Evaluating Performance Characteristics of the Spray and Wait, and Epidemic Routing Protocols Under Black Hole Attacks

Name: Ruijie Li

Student ID :20144302

Module Convenor: Milena Radenkovic

School of Computer Science

University of Nottingham

Contents

1.Delay-tolerant networking

1.1Background

The traditional networks we have learned so far, such as wired networks, wireless networks, and ad hoc networks, have similar characteristics: First of all, these networks have a complete path from node to node. Secondly, both round-trip delay (RTT) and the packet loss rate in traditional networks are low. However, it is difficult to apply the traditional network to some special scenarios, such as disaster communication scenarios, remote areas with weak signals scenarios, and satellite communication scenarios. This is mainly because the intermittent communication between nodes and long disconnecting and re-connection may frequently occur in these scenarios. Thus, the delay-tolerant network needs to be introduced. Unlike traditional networks, delay-tolerant network (DTN) can be well applied to the above special scenarios.

1.2 DTN introduction

DTN is a mobile ad hoc network which consists of a set of completely decentralized nodes that form an autonomous network. It is a dynamic network that changes over time. In DTN, there is no need to establish an end-to-end path and the propagation of messages would delay for a long time in the network. The connection of nodes in the DTN network is intermittent [1]. Nodes in DTN are decentralized and free to move and communicate with each other in the network. Each node has a certain range of communication. These nodes will search for and discover other nodes within the communication range and use the radio interface to communicate with the nodes that they encounter. At the same time, each node has a buffer of a certain size for receiving and storing messages. During the process of moving, when nodes encounter other nodes, they will send messages to each other and put the received messages into the buffer area. Nodes in a DTN network implement message passing through a store-and-forward mechanism. After receiving messages from the source node, nodes in the network send the message to other nodes through the three steps of continuously moving, establishing a connection, and exchanging messages until the destination node receive the messages.

2. Opportunistic Network Environment Simulator

2.1 overview of the one simulator

It is critical to choose a good DTN simulator due to the small quantity of nodes in the DTN and the limited transmission range of the nodes. ONE is a full-featured DTN Opportunity Network Simulator and an "agent-based discrete event simulator". It is an open-source software written in Java by the University of Helsinki, Finland. Users can use the ONE simulator to set different scenarios and different routing protocols to simulate how nodes receive and send messages in the DTN. In the process of simulating, the ONE simulator will use a graphical interface to represent the scene, which makes it easier for users to observe the movement trajectory of each node and the transmission process. Additionally, a visual report will be generated by the simulator for each simulation scene. Figure 1: One simulator interface

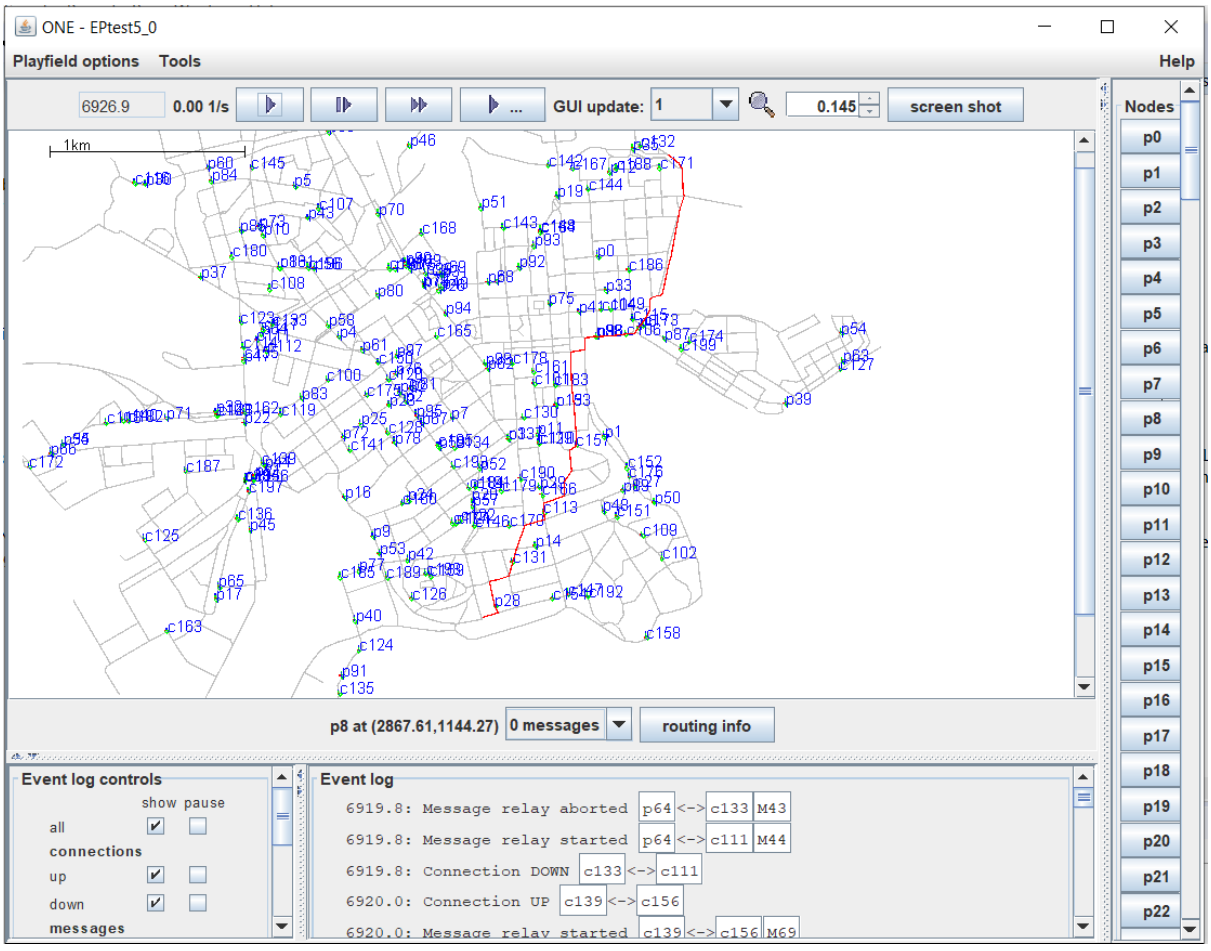


Figure 1 GUI of the ONE Simulator

2.2 Simulator introduction

As shown in Figure 2 ONE simulator contains different java packages, all of which implement different functions and complete the scene simulation through mutual calls and cooperation.

