Effective Controlling Scheme to Mitigate Flood Attack in Delay Tolerant Network

Hanane ZEKKORI, Saïd AGOUJIL, Youssef QARAAI
Dept. of Computer Science of Faculty of Sciences and Techniques, University of Moulay Ismail
Errachidia, Morocco

***Abstract*—Conventional routing protocols breaks down in opportunistic networks due to long delays, frequent disconnectivity and resource scarcity. Delay Tolerant Network (DTN) has been developed to cope with these mentioned features. In the absence of connected link between the sender and the receiver, in DTN mobile nodes replicate bundles and work cooperatively to improve the delivery probability. Malicious nodes may flood the network as possible by a huge number of unwanted bundles (messages) or bundle replicas which waste the limited resources. DOS (Denial of Service) attack especially Flooding attack attempt to compromise the availability service of the network. Traditional congestion control strategies are not suitable for DTN, so developing new mechanisms to detect and to control flooding attack is a major challenge in DTN network. In this paper, we presented a comprehensive overview of the existing solutions for dealing with flooding attack in delay tolerant network, and we proposed an effective controlling mechanism to mitigate this threat. The main goal of this mechanism is first to detect malicious nodes that flood the network by unwanted messages, and then to limit the damage caused by this attack. We also ran a large number of simulations with the ONE simulator to investigate how changing buffer capacity, message lifetime, message size, and message replicas affect DTN network performance metrics.**

***Keywords*—DTN; flooding attack; DOS; congestion; buffer capacity; bundle; ONE**

I. Introduction

Nowadays, the use of wireless technology has invaded the mobile network market. MANET (Mobile Ad hoc Network) [1] is a wireless network that does not rely on a pre-existing infrastructure. This traditional mobile network, on the other hand, does not support packet transfer in an environment characterized by an intermittent connectivity between the transmitter and the receiver. Which results in the birth of the DTN (Delay tolerant network) [2], that comes to cope with these challenges by the help of a Bundle layer added on top of lower-layer protocols (see Fig. 1). The bundle layer ensures interoperability between network regions and the transfer of bundles (messages) via a technique known as store carry and forward [2], in which network mobile nodes collaborate with each other to increase the message delivery rate.

Contacts in the DTN network are opportunistic [3]; nodes meet with no prior knowledge about the movement and the mobility of the other nodes in the network. So, flooding based routing strategy can be opted to improve the probability of delivery and to reduce the average latency. This routing strategy consists of flooding the network with multiple copies or replicas for each single bundle to increase the likelihood that one of these copies will reach its destination. This strategy, however, consumes more network resources.

DTN uses the store-carry and forward paradigm [2] to avoid data loss if the upstream path is interrupted. When a source node creates a bundle, it stores it in its persistent buffer until a contact opportunity with an intermediate node occurs. The mobile nodes exchange bundles in a hop-by-hop manner, and the process is repeated until each bundle arrives at its final destination. Each node has a persistent buffer B in which it stores the received bundles, and it is defined by its limited capacity C.

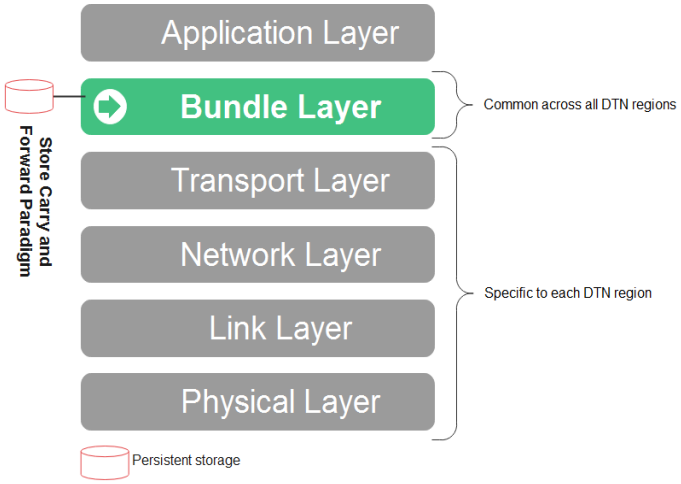


Fig. 1. Illustration of DTN Layered Architecture.

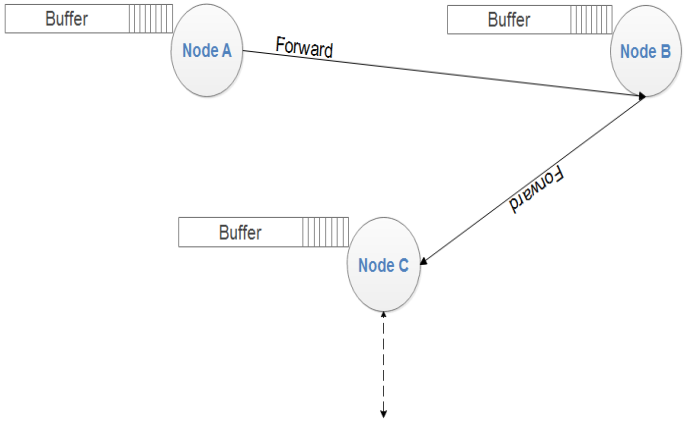


Fig. 2. Illustration of the Store Carry and Forward Transport Technique.

We have schematized the technique Store and Forward in the Fig. 2: to deal with the DTN network's intermittent connectivity, each node keeps the bundle in its buffer (store phase) while waiting for a future communication opportunity with a relay node to transmit that bundle (forward phase).

A. Security Requirements

The fundamental security requirements for DTN [4] are similar to those for wired and wireless networks with infrastructure. Security services are based on five fundamental concepts: Authentication, confidentiality, data and network traffic integrity, availability, and non-repudiation (see the Fig. 3 below) [5] [6].

Fig. 3. The Five Fundamental Security Requirements.

