Evaluation the Performance of Delay Tolerant Network Protocol with Black Holes Attack

Alaa Hassan [a], Wafa Ahmed El Gali [b]

[a] University of Kirkuk, Kirkuk, Iraq

eng.alaa.hassan@ieee.org

[b] United Arab Emirates

welgali@gmail.com

Abstract: The Delay Tolerant Network (DTN) is one of the most challenging networks due to its features of heterogeneity, long delay, frequent dis-connectivity and opportunistic routing. There is no instantaneous path existing from source to destination. The traditional protocols and MANET protocols fail to work properly in such an environment. Thus, DTN overcomes this challenging problem using a store-carry-forward paradigm to increase message delivery probability. Due to the sparse connectivity nature of DTN, it becomes vulnerable to attack, such as Black Hole attack. In this paper, we evaluate the performance of the DTN protocol in the present of the attack. Moreover, we develop behaviors of Black Hole attack using ONE simulator. Different experiments have been conducted to compare the performance of the epidemic protocol in the present of this attack, and we explore how different mobility patterns of nodes in terms of the speed, movement type and direction, and different range of black holes influence successfully delivery ratio, average latency, and overhead ratio. The results showed that delivery probability for the epidemic routing protocol decreased considerably by 29% when the entire network is infected by a Black Hole attack and reduced the overhead ratio by 11%. The average latency fluctuates and depends on the percentage of attackers.

Keywords: Black Hole, Delay Tolerant Network, Mobile Ad Hoc Network, Dynamic Source Routing.

1 INTRODUCTION

Traditionally, networks are designed to connect nodes whereby there is a continuous, bidirectional, end-to-end path existing between source and destination. The links connecting these nodes provide low latency and error rate. The messages will be buffered for a certain short time to avoid a buffer overload, which can cause message drops. The message is then forwarded to the destination or the next hop. Employing this paradigm when designing wireless networks may fail to work probably. Whereby challenging environments, such as wildlife tracking sensor networks, vehicular ad hoc networks [1] [25], interplanetary deep space, military networks and underwater sensor networks [2] [26] are sparse wireless networks. Moreover, they suffer from long delay, frequent disconnectivity due to high nodes mobility, and high error rates. As a result, under these conditions, wireless networks become extremely intermittent and the existence of an end-to-end path from source to destination is never guaranteed [3] [27].

The Black Hole attack represents one of the security issues, which threaten DTNs and degrades their performance. The major objective of this paper is to represent and simulate a

Black Hole attack in the ONE simulator, where the existing simulator lacks security issues. In addition, the DTN routing protocols' performance is analyzed. The evaluation of the epidemic routing protocol performance measures is based on three metrics: success delivery probability, message average latency and overhead ratio to deliver the message to destination. The main objectives can be divided into: 1) design and implement Black Hole attack behavior by extending the existing simulator. 2) study the impact of Black Hole attack; compare the performance of the epidemic routing protocol, when the network is compromised by malicious nodes and then without Black Hole nodes using different movement patterns and various range of black holes. In this paper, we are interested in studying the performance of some routing protocols in the DTN; where, the end-to-end path does not exist and is difficult to predict. However, communications between nodes can occur. In addition, we are also interested in investigating the Black Hole attack and its influence on the performance of the network. The rest of the paper is organized as follows: Section II represents the related work on DTNs, DTN routing protocols, DTN routing attack, and DTN security. Section III describes the adopted methodology throughout this research. Section IV includes design and implementation of black hole behavior by extending ONE simulator, where the proposed work and the extended simulator are explained. Section V is an evaluation and discussion about the results of behavior of black hole attack and its influence on DTN performance. Finally, the paper is concluded in Section VI.

2 RELATED WORK

In this section, we shed light on the work done by researchers on DTN and security issues. Since DTN is an extension of MANETs, we therefore briefly highlight work done on MANETs as well.

Routing protocols in MANETs have been classified into two groups which are adapted from [4] [28]. AODV and DSR are examples of reactive protocols. They maintain routing information only between nodes, which want to communicate [5]. Due to lack of pre-existing infrastructure, the routing information becomes vulnerable to some attacks, such as a Black Hole attack. A Black Hole will try to route false information, disrupt the discovery of the route (path), or advertise itself as having the shortest path using the routing protocol [6]. Therefore, with the need for securing MANETs, many researchers sought to secure routing protocols, such as DSR, AODV and Destination-sequenced distance vector (DSDV), since these protocols were initially developed devoid of security features. Another study by [5] proposed two mechanisms to secure the AODV protocol using digital signatures for authentication and hash chains for hop counts. K. Selvavinayaki et al. have presented a solution to prevent Black Hole attack by using security certificates in digital form [7]. Moreover, a survey by R.A. Raja Mahmood et al. presented seven methods to detect Black Hole attack in MANETs [8].

Although DTNs and MANETs share common properties, they differ from each other in the way they handle messages. In MANETs, the communication between nodes is possible only if the path exists to the destination; routing protocols, such as DSR and AODV [9] [25], assume the existence of the complete path from the source to the destination before sending messages. In addition, nodes have short usage time, which means the message could be lost easily. Moreover, the high mobility of the nodes in MANETs can cause loss of messages. When a message arrives at the node, and if there is no end-to-end contemporaneous path to the destination, the message will be dropped; this results in lost messages. Therefore, [10], [11] and [12] consider that these protocols fail to work properly in a DTN. On the other hand, DTNs allow communication between intermittently connected nodes, even if there is no pre-existing path to the destination. Using the existing DTN routing protocols, a new approach has been developed in order to overcome the problem of losing messages and to enable routing in the DTNs [2]. The approach is called "store-carry-forward", where the message can be held for a long time by the node (hours and sometimes days) until it encounters another relay to forward the message to, and so on, it reaches its destination. All the DTN routing protocols follow the "store-carry-forward" paradigm, which increases the delivery probability of the message. This distinguishes DTN from other traditional networks and makes it more challenging as its tolerance is quite long.

Jain et al. explain the DTN routing problem, where a message is to be sent end-to-end, on a time-varying directed multi-graph [11]. There may be more than one edge existing between two nodes, because of the availability of different links at different times. Routing decisions can be made based on the information available about the connection and the mobility of the nodes. However, sometimes such information may not be available or known to the nodes.

In recent years, some of the studies started to consider security when designing routing algorithms. However, they did not get adequate attention until now. As pointed out previously in the first chapter, one of the DTN challenges is providing efficient routing due to its nature of intermittent connectivity of the nodes, lack of stable connection between source and destination, and low nodes density [13].Thus, the DTN becomes vulnerable to a number of attacks, such as Black Hole attack [29] [30].

The Black Hole attack is one of the active routing attacks, where a compromised node can use fake information in the routing table, such as message delivery probability to increase its chance of being selected as the next hop node to deliver a message. Once a fake route has been established, it receives messages from other nodes, and it is then able to drop messages or utilize them to launch other attacks [14]. In traditional networks and MANETs nodes utilize evidence, such as temporal leashes [15], to detect such an attack. However, in a DTN such evidence is extremely difficult to collect. A Gray Hole attack [16] is one of the routing attacks. It has two phases, wherein the first phase, a node advertises itself to have the shortest path to the destination [17]. In the second phase, it drops messages received from a specific source or forwards these to a certain destination. However, this attack is considered more difficult in detecting than a Black Hole attack, because the drop process occurs with a certain probability.

