BiRep: A reputation scheme to mitigate effects of black-hole nodes in Vehicular Delay-Tolerant Networks

Catarina França Martins Rolão Nabais
Instituto Superior Técnico
Lisboa, Portugal
catarina.franca.martins.rolao.nabais@ist.utl.pt

***Abstract*—Delay-Tolerant Networks (DTNs) are networks that enable communication in disruptive scenarios where issues like sparse and intermittent connectivity, long and variable delays, high latency, high error rates or no end-to-end connectivity exist. Vehicular Delay-Tolerant Networks (VDTNs) are DTNs where the nodes are vehicles. VDTNs emerged and became a popular research topic due to the important applications that can be realized with them, such as notification of traffic conditions and road accident warnings. For VDTNs to work efficiently, a grade of cooperation between nodes is necessary in order to deliver the messages to their destination. However, nodes might misbehave and not transmit messages. Nodes misbehavior may significantly impact the network performance, being an important problem to study in the context of VDTNs. One of the most studied attacks is the black-hole attack where a node drops forwarded messages in which it is not the destination. Various solutions have been proposed to diminish the effects of black-hole nodes but not one yet that was proven fail-proof, and tested for various scenarios. In this sense, this paper focuses on creating a reputation scheme that identifies and punishes black-hole nodes in the network. The reputation scheme, denominated BiRep, is tested Prophet protocol and for seven different network scenarios. Simulation results show very good performance for Prophet in all scenarios, comparable or better to other reputation schemes comprised in this study. Most importantly, they show a significant increase in delivery ratio of messages.**

Keywords—Wireless communication, Delay-Tolerant Networks, Vehicular Delay-Tolerant Networks, Black-hole attack

I. INTRODUCTION

Nobody can deny the importance of internet nowadays. Specially in the times that we are now living, the internet has proven itself fundamental to connect not only communication devices, but us, across the Earth. The internet works using a homogeneous set of communication protocols. The devices on the networks that compose the internet use these protocols to communicate with each other, routing data and insuring the reliability of message exchanges. The usability of the Internet depends on various assumptions, but one of the most important is the fact that a continuous bidirectional end-to-end path must be established. What if an end-to-end path is not available? What if the connection is so long that it is hard to have an effective data transfer? Firstly, introduced to deal with large delays and data loss in interplanetary communications, Delay-Tolerant Networks (DTNs) were created to deal with these challenging scenarios and environments. But the potential applications on Earth are many. For example, in a natural disaster area, where no end-to-end connection can be established and internet access fails, the ability to communicate can literally save lives. In addition, wildlife tracking/monitoring sensor networks, communication in remote and rural areas, developing countries and vehicular communications are scenarios that benefit from Delay-Tolerant capabilities [1]. The last application is especially interesting for the real and fast implications it might have on our lives. Vehicle to vehicle and pedestrian to vehicle communication is already a reality and Vehicular Delay-Tolerant Networks (VDTNs) have delay-Tolerant capabilities to support long disruptions in network connectivity [2]. Some examples of applications of these networks are optimizing traffic flow and road capacity, software and map update optimization, commercial applications such as tourist and leisure information, parking space availability, but most importantly, assisting in communication between emergency services in areas lacking conventional communication.

For VDTNs to work and be efficient, cooperation between nodes of the network is necessary, but it cannot be expected. Since nodes might not transmit the messages they receive. Either because they are being controlled by a malicious user, they are lacking resources or, themselves are malicious and do not want to send messages from other network nodes, only wanting to receive messages for themselves. This latter case is called a black-hole attack. The node refuses to transmit any message in which it is not the source and deletes any messages it receives where it is not the destination. Black-hole attacks are one of the most studied attacks in vehicular delay-tolerant networks and although there are already some proposed solutions, none of them is bulletproof or tested for a vast number of scenarios. In this sense, this work tries to present an effective and robust reputation scheme to detect and diminish the effect of black-hole nodes in the network..

II. BACKGROUND

In this section, a brief description of the theoretical background for this work is given. Firstly, DTNs are addressed. Then, an overview of VDTNs fundamental concepts are presented.

Black-hole attacks are presented and some solutions already presented. Finally, the simulator chosen for the tests: The ONE is addressed.

