.1109/MCSA.1999.749281

Shivashankar, B.S. and G. Varaprasad, 2012. Identification of critical node for the efficient performance in MANET. Int. J. Adv. Comput. Sci. Applic., 3: 166-171.

Stamouli, I., P.G. Argyroudis and H. Tewari, 2005. Real-time intrusion detection for ad hoc networks. Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Jun. 13-16, IEEE Xplore Press, pp: 374-380. DOI: 10.1109/WOWMOM.2005.85

Thachil, F. and K.C. Shet, 2012. A trust based approach for AODV protocol to mitigate black hole attack in MANET. Proceedings of the International Conference on Computing Sciences, Sept. 14-15, IEEE Xplore Press, Phagwara, pp: 281-285. DOI: 10.1109/ICCS.2012.7

Wu, B., J. Chen, J. Wu and M. Cardei, 2010. A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks. In: Wireless Network Security, Xiao, Y., X. Shen and D.Z. Du (Eds.), Springer, New York, ISBN-10: 1441939199, pp: 103-135.

Yerneni, R. and A.K. Sarje, 2012. Secure AODV protocol to mitigate black hole attack in mobile Ad hoc. Proceedings of the 3rd International Conference on Computing Communication and Networking Technologies, Jul. 26-28, IEEE Xplore Press, Coimbatore, pp: 1-5. DOI: 10.1109/ICCCNT.2012.6396040