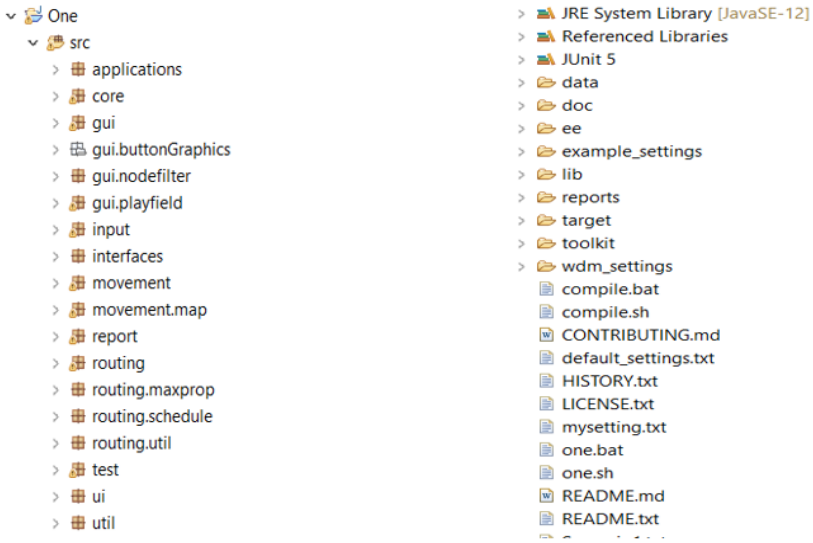


Figure 2: Hierarchy of java package of ONE simulator

The applications package is mainly used to simulate the application layer of the internet protocol stack.
The core package is a key module of the one simulator, which contains the core classes and interfaces of the simulator, implementing most of the simulator's functions: applications, links, DTN nodes, messages, inter-module communication buses, network interfaces, configuration file reading classes, emulator clock and simulation scene. settings.

GUI package is for designing user interaction interface.
The movement package is used to implement the movement model. The movement model which includes bus movement model, Car movement model, random walk model, Stationary movement model, etc. mainly specifies the movement rules of the DTN network nodes.

The routing package is used to implement the DTN routing algorithm which are mainly divided into two categories: active routing and passive routing. Active routing is where

nodes actively seek opportunities to forward data packets. The source code has implemented several different active routing algorithms, such as Direct Delivery Router, Epidemic Router、First Contact Router、MaxProp Router, etc. However, passive routing protocols fails to be implemented in the ONE simulator.

The report package is responsible for generating the reports that are the basis for users to analyse the performance of the network. These reports cover different types of data such as the start and end time and duration of contact, the generation time of the message, the success time of the transmission and the transmission time, the delivery success rate, and the message transmission path.

3. Opportunistic Delay-Tolerant Networking Protocols

Due to the long delay of DTN, a large number of packets in the network would be dropped and cannot reach to the destination node and TCP will eventually end the session if TCP / IP protocol is used for DTN communication. Therefore, TCP / IP protocol cannot be applied to the DTN communication. DTN should use some special routing protocols.

DTN routing protocols are divided into two types, one is a routing protocol based on forwarding and the other is a routing protocol based on replication[2] . Forwarding-based routing protocol, also known as single copy protocol which is one of the simplest forwarding schemes[3] . Its principle is that each message can only be kept by one node. After the message is forwarded, the node receiving the message is responsible for keeping the message. Therefore, only one copy of the message will exist in the network. Common forwarding-based routing protocols are Direct Transmission and First Contact routing protocols.

In replication-based protocols or multi-replication protocols, messages are propagated throughout the network by being continuously replicated by nodes [4]. Source node would send a copy of the message to the nodes it meet, and it will keep the original message after forwarding a copy of the message, while in the forwarding-based routing protocol, nodes will delete the local copy after forwarding the message. Direct Delivery, Epidemic, spray & wait, Prophet, and MaxProp are common replication-based routing protocols [5]. This protocol is also beneficial to increase the possibility that messages could be delivered to the target node.

3.1 Epidemic

The epidemic routing protocol is a flooding protocol based on multiple copies. In epidemic routing protocol, each node has two buffers. One is used to store messages generated by the node itself and the other is used to receive and store messages delivered by other nodes. Vectors are used to represent the messages in the buffer. Each message has a corresponding ID. Each node maintains a vector list of messages.

As shown in Figure 3, node A sends its own message list to node B when they meet. After receiving the message list from node A, node B compares this list with its own message list to find the different messages in the two lists. The two nodes then exchange messages that they do not have in common.

Through the above method, nodes continuously exchange messages with each other until these messages are transmitted to the target node.

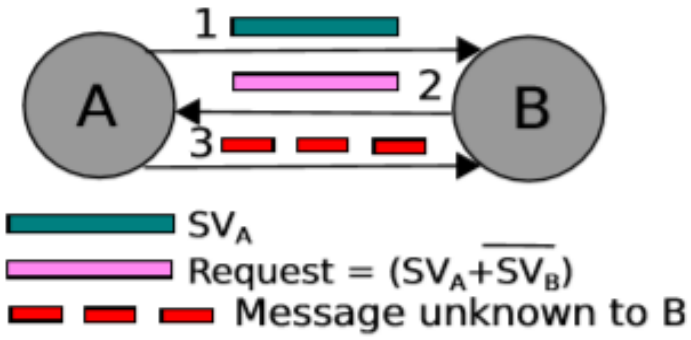


Figure 3. when hosts, A and B, are in transmission range of one another[6]

The advantage of the Epidemic routing protocol is that it can maximize the message delivery ratio and reduce the average latency. However, there are also some disadvantages. For example, during the transmission process, resources in the network would be over consumed since each node would create a great number of message copies.

3.2 spray and wait

Unlike the Epidemic protocol, the spray & wait only allow each message to have only L shares in the network, which can prevent messages from being copied blindly by nodes.

The source node creates L copies of the packages. In the Spray phase, L copies of the packages would be sent to L nodes which encounter the source node[7]. At this stage, the source node has two distribution methods. One is to send half of the L messages to the nodes that meets the source node and keep the other half of the messages, that is, send L / 2 message copies to the L nodes encountered by the source node. This allocation strategy is called Binary spray & wait.