A. Delay-Tolerant Networks

In most of the networks nowadays, an end-to-end path is assumed to exist as well as permanent and unlimited connectivity to the Internet for mobile and fixed devices. The nodes of the networks exchange topology information or have it stored and send messages along the existing paths, using different types of routing protocols. Even when a connection fails, there are other paths to reach the destination, allowing the information to be forwarded between any pair of nodes making the general delivery ratio high. However, this is a limited assumption, since there are disruptive scenarios where connectivity issues like sparse and intermittent connectivity, long and variable delays, high latency, high error rates, highly asymmetric links and no end-to-end connectivity exist [1]. For applications in this type of scenarios to have interoperability,

it is necessary to have a network architecture that can handle these problems, so DTNs began to be developed [3].

A typical Internet request using transmission control protocol (TCP) would require three round-trip times (RTTs) (one for name translation to an address, one for establishing the TCP connection and one for the first request), and once this was made, additional requests would be sent to retrieve additional necessary objects requiring other RTTs and some transfer time [1]. This type of protocol interaction in a challenging scenario would probably never complete successfully, so a special communication protocol, called the Bundle Protocol [4], was proposed for DTNs. With the Bundle protocol, a request message bundles together all information required for an application request and to resolve the address. All the parts of the answer are also bundled together in a response message [1]. Once the bundle, that is the message that we want to deliver, is ready, there is still the problem of how to carry it through the network that has no end-to-end connectivity. For this, a store-carry-and-forward (SCF) approach is used. Please note that, in this work, often message and packet are used with the same meaning as bundle.

Nodes store their messages while there is no contact opportunity. Once a contact is established, the message is sent, and a copy may be kept. The node that received the message will carry it through the network until a new contact is made, repeating the store-carry-and-forward mechanism until the destination is met. In this case, a response bundle may be created, if necessary, and the process repeats. Furthermore, to prevent overloading the network, bundles have a time expiration, being deleted when their useful lifetime expires.

B. Vehicular Delay-Tolerant Networks

Vehicular Delay-Tolerant Networks (VDTNs) are DTNs where the nodes are vehicles. This concept was developed having in account studies made with Mobile Ad Hoc Networks (MANETs), Vehicular Ad Hoc Networks (VANETs) and DTNs. The MANETs bring the concept of establishing direct communication between mobile nodes, which do not rely on fixed infrastructure [5]. VANETs use vehicles as nodes but contrary to VDTNs, they assume end-to-end connectivity exists through some path, which can be particularly challenging in high mobility scenarios or in very sparse scenarios such as rural or mountainous areas [1]. This is where the DTNs capabilities are brought in, since in these environments the traffic density is usually low, meaning less opportunities for contact and since the vehicles travel at a considerable speed, the contacts also will be short. One can say that VDTNs extend VANETs with delay-tolerant capabilities to support long disruptions in network connectivity [1].

VENIAM is a company that is presently already implementing services using the VDTN strategy, like Wi-Fi offloading [6].

C. Routing in Vehicular Delay-Tolerant Networks

In VDTNs, since there is no end-to-end connectivity, routing cannot be done in the traditional Internet sense nor using the algorithms designed for MANETs or VANETs.

Forwarding in VDTNs is done using the Bundle Protocol. However, it is not described in the protocol how to set up routes between nodes [1]. Plenty of applicable routing protocols were developed. Routing protocols in the next sections will be classified according to the number of copies of each message that are circulating in the network, as single-copy versus multiple-copy.

*1) Single-Copy Routing Protocols:*Single-Copy routing protocols maintain a single copy of a message circulating in the entire network, being passed on between nodes until being deleted or the destination is met.

Direct Delivery

In Direct Delivery (DD) [7], each bundle message is stored and carried by the source until its destination is met. No network information is necessary to make the forwarding decision.

First Contact

In First Contact (FC) [8] each bundle is sent by the source to the first random node encountered and then deleted from the source's buffer, being routed in the same manner by the other nodes, resulting in a random search for the destination. Because of the random character of the protocol, no network information is necessary to make forwarding decisions.

2) Multiple-Copy Routing Protocols: Multiple-Copy routing protocols, as the name indicates, can have more than one message copy circulating in the entire network. The number of message copies might be unlimited or limited..

Epidemic

In the Epidemic protocol [9], nodes at any contact opportunity try to change bundles which they do not have in common between them, flooding the network with an unlimited number of copies of each message to reach the destination.

Spray-and-Wait

Spray-and-Wait (SnW) [10] has two phases: spray phase and wait phase. For the common Spray-and-Wait, the spray phase consists of, for every message originating at a source node, a chosen number of message copies, let us say L messages, are spread to the first L different passing nodes. If the destination is not found in the previous phase, the wait phase begins, where each of the L nodes carrying a message copy performs DD.