In [18], Burgess et al. explain that a DTN is robust against the presence of malicious nodes, due to the opportunistic nature of DTN, which can reduce the negative effects of such attacks. The study shows that authentication mechanisms of securing routing are difficult to deploy and function in a DTN. Contrary to research by [18], the work in [19] studies the robustness of DTN against attack without authentication mechanisms. The study shows that replication-based routings can be exposed to attack if the authentication mechanisms are not used. This results in decreasing delivery probability. Another scheme called encounter tickets has been introduced by [15] to secure evidence of all contacts in the network. Malicious nodes can provide forged contact history to increase the likelihood of being selected by other nodes.

3 METHODOLOGY

This Section focuses on the technical tools, and the methodology, which have been used in this research.

3.1 Choice of the simulator

The Opportunistic Network Environment (ONE) simulator includes the traditional mobility models, and map-based model as well, which has the advantage of giving more realistic movement and results. The data provided by the Helsinki map allows simulation of the nodes movement when the nodes communicate with each other, then the contact information can be derived from the result of the simulation. On the other hand, this information can be derived using other approaches based on a random process. This approach gives values that may not be precise and difficult to prove because the behavior of the human not always random. Moreover, the information can be derived from real-world traces. Although this approach depends on real human interaction, it has problems related to the devices used to track people. Among these problems, the power for the devices is kept low to save battery life; therefore, the information may be not precise as well. In addition, the number of traces is limited [20]. The ONE simulator provides data from a real map (Helsinki map), where nodes can move along roads. Moreover, it provides diverse movement patterns, where trams, pedestrians, and cars can move on the roads. This data provides more realistic movement models. Therefore, the approach based on the simulation of nodes movement will provide more realistic results.

3.2 Simulation Scenario

A simulation scenario is constructed by defining node groups and their properties. This may include movement module, routing models, simulation time, interface type, world's size, event generator and other parameters. The parameters are defined in the configuration file "default_setting.txt ". Further simulation scenario settings are defined in a separate (optional) configuration file to add more settings or to override (some or all) settings in the default_settings.txt file. The behavior of all modules is implemented using the high-level language (Java). However, the behavior can also be adjusted in the comparison between batch mode GUI Mode Time 431.81 s 43200.1 s Speed 147.021/s 72.201/s 32 configuration file. Moreover, the simulator has a feature called run indexing, which is defined by the parameters in the configuration file. Thus, it can allow for sensitivity analysis. When the simulator starts, it reads "default settings" and takes the optional file if it exists as an input parameter. The result will be generated in the MessageStatsReport, which contains statistics about the simulation as mentioned before.

4 DESIGN AND IMPLEMENTATION

After gaining a deep understanding of the ONE simulator and reviewing its functionality, it is clearly noticeable that the current ONE simulator is capable of simulating a number of scenarios; however, it has some limitations in its design, as it does not provide the behavior required to simulate a Black-Hole attack. Based on our area of interest, which is studying the behavior of the Black Hole attack, thus there is a need to extend the simulator functionally to incorporate behavior of the Black Hole attack so that we can study and analyze malicious nodes' behavior.

Black Hole nodes act as malicious nodes, and in their behavior, will drop all the messages received from other nodes. This means that the nodes have to establish a connection first to provide communication with other nodes, and then start sending messages. Thus, as an initial idea for the design, it was suggested to implement the logic of Black Hole attack behavior when the node starts communication with the other nodes. After the connection is achieved, instead of forwarding a message, it will drop it. The abstract ActiveRouter class is the super class of all active routers, including the epidemic router. This class has a method responsible for checking if the host is ready for transferring based on the information available about the connection. Besides that, it checks if the transferring host is not a Black Hole so it can start transferring. Otherwise, it will drop the message. However, this approach depends on the connection between nodes, and since the connection can be affected by many factors, thus it may affect the transfer process and the result from this implementation may not be accurate. Thus, the idea of the design was directed to another approach. The MessageRouter Class has a method called createNewMessage. It is responsible for creating new messages in the router. If the creation process is done successfully, the method will return true. Otherwise, it returns false, for example, if the message size is too big to be carried in the buffer. Therefore, if the host (router) is a Black Hole, it would not allow the creation of the message. Otherwise, the creation process will be performed normally.

The DTNhost class is responsible for creating new hosts (nodes). Each host belongs to a specific group with a given groupID. Therefore, two methods need to be added to the class. One of the methods is responsible for checking if the created host (router) is acting as a Black-Hole (malicious node), and the other will control whether the message will be dropped or not. Since a Black Hole attack should not affect the message creation process, and should drop all incoming messages.

4.1 Implementation of the extended simulator

The ONE simulator lacks the representation of the Black-Hole behavior; therefore, a new Black-Hole Epidemic routing module has been implemented in order to provide behavior of the malicious nodes. In addition, a new feature in the MessageStatReport module has been added to give statistics about the messages dropped by Black-Holes.

The experiments to be conducted using the simulator include different groups. These groups are defined in the settings file. Each group consists of a number of nodes that vary from one group to another, as defined in the settings file. When conducting experiments, it is usually assumed that all the groups in the network are infected by a Black Hole attack. Therefore, in order to determine the percentage of the Black Hole attack by all groups or certain groups, a new property (key) with the percentage value of the Black Hole (percOfBlackHoles) has been defined in the setting file.

4.2 Black Hole Module

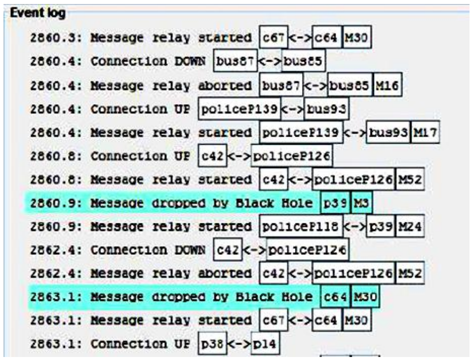
The ONE simulator makes extending and configuring of the simulator with different features easy for developers. Therefore, one of the goals when implementing the new code is to provide flexible code to facilitate the use of the extended simulator by other users. For this reason, the IBHRouter interface has been implemented in a separate package. It should be noted that when creating a new model, a new class has to be created [20] and the name of the class has to be defined in the setting file. When the scenario starts, the simulator will load the new configuration from the setting file automatically.

4.3 Message Listener

Message Listener is an interface for the classes, which want to be informed about message events; for example, the creation and deletion of messages. As in our implementation, the BHEpdiemic.java class contains the logic for handling Black Hole behaviors, which result in message drops. Therefore, message listener needs to be informed when a message is dropped.