B. The Five Fundamental Security Requirements

- Authentication

Authentication verifies the identity of network entities or nodes. This is a crucial step in controlling network resource access. Without authentication, a malicious node can easily spoof another node in order to gain the privileges assigned to that node, or attack using that node's identity in order to harm its reputation. The authentication process in wired or wireless networks with infrastructure is based on a trusted third party which has been approved by all network entities. The trusted third party is simply the certificate authority, which distributes certificates to nodes with access to specific network services. This centralized authentication scheme is known as Public Key Infrastructure (PKI) [7]. It is nearly impossible to apply the PKI model directly to the DTN network because the DTN network topology changes frequently and dynamically and the connectivity is intermittent, the nodes are autonomous, and their capabilities (energy, computation, buffer space, etc.) are limited.

- Confidentiality

The fundamental service for ensuring private communication between nodes is confidentiality. It is about protecting against threats that could lead to unauthorized disclosure or viewing of private information. It is fundamentally based on cryptography, specifically encryption algorithms. Encryption algorithms, whether symmetric or asymmetric, require an encryption key to encrypt a message before it is sent to its destination. However, in order to decrypt the message, the destination must have a decryption key. As a result, a key management and sharing mechanism tailored to the DTN network is required, however due to the DTN network's unique characteristics (intermittent connectivity…), it is a significant challenge to implement these traditional encryption algorithms.

- Integrity

This service ensures that traffic from the source to the destination has not been altered or modified without prior authorization during transmission. The risk that a malicious node modifies a message is always present in the DTN network. The goal of integrity service is to ensure that resources are working properly. This service protects information from unauthorized modification (ensure data integrity). Indeed, this service can be used in conjunction with security protocols that provide confidentiality and authentication.

- Availability

Availability refers to ensuring the continuity of a node's services even in the face of an attack. In other words, nodes must ensure network services continuity (such as routing, data access, and so on) in the event of a flooding attack. To accomplish this, it is necessary to protect against threats that may disrupt network functions to ensure that all nodes have access to network resources without any restriction.

- Non-Repudiation

The ability to verify that the sender and the receiver are the parties claiming to send or receive messages is referred to as non-repudiation security requirement. In other words, the undeniable source demonstrates that data was sent, and the undeniable destination demonstrates that data was received. Non-repudiation, in other words, ensures that the transaction (transmission/reception) cannot be denied. This is extremely helpful to detect and isolate infected nodes. Any node that receives an incorrect message can use evidence to accuse the sender, which helps other nodes believe in the sending node's compromise.

Because of long delays [5], frequent disconnections, and resource scarcity, traditional routing protocols fail in opportunistic networks. To address these issues, the Delay Tolerant Network (DTN) was created. In the absence of a connected link between the sender and the receiver, DTN mobile nodes replicate bundles and collaborate to improve the probability of delivery. Malicious nodes may flood the network with as many unwanted bundles or bundle replicas as possible, wasting the network's limited resources. A flood attack attempts to compromise the network's availability service. Because of the unique characteristics of DTN networks, traditional mechanisms are ineffective for detecting and controlling flooding attacks, so developing new mechanisms to detect and control flooding attacks is a major challenge in DTN.

In this paper we examined the impact of changing buffer capacity, message lifetime, message size, and message replicas on flooding-based routing protocols in terms of the following

performance metrics: delivery probability, overhead ratio, and latency average, and we proposed an effective controlling mechanism to mitigate the flooding attack. The primary goal of the proposed mechanism is to detect malicious nodes that flood the network with unwanted messages and then limit the damage caused.

This paper is structured as follows: Section 2 discusses related work on the existing security solutions against selfish behavior in Delay Tolerant network and presents flooding attack in DTN. Section 3 gives our proposed work whereas section 4 focuses on the simulation setting used to discuss the performance of routing protocols in DTN, also this section emphasizes and analyzes the obtained results. Finally, Section 5 concludes the paper providing a final summary of the study and suggests additional research topics for the future.

II. Related Work

A. Flooding Routing Protocols

To improve the delivery probability and to reduce the average latency, flooding-based routing protocols can be used (see the Table I). Flooding-based routing strategy [8] involves flooding the network with multiple copies or replicas of each single bundle (message) in order to increase the likelihood that one of these copies will reach its destination. This, however, consumes more network resources.

TABLE I. Description of the Flooding based-Routing Protocols

Routing Algorithm	Description
Epidemic[9]	In the epidemic routing protocol, each mobile node stores a copy of each message in the network in its buffer. When it makes a contact with another node, all its messages are routed to that node, and so on. Each bundle is labeled with a unique identifier (ID) and listed in a list known as a "state vector." When two nodes communicate, the list of bundle IDs is exchanged; at the end of this operation, both nodes should have the same bundles in their buffers. There is no prior network knowledge required for the epidemic routing protocol. This protocol, on the other hand, necessitates a substantial amount of buffer space, bandwidth, and energy.
Spray and Wait[10]	Spyropoulos et al proposed the Spray and Wait routing protocol, which works on the principle of starting the transmission with a limited number of copies L (with L>1) in order to preserve the DTN network's limited resources. For each bundle in the network, the Spray and Wait protocol algorithm consists of two phases: • The spray phase: The source node sends L copies of each bundle to the L relay nodes during the spray phase. • The wait phase: When each bundle has a single copy, each node will wait for a direct meeting with the destination node before sending the bundle copy to its destination.
Binary-Spray and Wait[10]	The spray phase here differs from the one described above (the spray phase of Spray & Wait protocol); in Binary-Spray &Wait protocol, the source node sends L/2 copies to the neighboring nodes, and when there is only one copy left in each node's buffer, it enters in the wait phase, as described above in the wait phase of Spray & Wait protocol.

B. The Queue Management

When the DTN runs out of storage space, it discards old bundles because they are likely to have arrived at their destinations. When storage resource becomes insufficient, the Bundle layer has only a certain amount of freedom in managing the situation, so it can drop older (TTL≈ 0) bundles in order to receive new bundles.