PRoPHET

Using the PRoPHET protocol [11], when two nodes are in contact, a new message copy will only be forwarded if the other node has a higher delivery probability to reach the destination. This probability is calculated using the past encounter history and transitivity. The transitive property is based on the observation that if node A frequently encounters node B, and node B frequently encounters node C, then node B probably is a good node to which to forward bundles destined for node A [11].

D. Attacks in Vehicular Delay-Tolerant Networks

The protocols described in the previous section demonstrate that a grade of cooperation between nodes belonging to VDTNs is necessary in order to deliver the messages to their destination. However, nodes might misbehave. The misbehavior of nodes may significantly impact the network performance as shown in [12], being an important problem to be studied in the context of VDTNs.

One of the most studied attacks is the black-hole attack. The impact on the network that results from this type of attack can vary, affecting the normal functioning of routing protocols in VDTNs.

Not only the impact black-hole attacks can have in a network but also the fact that is commonly studied within the DTN research community, show how important it is to prevent this attack. This work will focus in black-holes attacks in an attempt to identify nodes who perform this attack and decrease their effect in the network.

E. *Black-hole solutions in Vehicular Delay-Tolerant Networks*

Various mechanisms have been introduced to address black-hole attacks in DTNs.

One of the first solutions proposed was ferry-based intrusion detection and mitigation (FBIDM) [13]. In FBIDM, special nodes referred to as ferry nodes provide intrusion detection services to regular nodes. Ferry nodes travel regularly along the network in fixed paths and stop at various locations within their routes. At each location, a ferry broadcasts a secret service message that each legitimate node knows how to decipher. After receiving the message, each regular node shares some encounter and delivery predictability information it has with the ferry node. The ferry correlates the information from all nodes to identify potential malicious nodes. If a node is declared suspicious a certain number of times, the ferry will put this node in the blacklist that is broadcasted periodically. After receiving the information from the ferry, regular nodes update their own blacklists and will not choose any nodes in the blacklist as the next hop node. FBIDM overall performance is good, but is only suited for protocols that use information to route, like PRoPHET or Maxprop, since it requires the encounter and delivery information to make decisions. Furthermore, the dependency in the ferry node is a big problem. If the ferry node fails or misbehaves itself, the network becomes compromised.

A similar solution is presented with the mutual correlation detection scheme (MUTON) [14]. MUTON is similar to FBIDM but considers the transitive property when calculating the delivery probability. Despite the improvements, the problems associated with having a ferry node persist.

In [15], the authors proposed a Misbehavior Detection System (MDS) that uses encounter records (ER), that are similar to encounter tickets. When two nodes meet, a w number of ER are exchanged and used to assess a node's trustworthiness. The ERs are created after transmitting messages to another vehicular node. The ER includes both node's identifiers, unique sequence number from both vehicles that increases by one after each contact and a set that identifies the transmitted messages. Additionally, each node stores two lists in its memory, the Meeting List (ML) and the Local Black List (LBL). The ML stores the information from previously encountered nodes. Each ML entry includes the information of the identifier ID of the encountered node, the unique sequence number of the encountered node, the time of the contact and the trust reputation (TR) assigned to the encountered node. The entries can be used to check the validity of ERs later, as they store the last known combination of unique sequence number and time of encounter, t, of a certain node. It is expected that without any forged ERs, the greater a sequence number is for a given ID also implies a greater t. The LBL stores all malicious nodes locally detected by a node. Nodes will refuse to transfer or receive messages from nodes in the LBL. However, nodes in the LBL have an expiration time. The expiration time is implemented so to incentive misbehaving nodes to participate in the network. When the time in the LBL expires, a node is allowed back to the network, but it is on "probation", meaning it starts with a lower initial TR than other nodes that have just joined the network. The MDS system can be decomposed into two main components, the evaluation module and the decision module. In the evaluation module, vehicular nodes assess the trustworthiness of other vehicular nodes and the TR is updated. The decision module is responsible for making an appropriate decision after nodes receive an updated TR. The MDS achieves high detection rates, of over 90% and almost null false positive rates. Yet, it is important to notice that since trustworthiness is calculated upon contact based on the exchanged ERs, nodes that never meet will not be able to assert each other's trustworthiness. This means that a malicious node in the network might not be detected by all other nodes. This can be a problem since upon a new encounter, as a node does not have information about the level of trust that the encountered node has, but other nodes in the network might already have determined that the node has a malicious intent. Moreover, this scheme detects individual attackers well, but they cannot handle the case where attackers collude. This is because a node is considered malicious if its forwarding ratio, which is the total number of messages that are sent out by a node in a certain number of ERs over the total number of messages received by it, is lower than a threshold. If attackers cooperate creating valid ERs and a good forwarding ratio, the malicious behavior can be undetected. In [16] the authors extend the MDS with the idea of cluster analysis, which allows a better discrimination between good and malicious behavior, but the problems found in MDS [15] still occur.