4.4 Black Hole Attack Report

As pointed out earlier, the existing report generates information about the number of messages created, deleted, aborted, dropped, and relayed. Moreover, it gives information about the delivery probability, overhead ratio, and the latency. All these metrics are critical when analyzing behavior of the Black Hole attack, but do not provide any information about the Black Hole behavior in terms of the number of public boolean is BlackHole() public BHEpidemicRouter replicate() public void messageDroppedByBlackHole (Message aMessage, DTNHost where); dropped messages. Therefore, this report is extended to include new statistics about the number of messages dropped by Black Hole attack. It is notable that the number of dropped messages by Black Holes is always less than the total of dropped messages. In addition, in the event log panel within the graphical user interface, Black Hole events are displayed as shown in Figure 1.



```
Event log
  2860.3: Message relay started c67<->c64 M30
  2860.4: Connection DOWN bus87<->bus85
  2860.4: Message relay aborted bus87<->bus85 M16
  2860.4: Connection UP policeP139<->bus93
  2860.4: Message relay started policeP139<->bus93 M17
  2860.8: Connection UP c42<->policeP126
  2860.8: Message relay started c42<->policeP126 M52
  2860.9: Message dropped by Black Hole p39 M3
  2860.9: Message relay started policeP118<->p39 M24
  2862.4: Connection DOWN c42<->policeP126
  2862.4: Message relay aborted c42<->policeP126 M52
  2863.1: Message dropped by Black Hole c64 M30
  2863.1: Message relay started c67<->c64 M30
  2863.1: Connection UP p38<->p14
```

Fig. 1. Screen Shot from GUI Event Log Displaying Black Holes Events

5 EVALUATION AND DISCUSSION

After the design and implementation of the extended simulator, we conducted our experiments. In this section, we aim to focus on two parts. First, testing the performance of DTN routing protocols (Epidemic, Spray and Wait, Direct Delivery, First Contact, MaxProp and PRoPHET) in the present of Black Hole attack. Secondly, investigating and evaluating the effects of the Black Hole attack on the DTNs using the epidemic routing protocol.

5.1 Experiment aims and set up

The main aim of the following experiments is to explore the influence of Black Hole attack on DTNs. Therefore, many scenarios and experiments have been conducted to analyze and explore the effect of such attack. It is assumed that all groups communicate with each other, one (could be more or the entire group) of the groups behaves as a malicious group in order to prevent communication between other groups by dropping messages. For instance, the pedestrian group communicates with the bus group, while the attack source is from the third group (cars). As a result, it is expected that the malicious group will affect the communication between the other groups. Hence, there is no technique to detect this attack.

In order to evaluate the effect of Black Hole attack in a DTN, three realistic movement models have been used, namely *MapBasedMovement*, *ShortestPathMapBasedMovement* and *MapRouteMovement* models. The movements are in Helsinki city to give accurate results and closer to reality. The simulation space is an open area with dimensions (4500m × 3500m). Six groups have been created with 140 nodes in total. It is highly preferred to use a reasonable density of nodes, as this can affect the overall connectivity of the network, and thus affect message delivery ratio [21]. The groups have both common and specific settings. Groups include two groups of pedestrians with 40 nodes for each group; a bus group with 20 nodes; two groups of trams with 5 nodes in each group; and the last group comprising police patrols with 30 nodes.

The groups move in the map paths, which are roads and tram lines. The roads are specified for the cars, which use *MapBasedMovement* (road traffic), buses follow *MapRouteMovement* (with predefined routes and scheduled trips inside Helsinki city) and pedestrians move using *MapBasedMovement* (footpaths). The cars can only drive on the roads at 10-50 Km/s with waiting times of 10–120 seconds. The police patrol group uses *shortestPathMovement*. The *ShortestPathMovement* is used to represent how patrols move around the city, while they randomly drive around and stop for a few moments. The trams move at 25–36 km/h with pause times of 10–30 s in the predefined routes.

Three metrics have been considered in order to evaluate the performance of the network when it is under Black Holes attack, and also when there are no attacks. The metrics are *success delivery probability and average latency* which is defined as a delay in the message transfer from one node to another in specific time [22], [18], [23], and c) *overhead ratio*. These metrics are critical in measuring the performance of the DTN routing protocols and the effect of the Black Hole attack in the network. The overhead ratio is an interesting metric to be evaluated as well. Since we are exploring the effect of the Black Hole attack, this attack has a significant impact in the number of messages created and delivered.

5.2 Black Hole Attack

Our goal from the experiments is to observe changes in the delivery probability, and the average latency when the percentage of Black Hole nodes increases and decreases. We choose malicious nodes randomly to act as Black Holes with the percentage of 10%, 25%, 50% and 100%. 100% indicates that the entire network is infected with the Black Hole attack.

We are going to test different scenarios where for example the attack comes from the pedestrians Group, and this group communicates with the other groups in the network. It is expected that delivery probability will decrease as this group will deny forwarding messages to the other groups by dropping all messages. It is worth mentioning that the Black Hole attack implemented in this project is behaving randomly, where the number of attackers in each group is random. However, the level of the attack can be customized by changing the percentage of the attack.

5.3 Protocols Performance

First, the performance of the original DTN routing protocols including epidemic, spray and wait, and direct delivery protocols was studied in the present of attack. The protocols performance can be measured by evaluating three metrics: 1) successful delivery rate 2) average latency 3) overhead ratio. Table (1) shows a summary of the message statistics report of six routing protocols.

Table 1: Message Statistics Report for DTN routing protocols

Stat. Metric	Epidemic	SW	MaxProp	DD	FC	PRoPHET
Created	1465	1465	1465	1465	1465	1465
Started	264914	26301	351596	761	34556	293816
Relayed	242173	11012	328294	274	17448	273073
Aborted	22737	15288	23295	487	17106	20739
Dropped	240973	9839	312394	888	914	272001
Dropped by BH	0	0	0	0	0	0
Removed	0	0	14778	0	17448	0
Delivered	419	616	750	274	233	425
Delivery_prob	0.2860	0.4205	0.5119	0.1870	0.1590	0.2901
Overhead_ratio	576.9785	16.8766	436.7253	0.0000	73.8841	641.5247
Latency_avg	5880.1585	4713.4021	5943.1000	6697.8858	6041.3545	0.2901

Figure 2 presents a comparison of message delivery probability between DTN routing protocols. It is clearly observed that MaxProp delivers significantly greater message delivery percentage than other protocols at 51%. The reason is that MaxProp uses several mechanisms in order to increase delivery rate. As pointed out earlier in Section II, it uses a technique of PRioritized message send and delete process. This was closely followed by the spray and wait protocol, which restricts the number of message copies in order to increase delivery percentage. In our experiment, we considered 10 copies in replication, which results in increasing the delivery probability of the protocol to 42%. PRoPHET and Epidemic protocols are almost the same in delivering messages. However, PRoPHET is slightly superior as it is able to deliver more messages with a lower communication overhead, because it follows probabilistic routing (Figure 4) as it can be clearly seen, the overhead ratio for the Epidemic of 576.9785 decreased dramatically to 0.2901 for PRoPHET. Finally, Direct Delivery and First contact are single-copy based protocols, and they had the smallest delivery percentage, 19% and 16% respectively.