There are several service disciplines (Buffer management policies) to manage a queue, the simplest way to manage a queue is the FiFo (First in First out) discipline[11].

- DLR (Drop Least Received): is identical to FiFo, the first message to arrive will be the first served.
- DOA (Drop Oldest Arrive): deletes the oldest message because there is a high probability that this message has reached its destination.
- DLE (Drop Last Encountered): drops the message that has the smallest predictability.

C. Problem Statement: Flooding Attack

A Denial-of-Service (DOS) [12] attack is an active attack that aims to make a network's services unavailable for an extended period of time. The purpose of this type of attack is not to modify or drop bundles. But the goal is to disrupt or harm the reputation of a network service. This attack consumes resources such as bandwidth, energy, and storage space.

The basic idea behind this attack is to send bundles in an unusual pattern, causing saturation or instability in the victim nodes and preventing them from providing the network services that they are supposed to provide. When several nodes cause a Denial-of-Service attack. This is referred to as a "Distributed Denial of Service (DDOS)". A DDOS attack has the same goal as a DOS attack, except that the attack is launched from more than one node at the same time.

Such attacks are classified into two types [13]:

a) Denial of service by saturating a node's buffer to the point where it can no longer receive other bundles.

b) Denial of service by exploiting vulnerabilities, which involves exploiting a network flaw to render it inoperable.

D. Overview of the Existing Solutions for Detecting the Flooding Attack in Delay Tolerant Network

Table II summarizes the fundamental three techniques used in the literature to detect and prevent the flooding attack in DTN.

TABLE II. SURVEY OF THE EXISTING SECURITY SCHEMES USED FOR MITIGATING THE FLOODING ATTACK IN DTN

Scheme	Its process	Its limitation
Claim-Carry and Check scheme[14]	A rate limiting was proposed, each node has a limit on the number of messages that it can generate in each time interval and a limit on the number of replicas that it can generate for each message. When a node violates its rate limiting, a claim is generated as an alarm, and each node receiving the alarm must check for the inconsistency between the received claims.	False claims and inconsistency of the received claims.
Encounter Records (History of encounters) (ERs) scheme[14]	This scheme is based on recording the history of encounters. In order to record the messages sent during previous contacts, nodes must exchange their ER (Encounter Record) history. Malicious nodes will be identified, resulting in a flooding attack.	Removing favorable ERs. ERs falsification and modification.
Stream-Check scheme[14]	The streaming node is used in this scheme to monitor the network environment. Three tables must be maintained by the monitor node. The first contains the rate limits of all nodes in the network, the second contains the delivery probability of each node in the network, and the third contains the blacklisted nodes. The streaming node compares estimated probability of delivery to actual probability of delivery; if the difference is greater than the assigned limit value, the node is added to the blacklist by the streaming node.	A large number of resources are required by the streaming node.

III. THE PROPOSED MECHANISM TO CONTROL THE DISTRIBUTED FLOODING ATTACK

In this paper we are interested in the first type of DOS [12] (saturation of a node's buffer) in the DTN network because it appears to be more severe than the second due to DTN's scarcity of resources. Consider the scenario in which the attack is launched from multiple DTN nodes. In a brief, we are interested in a distributed flooding attack. This attack is carried out by several network nodes with the goal of disrupting the availability service of the nodes. The figure below (Fig. 4) depicts a node's inability to transmit messages due to the saturation of its buffer by unwanted bundles (bundles mean messages in DTN network).

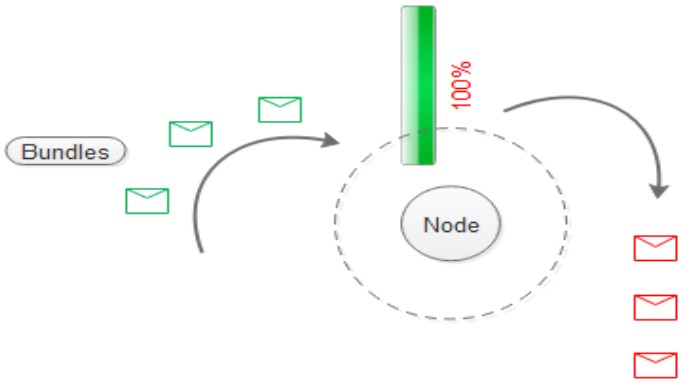


Fig. 4. Unwanted Bundles Saturating a DTN Node's Buffer.

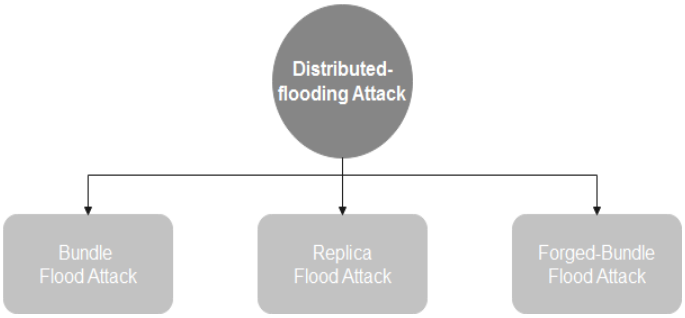


Fig. 5. Classification of the Flooding Attack.

The flooding attack [15] [16] can be classified into three types based on the type of bundles, as shown in the figure below (Fig. 5):

- Bundle-Flood Attack: when the attacker nodes flood the network by normal messages.
- Replica-Flood Attack: when the attacker nodes flood the network by replicas of each message.
- Forged Bundle-Flood Attack: when the attacker nodes flood the network by fake messages.