The other dispense strategy is vanilla spray & wait, the source node will send one of the L messages (1 / L) to the nodes it encounters. During the spray phase, if other nodes have not passed the message to the target node, the spray & wait routing protocols will enter the waiting phase.

During the waiting phase as it shown in Figure 4, if the source node buffer contains more than one copy of the message, the source node will continue to send the message to the nodes it meets. When there is only one copy of the message left in the source node's buffer, it will wait to encounter the target node and send the message to the target node rather than sending a message to other nodes.

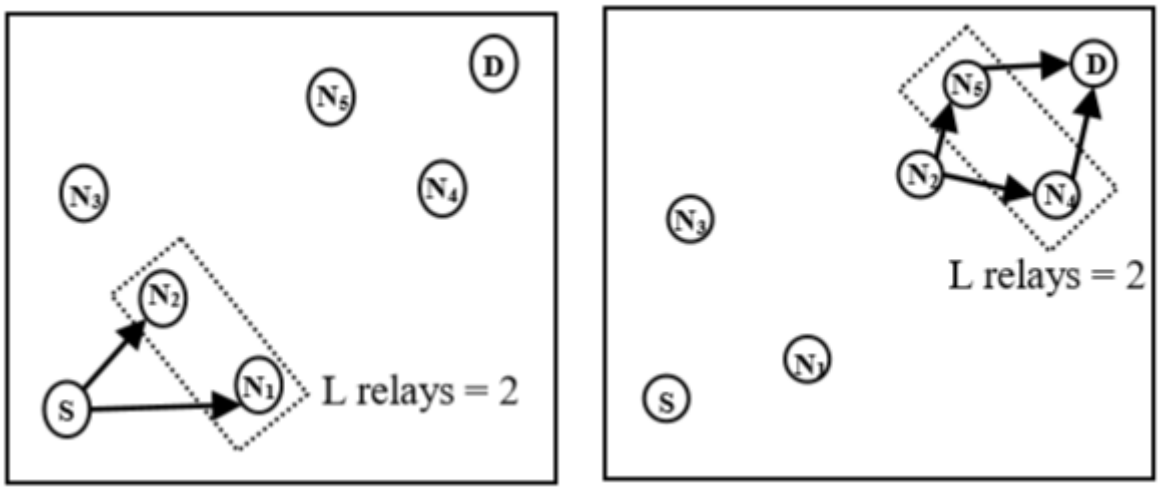


Figure 4. Spray &Wait Routing[8]

4.Experiment

4.1 Blackhole attacks

Security has become an important area of opportunity network research, since the openness and flexibility of opportunity network make it vulnerable to malicious attacks. Black hole attack is one of the common attack modes. If there are malicious nodes with black hole attack function in the network, they will block and disturb the communication between nodes by dropping the packages in the network. If the black hole node intercepts and deletes important messages, it will cause great loss to the whole network communication.

This experiment will use black hole attack to test the performance of epidemic algorithm and spray & wait algorithm.

Black hole attack is a network layer attack. There are three types of black hole attacks: ordinary black hole, active black hole and passive black hole [9]. Because DTN networks are more vulnerable to ordinary black hole attacks, the black hole attacks studied in this design are ordinary black hole attacks. Moreover, the behaviour of malicious nodes with black hole attack performance is similar with that of ordinary nodes. They can move freely and receive messages in the network. However, unlike ordinary nodes, these malicious nodes do not store and forward messages after receiving messages but discard the received messages. Therefore, these nodes form a black hole to absorb and delete messages, which might do harm to the performance of the network.

4.2 Scenario

4.21 Scenario1 description

Assuming a terrorist attack in Helsinki. Pedestrians dispersed immediately and reported to police cars in the city. There are also terrorist groups in the city who want to prevent pedestrians from communicating with police cars. Terrorist organizations can be seen as black hole nodes. This group of pedestrian nodes is set as the source node, and police car nodes are set as the target nodes. The number of malicious nodes (terrorists) in the city is constantly increasing to interfere with the normal communication between pedestrian nodes and vehicle nodes. Set 0, 20, 40, 60, 80, 100 malicious nodes in turn.

When the network contains malicious nodes, as the number of malicious nodes increases, which means that more and more malicious nodes invade the network and the intensity of black hole attacks in the network also increases.

There are two types of spray & wait routing protocols. Set binary Mode in the configuration file to true, that is, the protocol used in the scenario is the Binary Spray and Wait protocol. If set it to false, the vanilla spray & wait protocol will be launched. In the Scenario 1, the number of copies in the spray & wait is set to 8, that is, L = 8.

Parameters	Values
Simulation time	10000(24 hours)
Number of nodes	200-300
Node Groups	Pedestrians (100 nodes) Cars (100 nodes) Malicious (0-100 nodes)
Interface	Bluetooth High Speed
Buffer size	10M
Message TTL/min	300(5 hours)
Node speed(m/s)	Pedestrians (0.5-1.5) Cars (7-10) Malicious (7-10)
Movement model	Shortest Path Map Based Movement
Number of copies	8

Table 1 - Experiment Setup

4.22 Scenario2 description

In order to study the effect of the number of message copies on the performance of the spray & wait routing protocol in scenario 1, set the number of malicious nodes in scenario 2 to 100, and increase the number of message copies in scenario 1 with the number of black hole nodes unchanged. Set 5, 10, 15, 20, 25, 30 message copies.

4.3 Black Hole router

When setting up black hole nodes, the difference between black hole nodes and normal nodes is that they use different routing protocols. Therefore, a new black hole routing protocol needs to be added to the routing package in the ONE simulator. In order to implement the black hole routing protocol, the code of the Epidemic routing protocol and the spray & wait routing protocol need to be changed. The following figure shows the changed code.

In the first place, because a black hole node deletes the messages that it received directly, the code enabling the node to delete messages in its buffer need to add to Epidemic and Spray & Wait protocols. As can be seen from the following figure, addTOMessage function is added to the code of the routing protocol, which can obtain the information of the message received by the black hole node. The addTOMessage function is called when a malicious node receives a message. In this function, the ID of the message is obtained, and the deleteMessage function is called to delete the message from the node's buffer.