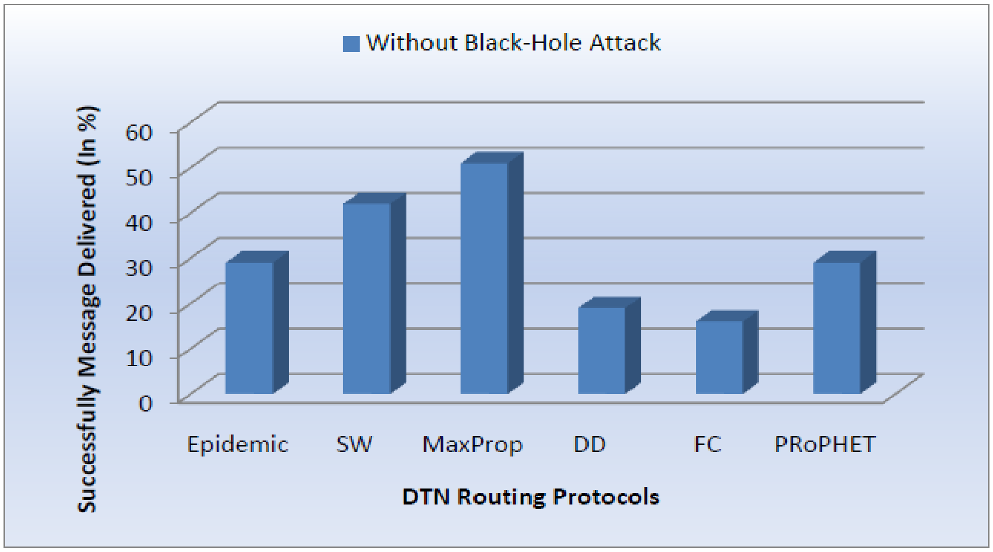


Fig. 2. Delivery Probability for DTN Protocol

Figure (3) shows a comparison of message average delay between DTN routing protocols. It can be observed that the direct delivery protocol has the highest average latency. Since this protocol is a single-copy based protocol, where only one copy of the message exists in the network and is forwarded to the destination only when the source communicates directly with the destination [24]. However, this probability is very low in a DTN. Therefore, the result makes sense. However, it is clear that the epidemic routing protocol has smaller average latency than direct delivery due to unlimited replication of the messages in the network to deliver the message with high probability. On the other hand, spray and wait protocol with controlled number of message copies has the smallest average latency.

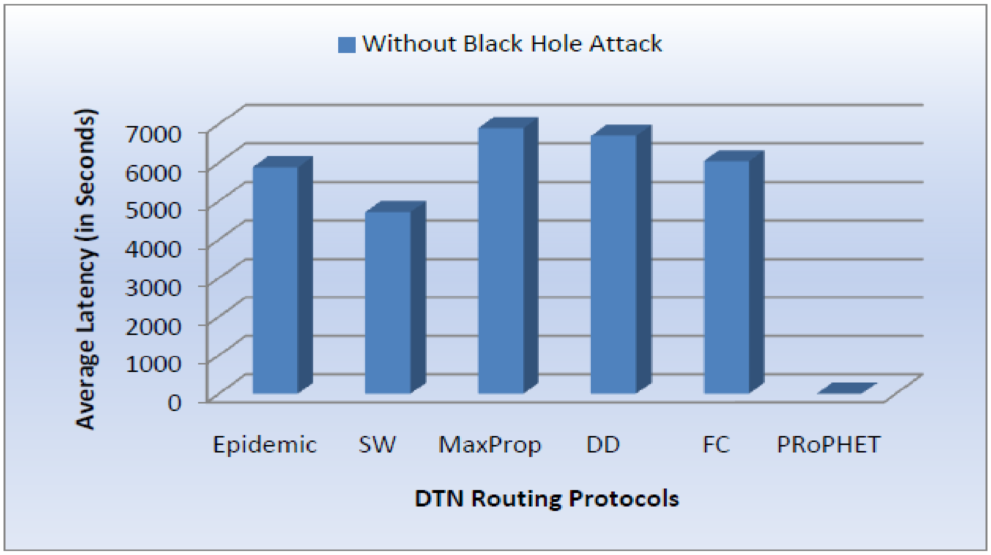


Fig. 3. Average latency for Three Protocols without Existing of Black Hole Attack

Figure (4) compares the overhead ratio for DTN protocol, it can be seen that the Epidemic protocol has the highest overhead (576.97), as this protocol floods an unlimited number of message copies. However, this ratio drops markedly for the spray and wait protocol to 16.87 as this protocol floods a controlled number of message copies. Followed by the single-based protocol direct delivery with zero overhead, where this protocol uses only one copy to deliver to its destination, and so only one copy is available in the network. The prediction-based protocol (PRoPHET) has the lowest overhead ratio (0.29) after direct delivery.

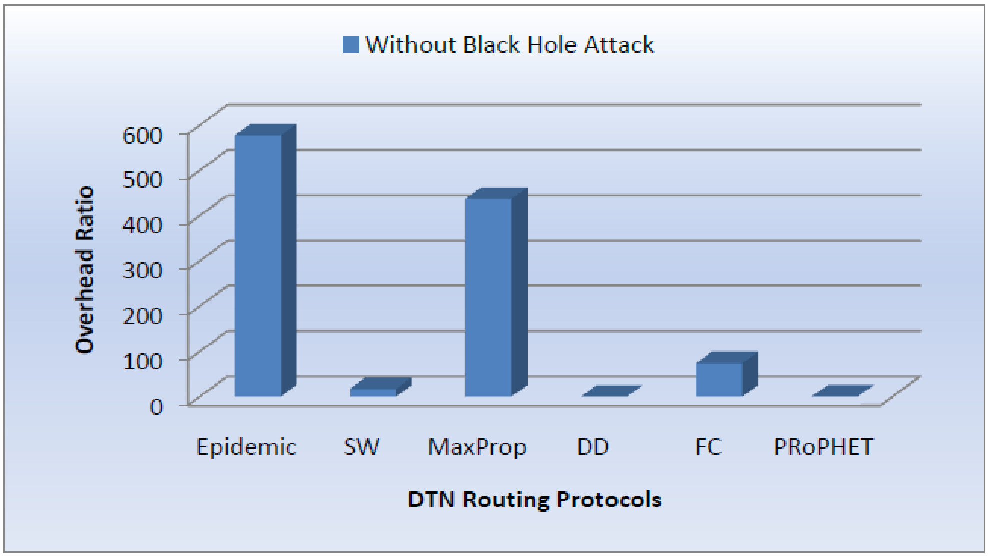


Fig. 4. Overhead Ratio for DTN Routing Protocols.

5.4 Black Hole Attack Evaluation Criteria

In order to compare the performance of the epidemic routing protocol in both scenarios, when trust between nodes is limited (under Black Hole attack) and without atta`k, it is important to present metrics to evaluate performance. Below, two important metrics, successful message delivery probability, and the average latency are explained.

5.5 Message Delivery Ratio

In order to evaluate the effect of Black Hole attack, it is extremely important to measure message delivery probability. It is rare to lose a message in the DTN environment, but the situation will be different under the influence of a Black Hole attack.