A. Our Assumptions

- A partition of the network is affected all by distributed flooding attack.
- Malicious nodes flood the network by bogus bundles, so we need to filter the traffic by filters.
- There are three groups of bundles which circulate into the network: Normal Bundles, Replica Bundles and Forged Bundles.
- Nodes are classified into three main groups, Nodes that are nearer to their destinations, they transfer very important (urgent) bundles, Nodes that are partially near to their destinations, they transfer important but not urgent bundles and finally, nodes that are far to their destinations, they transfer unimportant bundles.
- According to the priority of each bundle into the network, bundles are classified into three main groups: Urgent bundles, important bundles, and unimportant bundles.

TABLE III. TABLE OF THE USED NOTATIONS FOR OUR PROPOSED WORK

Notation	Signification
N	The total number of nodes in the network
TTL (Time To Live)	Bundle lifetime
di, i= {1,2,3}	Node classes based on their proximity to the destination with (d1<d2<d3).
Pi, i= {1,2,3}	Priority classes of bundles.

B. Our basic Idea

Each DTN node generates different bundles and then commits to prioritizing them as follows (More information about the notations used can be found in Table III):

- It classifies messages that are very important (urgent) in the set P1.
- It classifies the messages that are important but not urgent in the set P2.
- It classifies the messages that are less important than P2 in the set P3.

Nodes are classified into three categories based on their distances from the destination nodes: d1, d2 and d3 with (d1<d2<d3).

- Nodes that are closer to the destination, their distance to the destination is d1.
- Nodes that are partially close to the destination, their distance to the destination is d2.
- Nodes that are far away from the destination, their distance to the destination is d3.

The priority of each message is determined according to its lifetime (messages with a short TTL have a high priority because they must be transmitted before their TTL expires), its size (messages with a smaller size have a high priority than large messages because the latter may saturate the limited storage space) and its number of replicas (Messages with a small number of replicas have a higher priority than messages with a large number of replicas).

The distance of each node from its destination is determined by referring to the movement history of the DTN nodes (the hop-by-hop count taken before arriving at the destination). The value of this distance is predictive because DTN nodes are mobile.

Our basic idea is first to distribute the bundles to the various nodes based on their priorities in the following manner:

- The nodes whose distance to the destination is d1 agree to receive only messages with priority P1 and agree to forward them to their destinations.
- The nodes whose distance to the destination is d2 accept to receive only the messages of priority P2 and agree to transfer them to their destinations.
- The nodes whose distance to the destination is d3 accept to receive only the messages of priority P3 and agree to forward them to their destinations.

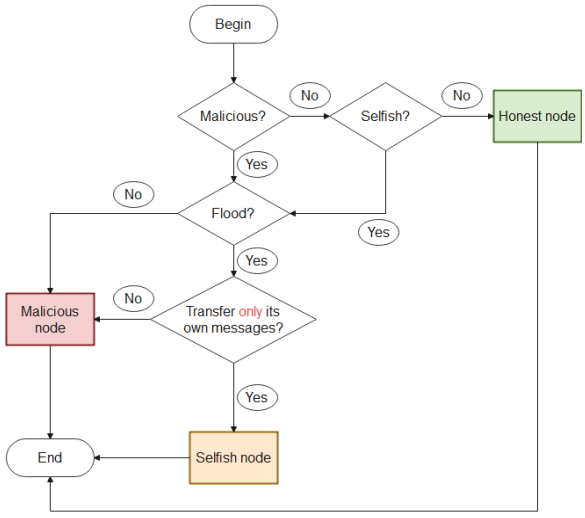


Fig. 6. Overall Flowchart.

Then, to identify malicious nodes that flood the network by unwanted bundles, we have proposed an effective scheme (see the below flowchart, Fig. 6).

C. The Objectives of our Proposed Work

1) Identify the nodes that flood the network with unwanted messages so that the other nodes in the network do not accept their messages the next time they contact them.

2) Reduce and optimize the network load by categorizing nodes and messages (as explained above in section 3). When exchanging messages between two neighboring nodes, it is not necessary for the receiver node to accept all the messages from the sender node; instead, it must accept a subset of these messages based on its type (close to the destination or not) and based on the priority class of the messages (P1, P2 or P3).

IV. SIMULATION AND ANALYSIS

The ONE (Opportunistic Network Environment Simulator) simulator [17] is an opportunistic networking simulator that provides several tools for creating complex mobility scenarios that are more realistic than many other synthetic mobility models. ONE supports various node movement models and simulates a variety of DTN routing algorithms. The ONE simulator is written in Java, and it allows to add routing algorithms by extending the built-in routing classes.

A. Simulation Environment Setup

The ONE simulator (Opportunistic Network Environment Simulator) [17] was used, as shown in Fig. 7. Our scenario includes a network of 140 DTN nodes (an average density): 120 pedestrians and 20 trams. The simulation time was 12 hours, with a 0.1 second update interval. The effect of changing the buffer capacity, bundle lifetime, bundle size and bundle replicas on flooding protocols was investigated. To make our simulation more realistic, we used a cluster-based mobility model with three clusters or regions (each cluster can be a remote village) spread across an area of 4.5 × 3.4 Km. The pedestrians within each cluster were moving at a speed ranging from 0.5 to 1.5 m/s. See the table below (Table IV) for more information on the simulation parameters that were used.

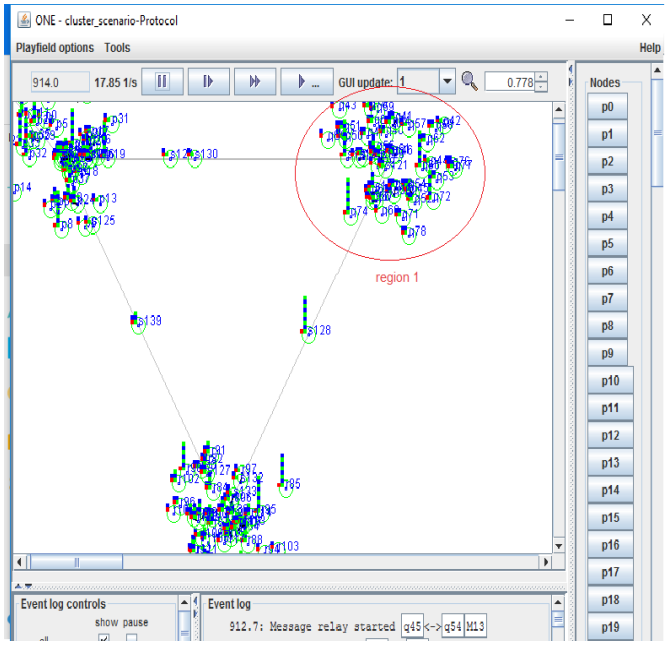


Fig. 7. The Screenshot of our Scenario on the ONE Simulator's GUI.