In [17], the authors propose to keep packet delivery records instead of ERs to detect the black-hole attack. A packet delivery record includes the identification of the nodes that exchanged packets, the number of received packets from the encountered node, the number of forwarded packets to the encountered node and the current time-stamp in the record. The un-forgeable packet is generated using the private key at each node, since it is assumed that each node in the network is issued a private key and public key pair and that each node possesses other node's public keys. Each node has two specific tables in its memory, a receiving record table (RRT) and a self record table (SRT). The RRT maintains the most recent packet records generated by its encountered nodes. The SRT keeps the most recent packet records it generates for each node encounter. Each entry contains the encountered node ID and the time when the encounter happened. The scheme begins when two nodes meet. Each node requests the other node's RRT. With the RRT, a node can determine the packet exchange information between the encountered node and other nodes during previous encounters and calculate a packet forwarding percentage. Although with a different name, the packet forwarding percentage is equal to the definition of forwarding ratio described above. If the packet forwarding percentage is less than a threshold, it indicates that the encountered node may selectively drop packets and is listed as a suspicious node. The RRT is used for a sanity check. If the threshold condition is passed, the SRT is used to determine whether the encountered node dropped packets generated previously by this node. This detection is made by a node comparing the RRT of the encountering node to its own SRT. If some records in the node SRT do not have corresponding entries in the encountering node's RRT, the node will conclude that some records were dropped and list the node as suspicious. If a node is listed as suspicious more than m times, it is declared as a malicious node. When both the packet forwarding percentage and comparison between RRT and SRT are validated, the nodes exchange packets and generate packet records. This method of detecting black-holes has a detection rate, defined as the percentage of malicious nodes that are detected by detection schemes, for different mobility schemes of over 85% and false positive rate of less than 1%. Although it can detect packet dropping which [15] and [16] could not, it still suffers from the same problems.

Furthermore, in [17] no punishment mechanism is described to identified malicious nodes, or a reward to well behaved nodes. Without punishment, malicious nodes do not have an incentive to cooperate in the network.

One scheme, called RCAR [18] does not detect black-hole attackers but limits the effects of their presence. This scheme also presents some interesting ideas. Such as previously described schemes, the node maintains a local notion of reputation. Every message carries the list of forwarding nodes the message has passed by. RCAR keeps track of the nodes a message has passed through as such. Every message carries the list called nlist of the identifiers of nodes the messages has passed through. When a node receives a message, it adds itself to the nlist. If the message passes more than one time in the same node the name is not added again. To avoid that malicious nodes, add or modify identifiers, the message also carries a list, called slist, of digital signatures that proves that the message has actually passed through the nodes specified in the nlist. When a node receives a message, it updates the reputation of the forwarding nodes specified in the lists. After, when the node forwards a message, it starts waiting for an acknowledgment from the destination. The destination node builds an acknowledgment (ACK) message and sends it back to the sender. The nlist and slist of the ACK are initialized with the nlist and slist of the original message. The ACK message is also updated along the path to the initial sender. An ACK behaves as a normal message that can follow a different path of the one taken by the original message, so different nodes can contribute to its forwarding. When the original sender receives the ACK message, it verifies the nlist and slist. If the check is successful, the sender updates the reputation of all the nodes contained in the lists. Some problems are found in the scheme. If a message gets lost, a node has no means to know whether a black-hole has dropped it or a node had no buffer space. Furthermore, a node can know that a message has not been delivered but does not know exactly which node dropped it. To manage this situation, a mechanism based on aging is used to decrease the reputation of all nodes periodically. This is done to have a conservative policy, because a node does not know which node has dropped the message. Obviously, the smaller your reputation is, the less likely it is that you are chosen to forward messages. Other problems can be found in RCAR. Namely, not knowing or having an idea of which node misbehaved, messages from that node can still be received and the node has no incentive to cooperate.