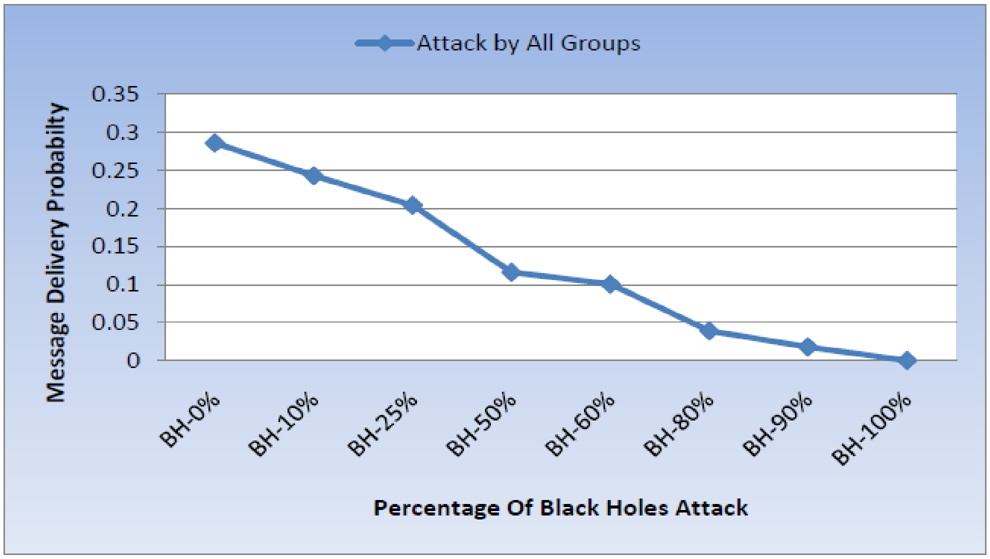


Fig. 5. Delivery Probability for Epidemic Protocol under Black Hole Attack

Figure (5) shows the effect of the Black Hole attack on message delivery probability for the epidemic protocol. The results present different percentages of the attacker. According to the graph, it can be observed that there is a significant decrease in delivery probability. Where for the entire network infected by Black Hole attack (percentage of the attack = 100%), all the nodes drop all messages, the delivery probability drops dramatically from 0.27 (with 0% attack) to 0.00 (with 100% attack). On the other hand, if 10 - 100% of the nodes in a certain group in the network act as Black Holes, the average successful delivery rate will decrease. This result shows that the throughput of the network can significantly degrade when a Black Hole attack exists.

5.6 Average Latency

The average latency has a special importance in the DTN. It indicates network speeds and time between message creation and when it is received by its destination. Therefore, average latency can be measured based on groups' buffer size and the number of nodes in these groups. Since DTN suffers from long delay due to its challenging nature in routing messages, therefore, it is expected to have a high average latency.

Figure (6) illustrates the impact of the Black Hole attack on the average latency for the epidemic routing protocol. It can clearly be noticed that the average latency is slightly increased when the percentage of the Black Hole attack increases. In the case of 25% of node groups acting as Black Holes, the average latency increases by about 300 seconds, from

5521.0476 seconds for a 10% attack to 5884.2181 seconds for a 25% attack. The overall trend in the average latency consistently increases by about 200 seconds for every 10% increase in attack.

It can be argued that the overall trend of the graph for epidemic routing is fluctuating. There is a peak at 6642 seconds at near 60% attack. However, the delay drops to (5610) seconds at near 90% attack. It has also been noticed that when the percentage of attack is 100%, the result of this attack is that no message is delivered. Therefore, the value for average latency is unavailable as message average latency is counted based on delivered message.

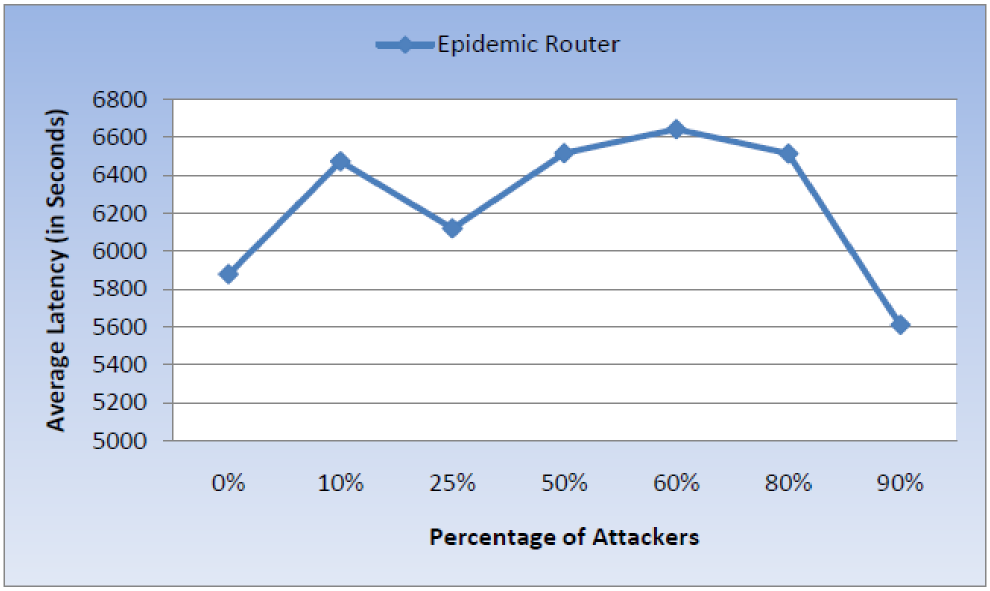


Fig. 6. Average Latency of Epidemic Router under Black Hole Attack

5.7 Impact of number of Black Holes within all groups

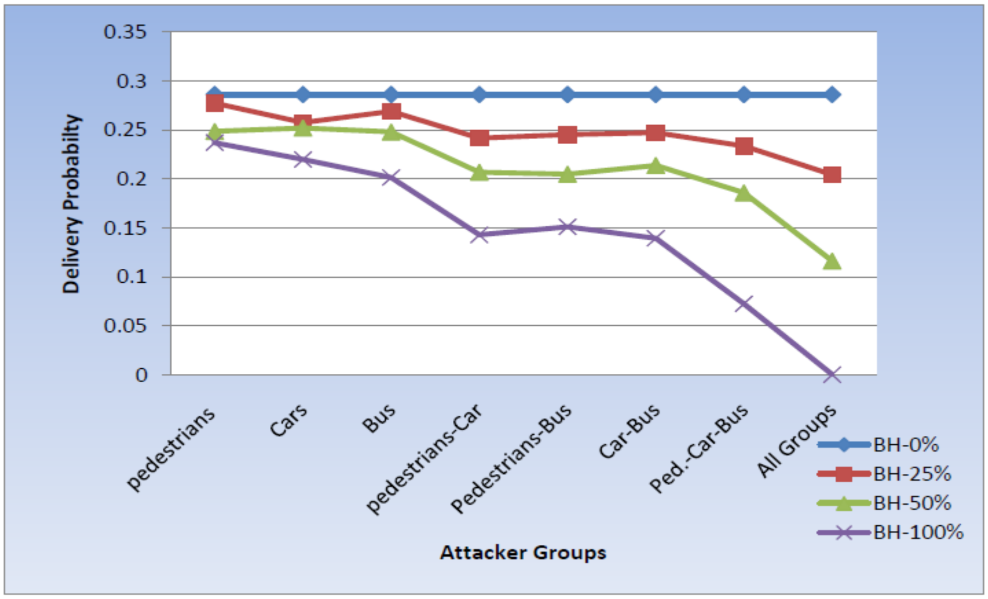


Fig. 7. Delivery Probability under Black Hole Attack from Certain Groups

Figure (7) shows the percentage of message delivery when the network is under Black Hole attack. When the percentage of Black Holes is 0% (no attack), the percentage of successful delivery is about 28 %. It is observed that there is a slight decrease from 28% to 25% in the percentage of messages delivered when the percentage of Black Holes is 10%. At 50%, where all nodes group are compromised by Black Hole attack, the delivery percentage drops sharply to 15%. As a result, it can be seen that the Epidemic routing protocol is vulnerable in the face of Black Hole attack.