TABLE IV. SIMULATION PARAMETERS

Parameter name	Value(s)
Simulation time	43200s
Number of Nodes	140
TTL	60Min-300Min (step 60)
BufferSize	20MB-180MB (step 20)
MsgSize	50kB-550kB
NBOfReplicas	20-100 (step 20)
movementModel	ClusterMovement
RoutingProtocols	Epidemic, Spray & Wait, Binary-Spray & Wait

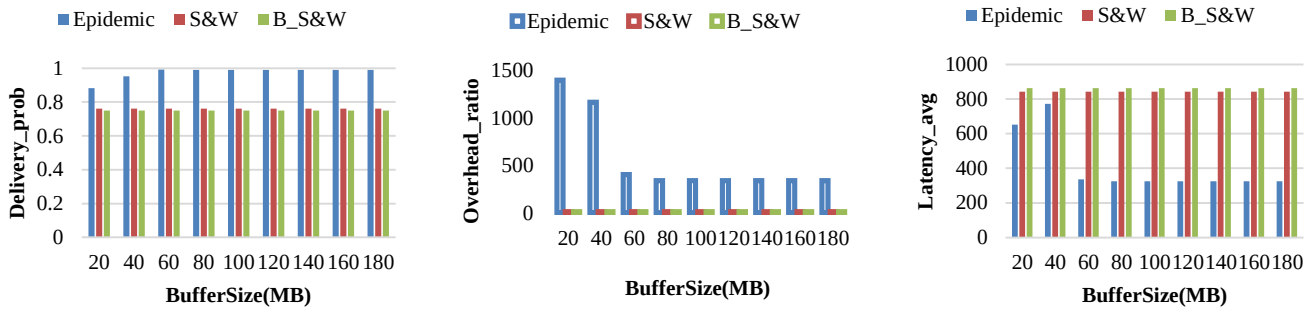
The following performance metrics are considered in analyzing the effect of changing buffer capacity, bundle lifetime, bundle size, and number of replicas on the flooding protocols:

- Delivery_prob: this metric describes the probability of message delivery at the end of the simulation. It is also known as the delivery ratio because it is the ratio of delivered messages to created messages. One of the primary goals of the DTN network is to maximize the value of this parameter. This metric's value is scaled in [0,1]. It is computed using the following formula: (NumberOfDeliveredMessages/NumberOfCreatedMessages).
- Overhead_ratio: it denotes a bandwidth efficiency evaluation during the simulation. The primary goal of the DTN network is to reduce the value of this metric. It is computed using the following formula: ((NumberOfRelayedMessages-NumberOfDeliveredMessages)/NumberOfDeliveredMessages).
- Latency_avg: it is the average message delay from the time a message is created at the source to the time it is delivered to the destination. In a DTN network, the terms delay and latency are used interchangeably. The DTN network's primary goal is to reduce the value of this metric.

B. Simulation Results and Discussions

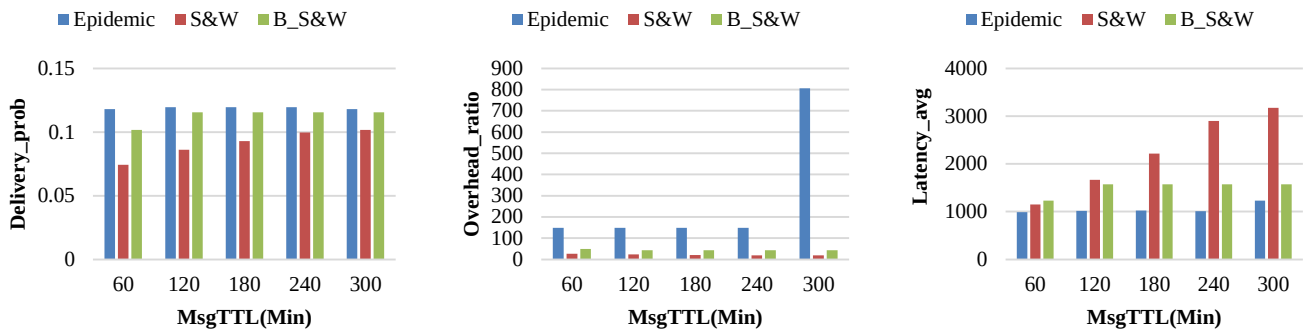
a) The impact of BufferSize on flooding-based routing protocols

Fig. 8 (a) depicts the delivery probability obtained by using the flooding-based routing protocols: Epidemic, Spray & Wait (S&W), and Binary-Spray & Wait (B-S&W) in terms of BufferSize (MB). When the Epidemic routing protocol is used, the delivery probability increases with the increase of the BufferSize (MB) since buffer space means more nodes can carry more copies of messages, as opposed to the B-S&W and S&W routing protocols, which have approximately similar invariant values. This is because the Epidemic protocol's message transmission logic necessitates a large buffer size as compared to the B-S&W and S&W routing protocols. While the overhead-ratio falls (Fig. 8 (b)) particularly when using the Epidemic protocol. This is due to an increase in buffer size, which means more free space is available to transmit and to carry more messages. Fig. 8 (c) shows that when using the Epidemic protocol, the average latency decreases as the buffer size increases thanks to the multiple-copy nature of this protocol, which spreads replicas blindly, as opposed to the spraying protocols (S&W and B-S&W), which spread limited replicas into the network. Briefly, the Epidemic protocol benefits the most because its process of exchanging messages is quick, lowering average latency, thereby improving performance.