Secondly, because black hole nodes do not forward messages or exchange messages with other nodes, the method in the update function needs to be deleted to prevent black hole nodes from transmitting messages to other nodes.

```
@Override
protected void addToMessages(Message m, boolean newMessage) {
    super.addToMessages(m, newMessage);


    deleteMessage(m.getId(), true);
}

@Override
public void update() {
/*  super.update();

    if (isTransferring() || !canStartTransfer()) {
        return; // transferring, don't try other connections yet
    }

    // Try first the messages that can be delivered to final recipient
    if (exchangeDeliverableMessages() != null) {
        return; // started a transfer, don't try others (yet)
    }

    // then try any/all message to any/all connection
    this.tryAllMessagesToAllConnections();*/
}
```

Figure 5 black hole code

5. Performance Evaluation

This experiment will evaluate the performance of Epidemic routing protocol and spray & wait routing protocol from three aspects: transmission capacity, transmission efficiency and node energy consumption [10]. The four values in Message Stats Reports are " Delivery ratio", " Average latency", "overhead ratio" and "Number of deleted messages", which will be used as indicators to evaluate the two routing algorithms.

5.1 Delivery Ratio

The delivery ratio indicates the ratio of the total number of messages successfully reaching the destination node to the total number of messages sent by the source node within a fixed period of time, that is, the ratio of the number of successfully delivered messages to the total number of messages generated[11]. Delivery ratio is an important metrics, which is applied to evaluated the delivery capacity of routing algorithms, can reflect network performance to a certain extent. The higher the message delivery ratio, the greater the number of messages successfully delivered to the target node, which indicates that the protocol has a strong performance.

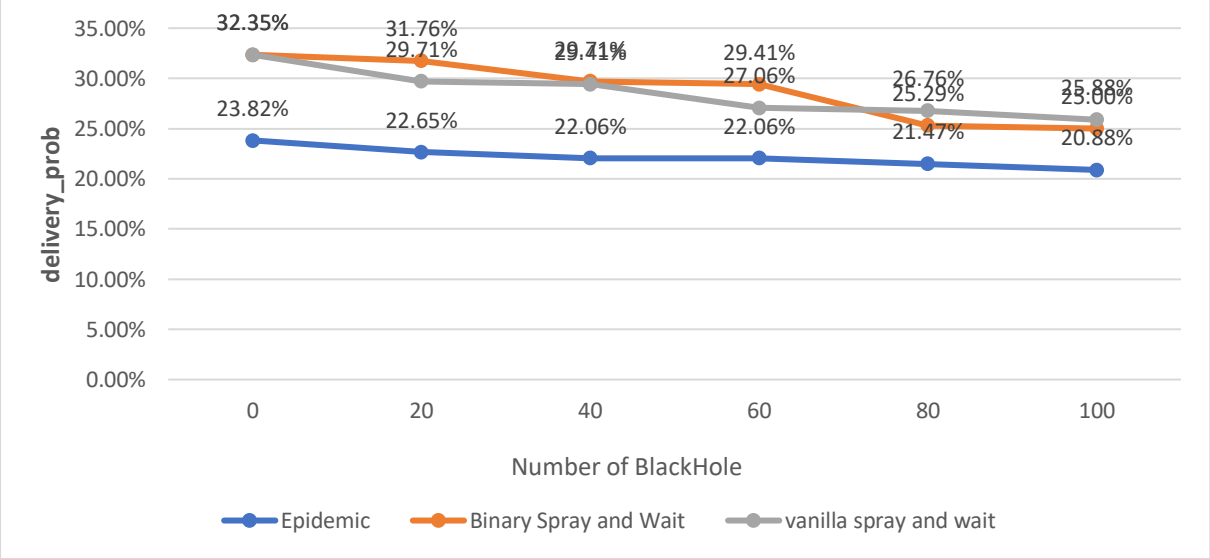


Figure 6 Delivery ratio

This experiment first explores the impact of black hole nodes on the delivery ratio of the routing protocol.

According to the figure 6, black hole nodes are constantly deleting messages in the network, causing delivery ratio of two routing protocols gradually decreasing with the increasing black hole nodes. As the number of malicious nodes increases, the probability that normal nodes in this network will encounter malicious nodes in the process of transmitting messages is increasing. Therefore, the probability of message being deleted is also increasing which would cause decreasing delivery ratio.

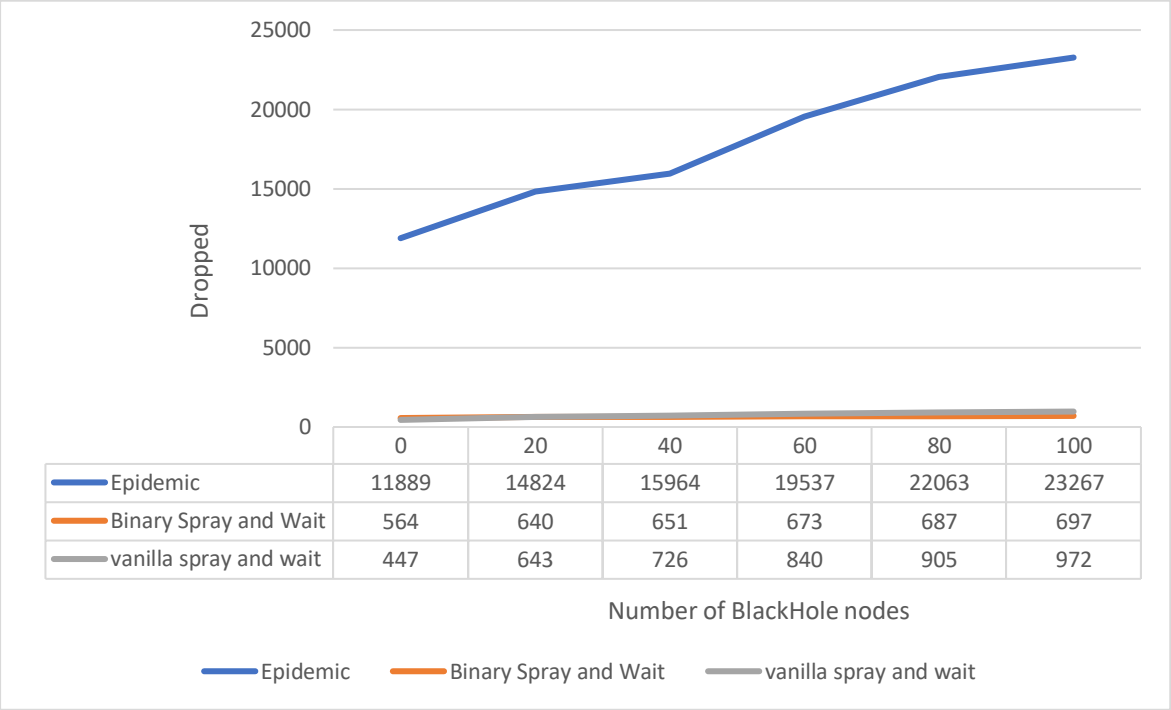
Another result with the increasing number of malicious nodes is that the delivery ratio of the spray & wait routing protocol decreased significantly, while the message delivery ratio of the Epidemic protocol decreased slightly. Because the Epidemic protocol is based on the flooding algorithm, which means that there are a great number of message copies in the network. Thus, when a malicious node deletes a copy of a message, there are still multiple copies of the message in the network. Consequently, the possibility of the message being transmitted to the destination node is still high. In summary, because the number of message copies generated by the Epidemic routing protocol is more than the spray & wait routing protocol, black hole nodes have less impact on the transmission rate of the Epidemic routing protocol.