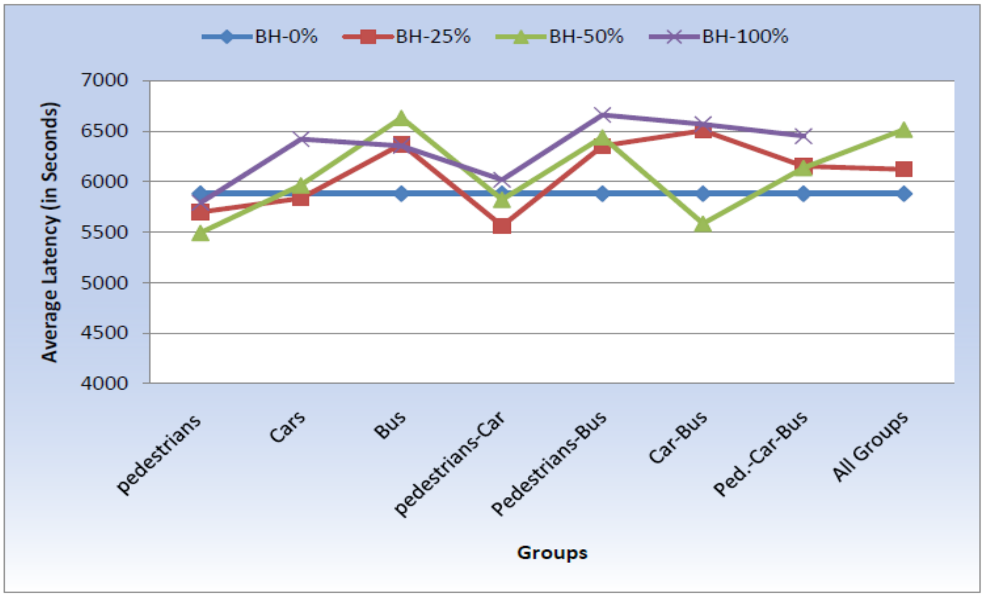


Fig. 8. Average Latency under different Levels of Attack

Figure (8) shows message delay for all groups under different levels of attack. It is observed that when Black Hole percentage is 100% in all groups, the delay remains the same. However, when the percentage of attack varies within the group, it is clearly observed that the overall trend of the graph of message delay fluctuated, and it has no stable pattern.

5.8 Impact of percentage of Black Holes within certain groups

On the other hand, since Black Hole attack affects the whole network, this means that when the attack comes from one group within the network all the other groups will be affected by it. Therefore, one of the aims is to analyze and evaluate the effect of such an attack, originating from certain groups in the network, while others are not compromised. As pointed out previously, it is assumed in the first scenario that the source of the attack comes from group1, which represents pedestrians (p) with different percentage levels of attack. The second scenario considers the attack source is the car group (c). The last scenario is where the bus group acts as a malicious group. It was also assumed that the police patrol and tram groups do not attack the network. Figure (8) shows the influence of a Black Hole attack, when it comes from pedestrians, car and bus groups (each group separately) on the delivery probability. It is clearly observed that the number drops slightly from 0.2771 with 25% of the pedestrian nodes group acting as Black Holes to 0.2369, where this group is 100% compromised by a Black Hole attack, which means preventing messages being sent. Similarly, when the attack source comes from the bus group, the delivery probability decreases by slightly more than the pedestrian and car group from 0.2698 (with 25% attack) to 0.2014 (100% attack).

On the other hand, the same figure illustrates the probability of delivery for epidemic router under Black Hole attack from more than one group. It can be clearly seen that whenever the number of Black Hole groups increase, the decline in delivery probability is far greater. However, the different sources of Black Hole attack made for a relative decline as a percentage is varied. From this result, it can be concluded that the epidemic protocol is vulnerable to Black Hole attack.

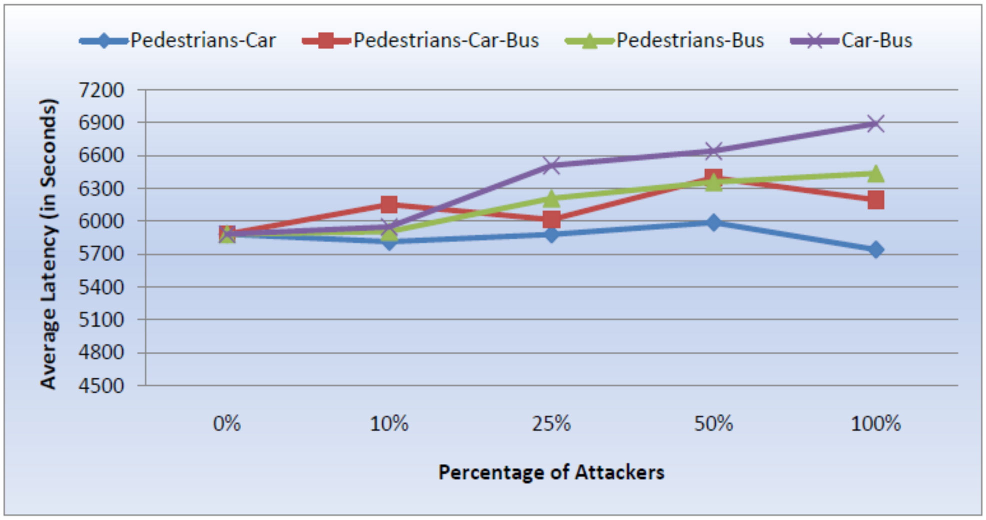


Fig. 9. Average Latency for Epidemic Protocol under Black Hole Attack from Certain Groups

Figure (9) shows when Black Hole nodes are selected from different groups (from pedestrians and car groups, or pedestrians and bus groups, or pedestrians, car, and bus groups). When the attack source, for example, is from the car and bus groups, the average latency consistently increased as the percentage of attack increased; from 5946.9803 seconds with 10% attack to 6889.8568 with 100% attack. Moreover, there was a slight increase between (20 – 150 seconds) per each level of attack, where the attack source is from pedestrians and bus groups. The delay remains almost the same when the number of attacking nodes grows in pedestrians and car groups, but fluctuates when it comes from three groups.