(a) (b) (c)

Fig. 8. The Effect of Changing the Buffer Size on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).



(a) (b) (c)

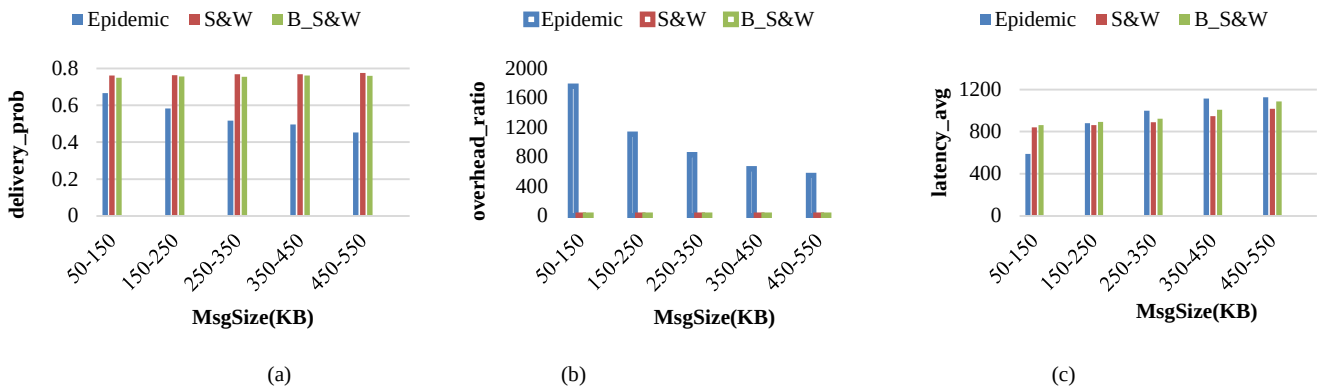
Fig. 9. The Effect of Changing the Message TTL on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

b) The impact of MsgTTL on flooding-based routing protocols (with BufferSize=5M)

Fig. 9 (a) shows that there is some progress in delivery probability as message TTL improves but the value of Delivery probability does not exceed 0.2 for the three protocols because messages with high MsgTTL values are classified as P3 Priority class (not important messages for transmission, see the third section) which lowering the delivery ratio. Furthermore, messages with a high MsgTTL value have a high chance of being delivered because these messages tolerate long RTT (Round Trip Time). However, increasing MsgTTL leads to an improvement in the network's overhead ratio, as shown in Fig. 9 (b). The epidemic protocol has higher values than the other protocols because it is possible that the replicas of each delivered message are still circling in the network, which increase the overhead ratio. Fig. 9 (c) depicts the effect of message TTL on average latency. The average latency for the three protocols has higher values. When the message lifetime is long, the average latency increases significantly. This behavior is easily explained by the fact that when a message has a large TTL value, it means that the transmission of this message is not a critical or urgent task. According to the third section, the priority class of the message is P3, and the nodes whose distance to their destinations is d3 are the nodes who accept to receive and transmit that category of messages. Because these nodes are so far away from their destinations, the average latency rises, which conform to our assumptions (see the third section).

c) The impact of MsgSize on flooding-based routing protocols (with BufferSize=5M)

Fig. 10 (a) shows the effect of varying Message size on the delivery probability for flooding-based routing protocols. When the message size increases, it seems that the delivery probability significantly decreases especially in the case of using Epidemic as a routing protocol, but it does not have much effect on the other protocols (S&W and B-S&W). Increase message size, reduce the limited buffer size, and make congestion and cause continuous buffer space occupation. Which force relay nodes to accept to store only a small number of messages in their buffers, lowering the delivery rate. According to our assumptions, messages with a small size have a higher priority than messages with a large size. As a result, the delivery ratio has low values when large messages circulate in the network (as Fig. 10 (a) depicts). The priority class of messages with large sizes is P3, and the nodes transmitting these messages are far from their destination nodes (with distance d3), which explains the decrease in the delivery probability (see the third section). Fig. 10 (b) shows how changing the size affects the overhead ratio. As we can see, increasing the message size reduces the overhead ratio, especially when using Epidemic routing protocol. The overhead ratio is defined as ((NumberOfRelayedMessages-NumberOfDeliveredMessages)/NumberOfDeliveredMessages) , and as shown in Fig. 10 (a), the delivery ratio decreases as message size increases, implying that the number of relayed messages decreases as MsgSize increases. This behavior can be explained by the loss of large messages. Therefore, to avoid saturating their buffers, nodes rarely accept large messages (these large messages have a low priority class P3), resulting in a decrease in the delivery rate and a decrease in the network overhead ratio that can only be explained by the loss of large data. However, because large-sized messages are considered to have the lowest priority class (P3) according to our assumptions, and the nodes whose distance to their destinations is d3 are the nodes who accept to receive and transmit this category of messages, and because these nodes are so far away from their destinations that their transmission will take a long time, the average latency increases which conform to our assumptions see Fig. 10 (c)).