Furthermore, an interesting phenomenon could be found by observing the data in the figure. In a network without black hole nodes, the delivery ratio of the Spray & Wait protocol is significantly higher than that of the epidemic protocol. However, the delivery ratio of the epidemic routing protocol changes slightly when the number of malicious nodes in the network continues to increase, while delivery ratio of the Spray & Wait routing protocol has a significant decrease. As a result, the epidemic routing protocol is more stable when the number of black hole nodes increasing unceasingly, which means that the black holes have a greater negative effect on Spray & Wait than on Epidemic. Based on the delivery ratio, the epidemic routing protocol is slightly better than the Spray & Wait protocol.

By comparing the delivery ratio changes of the two Spray & Wait routing protocols in the figure 6, it is evident that in scenario1, the delivery ratio has a greater relationship with the number of message copies. There is no apparent correlation between the delivery ratio and how the protocol disseminates messages.

5.2 Number of deleted messages

Figure 7 shows the change of the total number of messages deleted by malicious nodes, which could reflect the influence of malicious nodes on network performance to some extent. The more messages are deleted, the severer the network is destructed.



	0	20	40	60	80	100
Epidemic	11889	14824	15964	19537	22063	23267
Binary Spray and Wait	564	640	651	673	687	697
vanilla spray and wait	447	643	726	840	905	972

Figure 7 Number of deleted messages

The figure clearly illustrates there is a positive correlation between the number of malicious nodes in the network and the number of deleted messages. The number of the messages deleted by the black hole nodes in Epidemic routing protocol increase sharply and it is greater than the number of messages deleted by spray & wait. This phenomenon can be attributed to the fact that the quantity of message copies in the Epidemic routing protocol is much larger than that of the spray & wait routing protocol. Accordingly, the chances of messages being deleted are also greater than the spray & wait routing protocol.

From the relationship between the number of lost packets and malicious nodes, it can be seen that Epidemic routing protocol will cause a large amount of data loss in the network. At the same time, Epidemic wastes more node resources. Therefore, spray & wait routing protocol outperforms Epidemic routing protocol.

5.3 Average latency

Delivery Delay is the time required for a message to reach the destination node from the source node. Average delivery delay is the average time for nodes to deliver messages from the source node to the target node. A small Delivery delay means that the routing algorithm has a strong transmission capacity and high transmission efficiency and that the message will occupy less network resources during the transmission process[12].

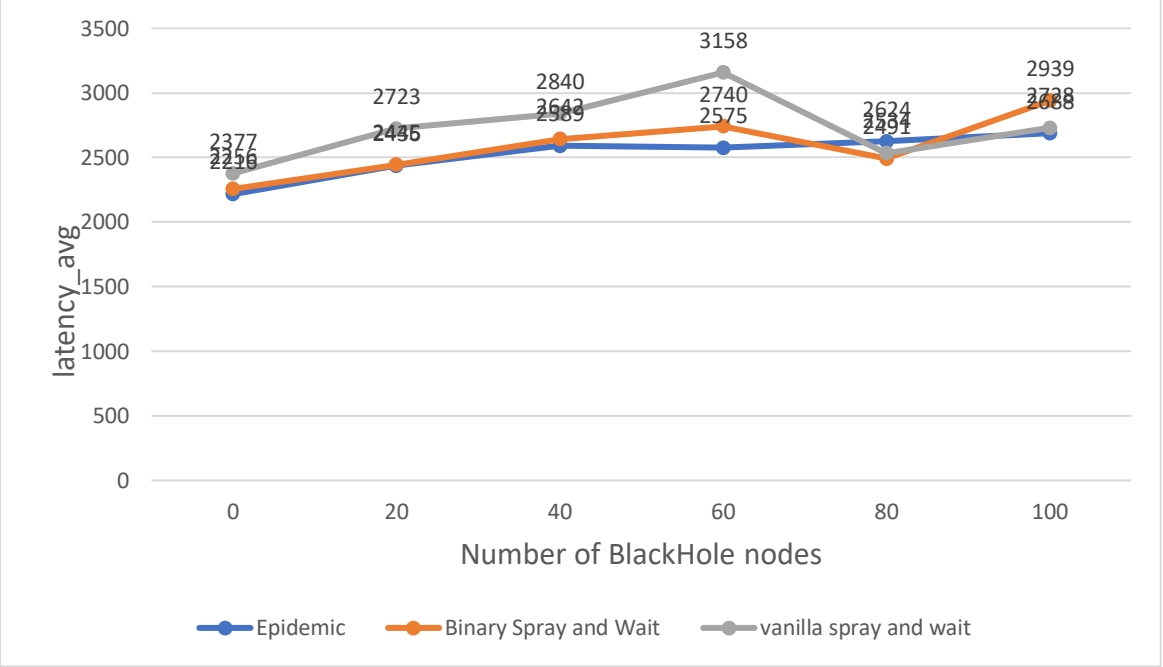


Figure 8 Average latency

Figure 8 reflects the effect of black hole attacks of different strengths on the average transmission delay. There is a slow increase in the Epidemic because there are many copies of the message in a network using the Epidemic routing protocol and most messages take a long time to reach the destination node. Impressively, as the number of black hole nodes goes up, the average latency goes down slightly in Spray & Wait protocol, which is attributed to the fact that the number of message copies is relatively small. The longer it takes for each message to reach the target node, the greater the chance that they will encounter a malicious node. Thus, as the number of malicious nodes increases, messages with longer delays are likely to encounter the malicious nodes and be deleted. The proportion of messages with shorter delivery delays in the network would definitely increase, resulting in lower average delivery delays.