Other methods exist to try to solve black-hole attacks. This section only presented some of them and the most relevant parts of those schemes.

The main motivation to try to solve the problem of black-hole nodes was the fact that most effective protocols use a reputation value as a base for judgement, the dependency of other nodes for information and the fact that to classify a node in most reputation schemes there must be an encounter, not allowing for a great network awareness. A wrong reputation value is problematic in the case that you want to punish nodes for malicious behavior. Nodes, good or bad, might be in a limbo of classification before reaching a certain threshold. Furthermore, the possibility that good nodes might have to be constantly proving they are good, may slow down message exchanges. The dependency on other nodes' information is a clear drawback when analyzing scenarios with black-holes. Having to meet a node before being able to classify it also is a clear drawback, because in that way, a node will never be able to identify all the malicious nodes in a simulation. Having these primary three factors in mind, an attempt was made to try and create a reputation system that corrected this drawbacks and also achieved a high detection ratio and a 0% false positive rate.

F. Simulator

In order to test the effectiveness of the reputation system in early stages, it is imperative to find a tool that can realistically and reliably simulate a VDTN. In [19], authors offer a thorough review of existing simulation models and tools available for DTNs, comparing them in terms of their precision, scalability and performance. The ONE [20] stands out, being specifically designed for opportunistic networks. It allows for the generation of node movements using different models, the reproduction of message traffic and routing, cache handling and the visualization of both mobility, message passing through its powerful graphical user interface among other possibilities. The ONE also can produce a variety of reports, such as general message statistics and buffer occupancy reports. Furthermore, the ONE appears to be the simulation tool of choice for the most recent studies made in VDTNs. Being, for these reasons, the simulator selected to use in this work.

The ONE is a discrete event simulation engine. This means that a simulation occurs as a sequence of events in time. Each event takes place and marks a change of state in the system, in which various modules are updated that implement the main simulation functions. Also, the collection of results and analysis are done through visualization, reports and post-processing tools [20]. The simulator offers different options for movement models. The routing options in this simulator include all the routing protocols mention in the section above which allows for a great range of tests to be done.

III. Building the Reputation System

A. Reputation System Performance Metrics

Before conducting a comparative analysis on the reputation systems, it is important to make clear the performance metrics that will be used.

The metrics are divided into two groups. The first, for purposes of evaluating the routing protocols performance. The second, to evaluate the node's classification of each other. In this work, extra metrics are used in both groups. These serve to measure the same metrics but only in relation to the good nodes in the network.

1) Routing Protocol Metrics

These metrics have the goal of measuring how well do the routing protocols perform when faced with various percentages of black-hole nodes.

Delivery Ratio

The delivery ratio indicates the successfully delivered messages from all the messages that were sent as in (1).

$$\frac{number\ of\ delivered\ messages}{number\ of\ created\ messages} \quad (1)$$

Notice that, although in the ONE, the same message can be delivered more than once to the recipient, only the first time is accounted for the equation.

Delivery Ratio for Good Nodes

This ratio is essentially the same as the Delivery Ratio, but only the delivered and created messages from good nodes to good nodes are accounted for, as in (2).

$$\frac{number\ of\ delivered\ messages\ from\ good\ nodes\ to\ good\ nodes}{number\ of\ created\ messages\ from\ good\ nodes\ to\ good\ nodes} \quad (2)$$

Average Latency for Good Nodes

The latency of a message is the time delay between the creation and the delivery of the message. In this metric, only messages from good nodes to good nodes are accounted for as seen in (3).

$$\frac{\sum_{i=0}^{number\ of\ delivered\ messages} (delivery\ time_i - creation\ time_i)}{number\ of\ delivered\ messages} \quad (3)$$

Overhead Ratio for Good Nodes

The overhead ratio of a protocol indicates the excess of messages successfully transmitted when compared to the total number of messages delivered. In this metric, only messages from good nodes to good nodes are regarded, as shown in (4). The *t* represents the number of transmitted messages and *d* the number of delivered messages.

$$\frac{t_{from\ good\ nodes\ to\ good\ nodes} - d_{from\ good\ nodes\ to\ good\ nodes}}{d_{from\ good\ nodes\ to\ good\ nodes}} \quad (4)$$

2) Node Classification Metrics

These metrics objective is to measure how well and how fast can nodes classify each other as good or malicious, in the simulation, when faced with various percentages of black-hole nodes.