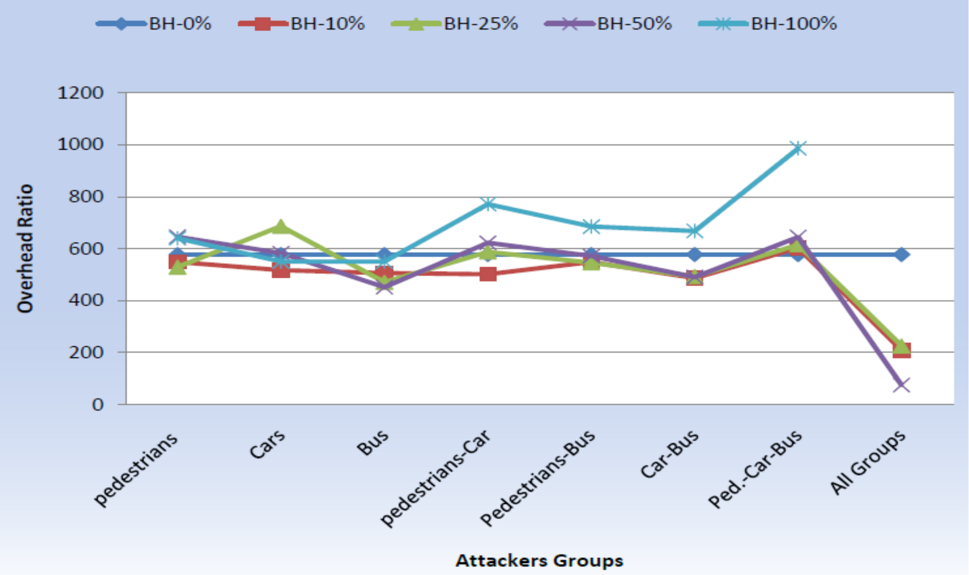


Fig. 10. Overhead Ratio under Black Hole Attack from Different Groups

On the other hand, figure (10) shows the overhead ratio of the epidemic protocol is not affected by a Black Hole attack when the source of attack comes from certain groups. It almost remains the same, and may increase and decrease by 1-2% with different levels of attack. However, the proportion is dramatically decreased by 8% (from 576.9785 at 0% attack to 74.7176 at 50% attack). However, when the entire network is infected by a Black Hole attack, the overhead is negligible, as there is no resources consumption to deliver messages to destinations because all messages are dropped.

5.9 Total Message Drop/ Drop by Black Hole

When a message arrives at a node, the node becomes subject to a number of tests, including the Black Hole test. If it is a Black Hole, the message will be dropped. Otherwise, it will be added to the buffer. Accordingly, messages dropped by Black Holes will usually be less than the total dropped. It can be observed from the figure (11) that when the percentage of attack is 0, the total drop is 240973, where the drop by Black Holes is 0. For a 25% attack, the total drop for other reasons is 508027, and the drop by a Black Hole is 440895. Therefore, it is more likely, when the percentage of attack increases, that the number of dropped messages by Black Hole rapidly increases from 0 to 867800 message (at 100% attack), where the observed total drop is always greater than the drop by Black Holes.

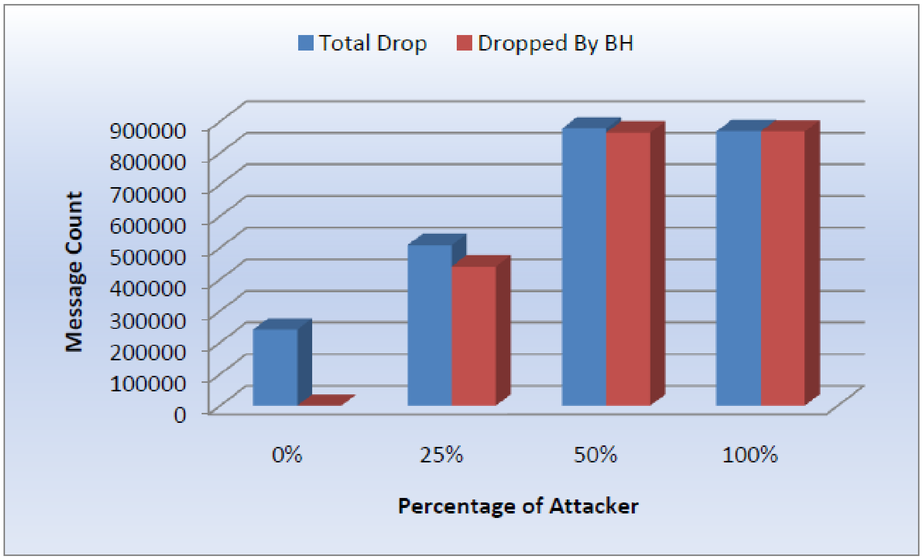


Fig. 11. Total Message Drop/ Drop by BH Ratio

The simulation results show that the epidemic routing protocol performs well in terms of delivering messages with reasonable average latency and high overhead ratio compared to other DTN routing protocols. However, the performance of the protocol in delivering messages is dramatically degraded under Black Hole attack. The percentage of messages delivered decreased as the percentage of attack increased. Moreover, the overhead ratio is considerably decreased in the presence of the attack. On the other hand, the latency for the protocol fluctuates under such attack. These results showed that the Epidemic protocol is vulnerable in the face ofsuch attack.

6 CONCLUSION

Most of the DTN routing protocols consider delivery probability as a primary metric in routing. Such a metric can be abused by malicious nodes to launch a Black Hole attack causing a high proportion of message drop. In this paper, we have evaluated the performance of DTN routing protocol in the present of Black Hole attack, including the epidemic protocol. The evaluation is based on three metrics in terms of delivery probability, average latency, and overhead ratio. We have noticed that the MaxProp routing protocol delivers a significantly greater message percentage than other protocols at 51%, followed by spray and wait at 42%, while the epidemic protocol delivers 29%. On the other hand, we have considered the results of the Epidemic routing protocol as a baseline and addressed the Black Hole attack problem. On this basis, we have developed and implemented a new epidemic routing module using the ONE simulator. A router is supposed to behave as malicious node (Black Hole) and deliberately drop all the messages. We have investigated the impact of the Black Hole attack in the DTN environment. A number of experiments and different scenarios have been conducted using the epidemic routing protocol, including an attack from all, as well as specific, groups. We have explored how different mobility patterns of nodes in terms of the speed, movement type, direction of movement and range of black holes influence the successful delivery ratio, average latency, and overhead ratio. From the results, it has been noted that the epidemic protocol, which floods an uncontrolled number of message copies is susceptible to Black Hole attack. This attack has a negative effect on the performance of epidemic protocol in terms of successful message delivery probability, average latency, and overhead ratio. Moreover, these metrics are also influenced by the percentage of attackers. It has also been observed that this attack dramatically decreased delivery probability when the percentage of attackers increased due to the large amount of message drops. The result showed message delivery percentage declined by about 29% where the entire network is infected by the attack. Moreover, the result showed delivery probability decreased by between 5 – 9% when the source of attack is selected from one group and declined to between 15 – 16% when the attack came from two groups. It also drops by 22%, when the 62 attack originated from three groups. On the other hand, the message delay for the epidemic protocol under Black Hole attack remains almost the same when the number of attacking nodes grows in one group. However, it fluctuates when it comes from three groups. The overhead ratio of the epidemic protocol is not affected by a Black Hole attack when the source of attack comes from certain groups. It remains almost the same, and may increase and decrease by 1-2% at different levels of attack. However, the proportion is dramatically decreased by 8% (from 576.9785 at 0% attack to 74.7176 at 50% attack). However, when the entire network is infected by a Black Hole attack, the overhead is negligible, as there is no resources consumption to deliver messages to destinations because all messages are dropped. The present findings clearly indicate how one of the DTN routing protocol, "Epidemic", is vulnerable in the face of a Black Hole attack.

Acknowledgments

We would like to express our sincere gratitude and thanks to the Professor Dr. Ibrahim El-Emary,Ph.D in computer science and systems, University of king Abdul Aziz, KSA for his continuous support, cooperation, and assistance.

References

[1] S. Rashid, Q. Ayub, M. S. M. Zahid and A.H. Abdullah, "*Impact of Mobility Models on DLA (Drop Largest) Optimized DTN Epidemic routing protoco"*. 5, March 2011, International Journal of Computer Applications, Vol. 18, pp. 35-39.