5.4 Overhead Ratio

Overhead ratio refers to the ratio of all messages successfully transmitted to the destination node to the total number of messages forwarded by all nodes. If the overhead ratio is high, it means that the network is full of many message copies, which will increase the collision probability of messages in the network, and then consume the energy of nodes.

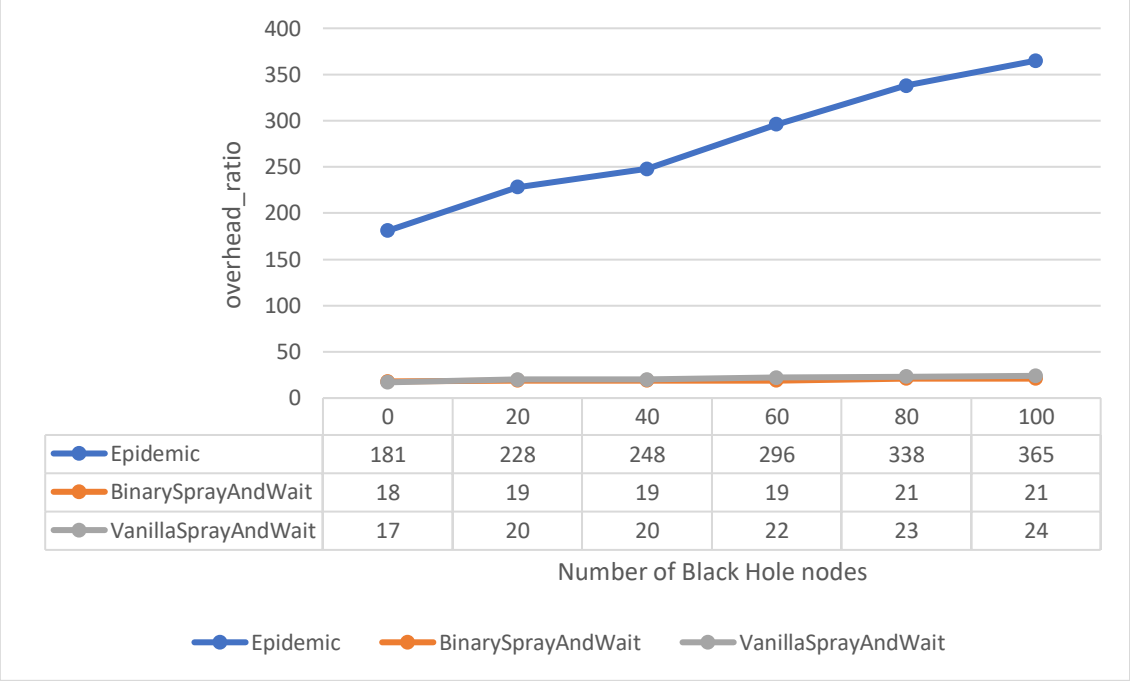


Figure 9 Overhead Ratio

As can be seen in the figure 9, when the number of malicious nodes goes up, the overhead ratio of the two protocols also increase. This shows that the growth of malicious nodes will make the nodes consume more energy, resulting in the performance degradation of the network. There is a clear pattern that Epidemic has an overhead ratio than Spray & Wait. The reason for this result is that nodes in epidemic routing protocol will copy messages without restraint, creating a large amount of messages copies. The spray & wait protocol could control the number of copies of messages, which is the reason why its overhead ratio is low.

Therefore, the spray & wait protocol performs better than that of the epidemic protocol since its overhead ratio is lower.

In conclusion, although delivery ratio of the Epidemic protocol is less affected by black hole nodes, it is still lower than the delivery ratio of Spray And wait. At the same time,

both overhead ratio and the number of deleted messages in Epidemic protocol are higher than Spray And wait, which means Epidemic protocol might occupy more network resources and consumes more nodes energy to get low delivery ratio. As a result, in a comprehensive view, it seems fair to say that the than Spray And wait protocol will perform better in these cases than the Epidemic protocol will.

5.5 Spray &Wait Performance in scenario2

The performance of the two schemes of the routing protocol will be analysed in this section by using three metrics: the delivery ratio, the average latency, and the overhead ratio.