(a) (b) (c)

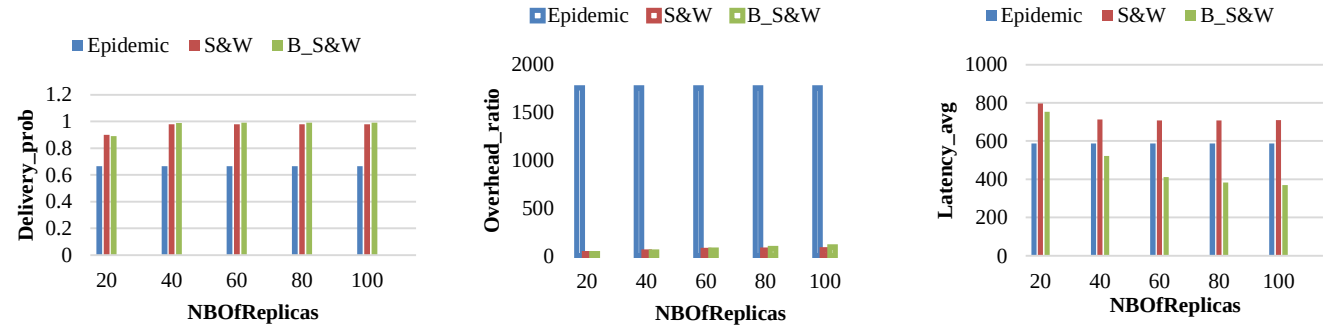
Fig. 10. The Effect of Changing the Message Size on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

d) The impact of NBOfReplicas on flooding-based routing protocols (with BufferSize=5M)

Fig. 11 depicts the message delivery, network overhead, and latency ratios when flooding-based routing protocols were used with different replica number values. The delivery rate, overhead ratio, and latency average for the Epidemic protocol are invariant to the number of replicas, which is due to the nature of this protocol, which floods the network with an unbounded number of copies (replicas); in comparison to the spraying protocols (Spray & wait protocol and Binary-spray & wait protocol), it has a higher value of the overhead ratio because it floods the network with unlimited replicas and the buffer space is limited in size (5M). As a result, we will concentrate on the comparison between Spray &Wait protocol and Binary-Spray &Wait protocol. For S&W and B-S&W the delivery rate shows an increasing trend up to a certain extent beyond which it saturated but B-S&W has higher values of delivery probability compared to S&W, see Fig. 11 (a). Fig. 11 (b) shows that the overhead ratio for S&W is invariant to the number of replicas, whereas the overhead ratio for B-S&W always increases continuously with the increase of the number of replicas. Messages with a small number of replicas have a higher priority than messages with a large number of replicas, according to our assumptions, and nodes whose distance to their destination is d1 (close to the destination) agree to receive and to forward only messages with priority P1 (highest priority class). This means that as the number of replicas increases, the delivery probability must decrease (because messages are transmitted by nodes located far from their destinations) and the overhead must increase. Fig. 11 (a) shows, however, that the increase of the number of replicas leads to the increase in the probability of delivery, which contradicts our assumption. Fig. 11 (b), on the other hand, depicts the increase in overhead as the number of replicas increases, which is a natural result of the increase in delivery probability (as shown in Fig. 11 (a)). Fig. 11 (c) shows that as the number of replicas increases, the average latency decreases, particularly when using the B-S&W, implying that nodes have a short Round Trip Time (RTT) before being delivered to their destinations.

e) Message Graphs by using graphviz (with MsgTTL=60min)

The graphs below (Fig. 12, Fig. 13, Fig. 14) depict the node connections as well as the network paths that the delivered messages took. The MessageGraphviz [18] report module creates directed graphs of delivered message paths. The figures below show three examples of delivered messages graphs that contain all the messages sent from one network node to another during the simulation (Fig. 12, Fig. 13, Fig. 14). The figures show an example of a message graph, which contains all the messages sent from node to node during the simulation.



(a) (b) (c)

Fig. 11. The Effect of Changing the Number of Replicas on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

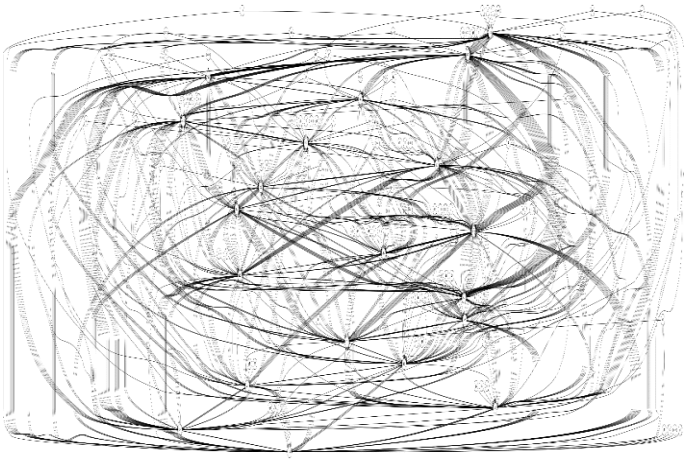


Fig. 12. Graph of the Messages that were sent from r113 to s128 for Epidemic Routing Protocol (173 Messages Delivered).

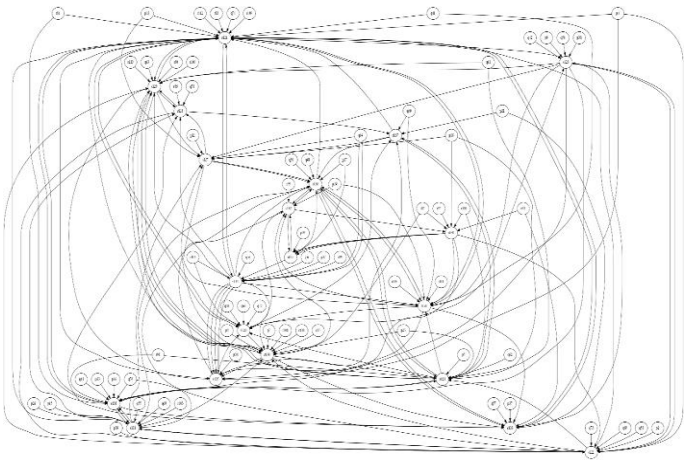


Fig. 13. Graph of the Messages that were sent from r112 to s121 for Spray and Wait Routing Protocol (109 Messages Delivered).