[2] T. Spyropoulos, K. Psounis and C. S. Raghavendra, "*Efficient Routing in Intermittently Connected Mobile Networks" : The Multiple-Copy Case.* IEEE/ACM, February 2008, TRANSACTIONS ON NETWORKING, Vol. 16, pp. 77-90.

[3] M. J. Khabbaz, C. M. Assi and W. F. Fawaz, "*Disruption-Tolerant Networking:A Comprehensive Survey on Recent Developments and Persisting Challenges"* : IEEE COMMUNICATIONS SURVEYS & TUTORIALS, 2011.

[4] S. Dokurer, " *SIMULATION OF BLACK HOLE ATTACK IN WIRELESS AD-HOC NETWORKS".* Computer Engineering : Atilim University, 2006. Master Thesis.

[5] M. G. Zapata and N. Asokan, "*Securing Ad hoc Routing Protocols".* Atlanta, Georgia, USA. : In WiSe'02, 2002.

[6] M. AlShurman, S. Yoo and S. Park, " *Black Hole Attack in Mobile Ad Hoc Networks".* Huntsville, AL, USA. : ACM press, April 2004. In the proceedings of The 42nd annual Southeast regional Conferene. pp. 96-97.

[7] K.Selvavinayaki, K.K.Shyam Shankar and E. Karthikeyan, "*Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs".* 11, U.S. : Foundation of Computer Science, October 2010, International Journal of Computer Applications, Vol. 7, pp. 15-19.

[8] R.A. Raja Mahmood, A.I. Khan, "*Survey on Detecting Black Hole Attack in AODV based Mobile Ad Hoc Networks"*. Australia : In the Proceedings of 4th International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET2007), 2007. IEEE CONFERENCES. pp. 1-6.

[9] D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks". [ed.] T. Imelinsky H.Korth. *Mobile Computing.* Pittsburgh, PA : Kluwer Academic Publishers, 1996, Vol. 535.

[10] S. Burleigh and K. Fall, "*Delay tolerant networking: An approach for interplanetary internet"*. 6, Pasadena, CA, USA : IEEE Communications Magazine, June 2003, Vol. 41, pp. 128-136.

[11] S. Jain, K. Fall, and R. Patra, "*Routing in a Delay Tolerant Network.* New York" : In Proceedings of the 2004 conference on Applications, technologies, architectures, and protocols for computer communications(SIGCOMM '04), 2004. pp. 145-158.

[12] Z.Zhang, "*Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks : Overview and Challenges"*. 1,: IEEE Communications Surveys & Tutorials, 2006, Vol. 8, pp. 24-37.

[13] E. Bulut and B. K. Szymanski, "*On Secure Multi-copy based Routing in Compromised Delay Tolerant Network"s.* Hawaii : In 20th IEEE International Conference on Computer communication and Networks ICCN, July 2011.

[14] Y. Ren, M. C. Chuah, J. Yang and Y. Chen, " *Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording"*. Montreal : In11th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, WOWMOM 2010, 2010. pp. 1-6.

[15] F. Li, J. Wu and A. Srinivasan, "*Thwarting blackhole attacks in disruption-tolerant networks using encounter tickets"*. Rio de Janeiro, Brazil : In IEEE INFOCOM 2009 - The 28th Conference on Computer Communications, 2009. pp. 2428-2436.

[16] R. H. Jhaveri,A. D. Patel, J. D. Parmar and B. I. Shah, "*MANET Routing Protocols and Wormhole Attack against AODV"*. 4: IJCSNS International Journal of Computer Science and Network Security, April 2010, Vol. 10.

[17] J. Sen, M. G. Chandra, H. S.G., H. Reddy and P. Balamuralidhar, "*A Mechanism for Detection of Gray Hole Attack in Mobile Ad Hoc Networks"*. Bangalore : Embedded Systems Research Group, 2007.

[18] J. Burgess, G. D. Bissias, M. Corner, and B. N. Levine, "*Surviving Attacks on Disruption-Tolerant Networks without Authentication"*. Canada : In Proceedings of MobiHoc’07, 2007. ACM.

[19] F. C. Choo, M. C. Chan and E. Chang, "*Robustness of DTN against Routing Attacks"*. Singapore : in Proceedings of Second International Conference on Communication Systems and Networks (COMSNETS), 2010. pp. 1-10.

[20] Keranen, Ari, "*Opportunistic Network Environment Simulator"*. Communications and Networking : Helsinki University of Technology, 2008.

[21] A. Keranen and J.Ott, " *Increasing Reality for DTN Protocol Simulation"*. Networking Laboratory: Helsinki University of Technology, 2007. Technical.

[22] J. Kong, X. Hong, Y. Yi, J.-S. Park, J. Liu, and M. Gerla, "A secure ad-hoc routing approach using localized self-healing communities" . Illinois : In Proceedings of MobiHoc’05, 2005. 6th ACM international symposium on Mobile ad. pp. 254-265.

[23] A. Lindgren, A. Doria, and O. Schelen, "*Probabilistic Routing in Intermittently Connected Networks"*. Korea : In Proceedings of SIGMOBILE Mobile Computing and Communication Review, 2004.

[24] L. Song and D. F. Kotz., "*Evaluating Opportunistic Routing Protocols with Large Realistic Contact Traces"*. Montreal : In Proc. of ACM 2nd Workshop on Challenged Networks (CHANTS ’07), 2007. pp. 35–42.

[25] P. Vinayakray-Jani, and S. Sanyal, 2012. "*Routing protocols for mobile and vehicular ad-hoc networks: A comparativeanalysis"*. Computing Research Repository abs/1206.1918, 1–7.

[26] A. Omidvar and K. Mohammadi, "*Intelligent routing in delay tolerant networks*," *2014 22nd Iranian Conference on Electrical Engineering (ICEE)*, Tehran, 2014, pp. 846-849.

[27] S. Kumagai and H. Higaki, "*Intermittent wireless multihop transmission protocol in mobile wireless sensor networks*," *Signal Processing and Communication Systems (ICSPCS), 2014 8th International Conference on*, Gold Coast, QLD, 2014, pp. 1-8.

[28] A. Kodole, P.M. Agarkar, “*A survey of routing protocols in mobile ad hoc networks*”, Multidisciplinary Journal of Research in Engg. & Tech, vol.2 no. 1, pg – 336-341, 2015.

[29] A. K. Gupta, I. Bhattacharya, P. S. Banerjee and J. K. Mandal, "*A Co-operative Approach to Thwart Selfish and Black-Hole Attacks in DTN for Post Disaster Scenario*," *Emerging Applications of Information Technology (EAIT), 2014 Fourth International Conference of*, Kolkata, 2014, pp. 113-118.

[30] A. Al Hinai, H. Zhang and Y. Chen, "Mitigating Black-hole Attacks in Delay Tolerant Networks", In Proc. of the 13th International Conference on Parallel and Distributed Computing, Applications and Technologies, 2012.

Biographies

Mrs. Alaa Hassan has received her master degree in Information Technology from the School of Computer Science/ University of Nottingham/ United Kingdom. Currently, she is working as a lecturer and a director of Computer and Internet Center at the College of Dentistry at the University of Kirkuk/ Iraq. Her extensive research covers information access, retrieval and visualization, security issues, and wireless and internet computing.

Mrs. Wafa Ahmed El Gali has a master degree in Information Technology from the School of Computer Science/ University of Nottingham/ United Kingdom. She is passionate about computer communications and network security and reliability.