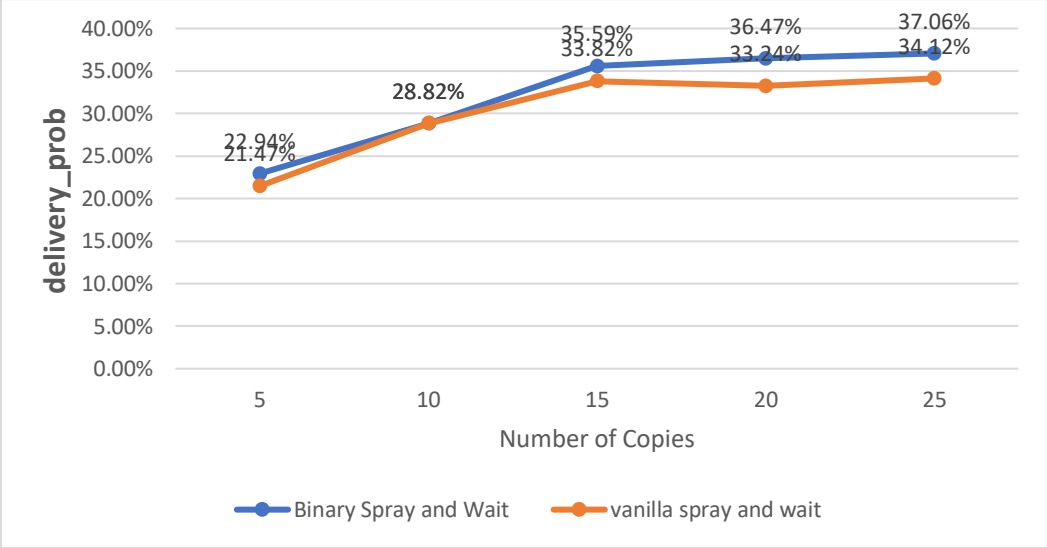


Figure10 Delivery ratio for scenario2

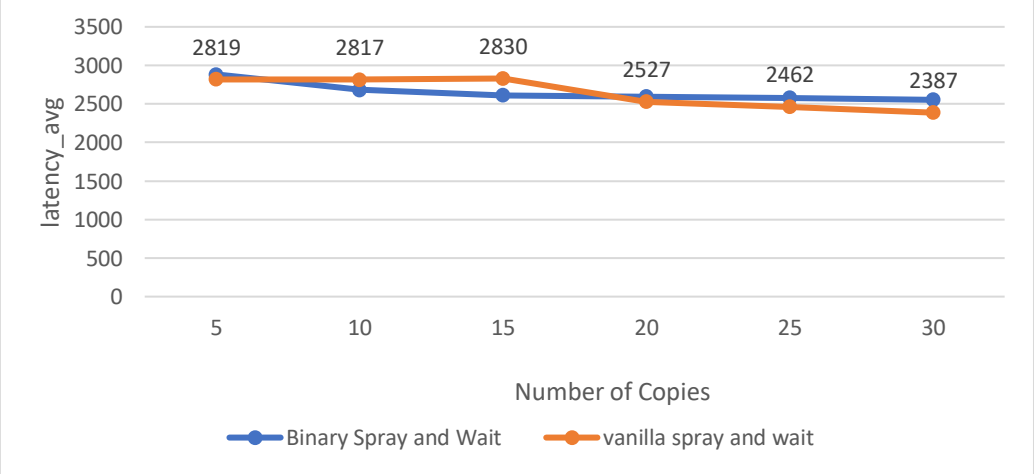


Figure11 Delivery latency for scenario2

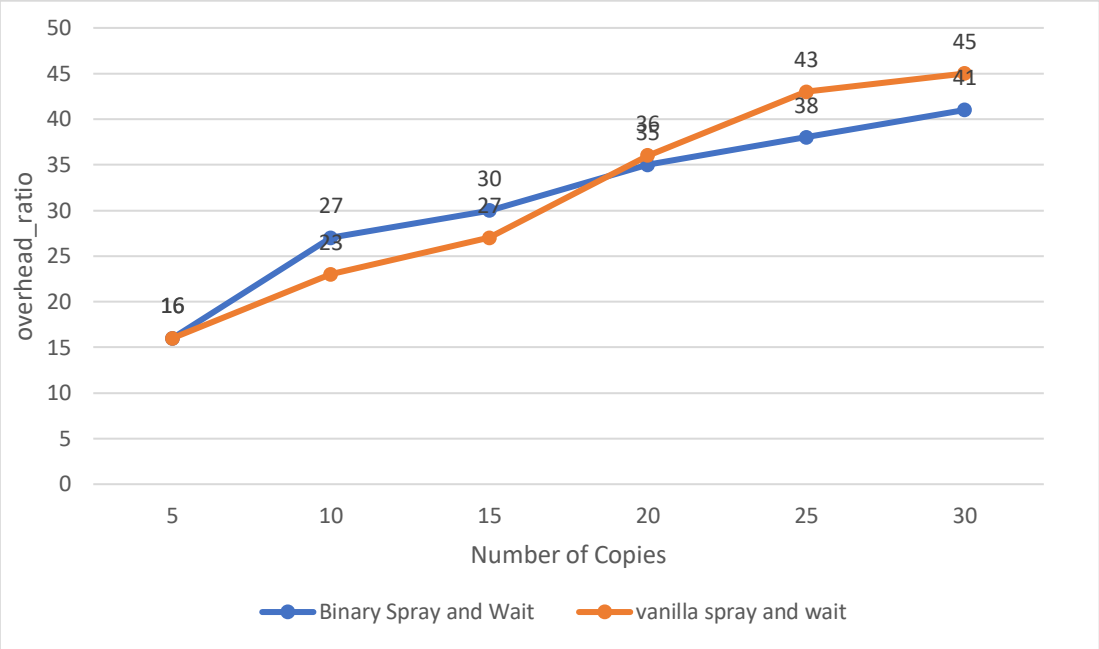


Figure 12 Overhead ratio for scenario2

By observing Figures 11, 12, and 13, the following conclusions can be drawn:
First, when the number of message copies raising, the delivery ratio of the two spray and wait routing protocols go up rapidly as well as the average latency fall gently, which indicates that increasing the number of message copies could enhance the performance of the network, reducing the degree of damage caused by black hole nodes. However, excessive message copies cause the growth of overhead ratio, because nodes need to copy more messages and would lose more energy.

Secondly, when the number of message copies rises to 15, the delivery ratio increases slower than before, while the overhead ratio is still increasing dramatically. This phenomenon indicates that the existence of an excessive number of message copies in the network does not mean that the performance of the network will be better. On the contrary, it may reduce the performance of the network. Therefore, when using the spray and wait routing protocol, it is necessary to control the number of replicas in the network.

Finally, combining the three metrics, we can see that the performance of Binary spray & wait is slightly higher than the performance of vanilla spray & wait. However, there is only a slight difference between the two spray & wait protocols, which means that

conclusion of 5.1 is verified. For black hole attack scenarios, the message distribution method of the spray & wait routing protocol will less affect the network performance. Instead, the number of copies of messages has a great relationship with the performance of the network.

5.6 Evaluation summary

Firstly, both the epidemic protocol and the spray & wait protocol can be affected by the black hole node. The performance of two protocol would be worse with the introduction of malicious nodes to the network.

Secondly, the black hole nodes will discard the received messages, which means that the more copies of packages in the network, the higher the chance of packages being sent to the target node.

Third, although the message delivery ratio of epidemic protocol is less affected by black hole nodes, the routing overhead of this protocol is much larger than that of spray & wait protocol. Therefore, the protocol will take up a lot of network resources.