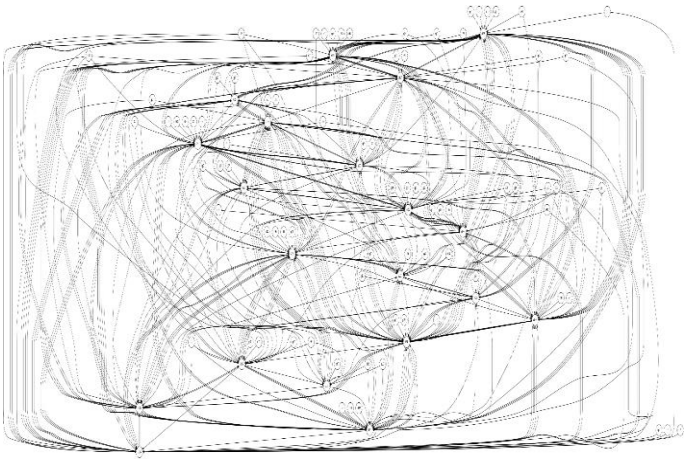


Fig. 14. Graph of the Messages that were sent from r113 to s128 for Binary-Spray and Wait Routing Protocol (149 Messages Delivered).

The graphs show that the Epidemic routing protocol's delivered message graph (Fig. 12) has more edges than the other graphs (when using the S&W and B-S&W protocols), resulting in an increase in delivered messages when using the Epidemic protocol, as evidenced by the way Epidemic protocol messages are transmitted.

V. Conclusion

Security is still a major concern in the Delay Tolerant Network. The DTN network lacks a centralized authority in charge of network filtering, and each mobile network node functions as both a router and a host. Malicious nodes can quickly flood the network with unwanted messages. Flooding attacks, in particular, disrupt the availability of network services. In this paper, we have proposed a security mechanism for controlling the distributed flooding attack, as well as a security scheme for detecting malicious nodes that flood the network. Then, in terms of three important metrics: delivery probability, overhead ratio, and latency average, a comprehensive study of the impact of changing buffer capacity, message lifetime, message size, and message replicas on flooding-based routing was presented. The simulations validate our most important hypotheses. In future work, we intend to improve our mechanism for dealing with flooding attack in order to improve the network performance in DTN, and we intend to design and implement a collaborative trust management protocol with an integrated buffer management scheme for dealing with flooding attack.

References

[1] P. M. Jawandhiya, M. M. Ghonge, M. S. Ali, and J. S. Deshpande, "A survey of mobile ad hoc network attacks," Int. J. Eng. Sci. Technol., vol. 2, no. 9, pp. 4063–4071, 2010.

[2] F. Warthman, "Delay-and disruption-tolerant networks (DTNs)," Tutor. V 0 Interplanet. Internet Spec. Interest Group, pp. 5–9, 2012.

[3] V. Kushwaha and R. Gupta, "Delay tolerant networks: architecture, routing, congestion, and security issues," in Handbook of research on cloud computing and big data applications in IoT, IGI Global, 2019, pp. 448–480.

[4] P. Kumar, N. Chauhan, and N. Chand, "Security framework for opportunistic networks," in Progress in Intelligent Computing Techniques: Theory, Practice, and Applications, Springer, 2018, pp. 465–471.

[5] P. K. BVSP, S. Sarma, and G. B. Prasad, "A BRIEF SURVEY ON SECURITY IN DELAY/DISRUPTION TOLERANT NETWORKS," Int. J. Pure Appl. Math., vol. 118, no. 14, pp. 157–162, 2018.

[6] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks–a survey," Comput. Commun., vol. 51, pp. 1–20, 2014.

[7] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "RFC3647: Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." RFC Editor, 2003.

[8] E. P. Jones and P. A. Ward, "Routing strategies for delay-tolerant networks," Submitt. ACM Comput. Commun. Rev. CCR, vol. 1, 2006.

[9] R. Wang, Z. Wang, W. Ma, S. Deng, and H. Huang, "Epidemic Routing Performance in DTN with Selfish Nodes," IEEE Access, vol. PP, pp. 1–1, May 2019, doi: 10.1109/ACCESS.2019.2916685.

[10] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking - WDTN '05, Philadelphia, Pennsylvania, USA, 2005, pp. 252–259. doi: 10.1145/1080139.1080143.

[11] J. A. Davis, A. H. Fagg, and B. N. Levine, "Wearable computers as packet transport mechanisms in highly-partitioned ad-hoc networks," in Proceedings Fifth International Symposium on Wearable Computers, 2001, pp. 141–148.

[12] P. Pathak, A. Shrivastava, and S. Gupta, "A Survey on Various Security Issues in Delay Tolerant Networks," J. Adv. Shell Program., vol. 2, no. 2, pp. 12–18, 2015.

[13] D. S. Eswari, "A Survey On Detection Of Ddos Attacks Using Machine Learning Approaches," Turk. J. Comput. Math. Educ. TURCOMAT, vol. 12, no. 11, pp. 4923–4931, 2021.

[14] M. Shah and P. Khanpara, "Survey of Techniques Used for Tolerance of Flooding Attacks in DTN," in Information and Communication Technology for Intelligent Systems, Springer, 2019, pp. 599–607.

[15] R.-T. Lee, Y.-B. Leau, Y. J. Park, and M. Anbar, "A Survey of Interest Flooding Attack in Named-Data Networking: Taxonomy, Performance and Future Research Challenges," IETE Tech. Rev., pp. 1–19, 2021.

[16] K. Salunke and U. Ragavendran, "Shield Techniques for Application Layer DDoS Attack in MANET: A Methodological Review," Wirel. Pers. Commun., pp. 1–27, 2021.

[17] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," presented at the 2nd International ICST Conference on Simulation Tools and Techniques, Rome, Italy, 2009. doi: 10.4108/ICST.SIMUTOOLS2009.5674.

[18] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in Proceedings of the 2nd international conference on simulation tools and techniques, 2009, pp. 1–10.