Fourth, because both the epidemic protocol and the spray & wait protocol are multi-replication protocols, there are still some message replication remind in the network although they can be affected by malicious nodes. If the single copy protocol can be added to this experiment for comparison, the advantages of the multi replication protocol will be more prominent.

Fifth, the network resources could be saved as spray & wait routing protocol can control and adjust the number of node message replication. When the number of spray & wait routing message copies is adjusted to the appropriate number, the protocol will be more suitable for the scenario1 than the epidemic protocol. To sum up, the spray & wait is more flexible and has more potential than the epidemic.

6. Wider Discussion

6.1 Advantages of Opportunistic Networks in the Scenario

Traditional network cannot satisfy the need of scenario 1, as the pedestrians and police cars in scenario1 are constantly moving and difficult to establish a complete end-to-end path. However, the advantage of opportunistic networks is that nodes are completely free to move and can forward and transfer messages while moving, which exactly meet the requirement. While propagating the message, nodes in opportunistic networks can copy the message and spread the message quickly, which means that the pedestrian in the scenario not only can be used as the source node to send the message but also be used as the router to transmit the message, which increases the chance of the message being transmitted to the target node.

In addition, if a path in traditional networks is attacked, it means that the target node cannot receive packages from the source node, which may cause serious losses to the network. In contrast, in an Opportunistic Networks, if a message is deleted by a malicious node, the copies of message still exist in the network, and other nodes can continue to deliver the message copies.

6.2 Disadvantages of Opportunistic Networks in the Scenario

Many traditional networks use authentication mechanisms, such as AAA and PKI, to solve security problems. However, in the opportunistic network, many authentication mechanisms are not applicable, which makes the opportunistic network more vulnerable to attack.

In this simulation scenario, encryption and decryption and authentication mechanisms are not used to ensure the security and reliability of the message during transmission, which prevents pedestrians from identifying malicious nodes and increases the possibility of message being intercepted.

Furthermore, in this scenario, Opportunity Network failed to provide a scheme for pedestrian nodes to avoid black hole nodes.

In future research, a list can be designed and added to the nodes buffer to record the label of the black hole nodes. If one node encounters a black hole node, other nodes will be informed to avoid transmitting messages to this black hole node.

6.3 Other Real World Scenarios Where Opportunistic Networks May Be Of Benefit

Currently, the application of opportunity network becomes more and more widely. One of these applications is to provide network connection for remote areas. In remote areas, many users are often unable to access the Internet due to inadequate infrastructure. Opportunity network can provide low price and relatively available network services for remote areas [13].
In addition, another application scenario of opportunity network is disaster scenario. Power and communications were disrupted after hurricanes, earthquakes, tsunamis and other severe natural disasters. In this context, disaster might do damage to a lot of network infrastructures, causing valuable messages cannot be sent to the rescue organization. However, Opportunistic network requires less infrastructure, which make Opportunistic network suitable for being applied to disaster scenarios. Each person could be regarded as a node in the disaster scenario and Opportunistic network allows these nodes store, carry and forward messages. In this situation, messages can spread quickly, enabling rescue team to get the messages from victims.

Finally, Opportunistic network has been used for Inter-Planet Satellite Communication and military Battlefield communication. In these kinds of scenario, security and reliability of the messages are required. Consequently, the security of the opportunistic networks is a prerequisite for utilizing opportunistic networks to some important communication scenarios and a focus which needs to be further discussed in future experiments.

Reference List

[1] Jalade, S.C. and Patil, A., 2014. The Concept of Delay Tolerant Network Approaches and Issues. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 3(4).

[2] Hunjan, Roshan, 2017. Optimising DTN routing protocols for efficient use in disaster scenarios.

[3] Jain, S. and Chawla, M., 2014. Evaluation of Spray Based Routing Approaches in Delay Tolerant Networks.

[4] Agussalim, M. & Tsuru, 2014. Comparison of DTN Routing Protocols in Realistic Scenario. 2014 International Conference on Intelligent Networking and Collaborative Systems, pp.400–405.

[5]Jain, S., Chawla, M., Soares, V.N. and Rodrigues, J.J., 2016. Enhanced fuzzy logic-based spray and wait routing protocol for delay tolerant networks. International Journal of Communication Systems, 29(12), pp.1820-1843.

[6] Bista, B.B. & Rawat, D.B., 2015. A Robust Energy Efficient Epidemic Routing Protocol for Delay Tolerant Networks. 2015 IEEE International Conference on Data Science and Data Intensive Systems, pp.290–296.

[7]Iqbal, S.M.A., 2012, December. Multischeme spray and wait routing in delay tolerant networks exploiting nodes delivery predictability. In 2012 15th International Conference on Computer and Information Technology (ICCIT) (pp. 255-260). IEEE.

[8] Alaoui, E.A., Agoujil, S.A.I.D., Hajar, M.O.H.A. and Qaraai, Y.O.U.S.S.E.F., 2015. The performance of DTN routing protocols: a comparative study. WSEAS Transactions on Communications, 14, pp.121-130.

[9] Ding, Y., Qu, H. and Li, G., 2015. Black hole attack model and simulation for mobile ad hoc network. INTERNATIONAL JOURNAL OF INNOVATIVE COMPUTING INFORMATION AND CONTROL, 11(1), pp.203-211.

[10] Yu, G., Yuan, D.F., Cui, Y., Wang, Y.D. and Zong, P., 2014. Research on Robustness of Typically Opportunistic Network Routing Algorithm under Flooding Attack. In Advanced Materials Research (Vol. 989, pp. 2227-2231). Trans Tech Publications.

[11] Kumar, S. and Dutta, K., 2015. Intrusion detection technique for black hole attack in mobile ad hoc networks. International Journal of Information Privacy, Security and Integrity, 2(2), pp.81-101.

[12] Yu, G., Yuan, D.F., Cui, Y., Wang, Y.D. and Zong, P., 2014. Research on Robustness of Typically Opportunistic Network Routing Algorithm under Flooding Attack. In Advanced Materials Research (Vol. 989, pp. 2227-2231). Trans Tech Publications.

[13] Burleigh, S., Hooke, A., Torgerson, L., Fall, K., Cerf, V., Durst, B., Scott, K. and Weiss, H., 2003. Delay-tolerant networking: an approach to interplanetary internet. IEEE Communications Magazine, 41(6), pp.128-136.