Detection Rate

The detection rate represents the percentage of malicious nodes detected by all nodes in the simulation. So, if the simulation has *B* black-hole nodes, each good node should identify *B* black-hole nodes and each malicious node should identify *B*-1 black-hole nodes, not counting itself. Considering, *N* as the total of good nodes, *B* as the total of black-hole nodes and *T* as the total number of nodes in the simulation, the detection ratio is calculated using (5).

$$\frac{\sum_{i=0}^{T} (number\ of\ correct\ classifications_i)}{N \times B + B \times (B-1)} \times 100 \quad (5)$$

Detection Rate for Good Nodes

The detection rate for good nodes is the percentage of malicious nodes detected by good nodes in the simulation. Here, in contrary to the detection rate, only the classification of black-hole nodes by good nodes is relevant. The distinction is made between the two detection rates because in a reputation system, although it is important that all nodes identify the threats, is more valuable for the network if all good nodes identify all bad nodes. The detection rate for good nodes presents a clearer view of this point.

Considering, *N* as the total of good nodes and *B* as the total of black-hole nodes, this metric is calculated with (6).

$$\frac{\sum_{i=0}^{N} (number\ of\ correct\ classifications_i)}{N \times B} \times 100 \quad (6)$$

False Negative Rate

The false negative rate is the percentage of black-hole nodes mistakenly classified as good. With a high false negative rate, good nodes exchange messages with malicious nodes thinking they are good and cooperating message exchange.

Considering *T* as the total number of nodes in the simulation, the false negative rate is obtained using (7)

$$\frac{\sum_{i=0}^{T} (number\ of\ black\text{-}hole\ nodes\ classified\ as\ good)_i}{total\ number\ of\ classifications} \times 100 \quad (7)$$

False Negative Rate for Good Nodes

The false negative rate for good nodes is the percentage of black-hole nodes mistakenly classified as good by good nodes. Considering *G* as the total number of good nodes in the simulation and *BHs* as number of black-hole nodes, the false negative rate for good nodes is obtained using (8)

$$\frac{\sum_{i=0}^{G} (BHs\ classified\ as\ good\ by\ good\ nodes)_i}{total\ number\ of\ classifications\ by\ good\ nodes} \times 100 \quad (8)$$

False Positive Rate

The false positive rate is the percentage of good nodes mistakenly classified as malicious. This is a very important metric if it is decided to punish bad behavior. If the false positive rate is high, it is possible that good nodes are prevented from contacting other nodes, unfairly impairing the exchange of messages.

Considering *T* as the total number of nodes in the simulation, the false positive rate is obtained using (9)

$$\frac{\sum_{i=0}^{T} (number\ good\ nodes\ classified\ as\ black\text{-}hole\ nodes)_i}{total\ number\ of\ classifications} \times 100 \quad (9)$$

False Positive Rate for Good Nodes

The false positive rate is the percentage of good nodes mistakenly classified as malicious by good nodes. Considering *G* as the total number of good nodes in the simulation and *BHs* as an abbreviation of black-hole nodes, the false negative rate for good nodes is obtained using (10).

$$\frac{\sum_{i=0}^{G} (good\ nodes\ classified\ as\ BHs\ by\ good\ nodes)_i}{total\ number\ of\ classifications\ by\ good\ nodes} \times 100 \quad (10)$$

B. Approach to the problem

To create a reputation system, various variables must be considered. The scenario for testing has to be studied, the detection method chosen and how to apply it is also very important.

To choose the scenario, the first step was to select the number of nodes. Having the number of nodes chosen, it is relevant decide the profile of the network. By profile, is meant what is considered a vehicle in the network and how are they distributed. Although the number of messages created is an important variable, especially to evaluate a reputation system, it was decided that for the initial simulations all nodes would create messages at the same rate. There are more factors involved in the simulation scenario, but these were the main factors chosen to be evaluated at a specific level.

With the simulation scenario set, the reputation system begun to be created. The system's creation was divided into two parts, the detection phase and the action phase. The detection phase, as the name suggests, addresses the detection of black-hole nodes by nodes in the network. In turn, the action phase uses the detection made to punish the bad nodes.

C. Simulation Scenario

The ONE simulator gives a plethora of options when it comes to the simulation scenario. A small study was made to evaluate what would be the ideal scenarios to test a reputation system. Firstly, studying the number of nodes in the simulation and, afterwards, the profile of the network. The number of nodes in a network influences highly the number of contacts between nodes. Consequently, the number of messages transmitted. In a same size map, less nodes will possibly lead to a sparser network, whilst more nodes possibly lead to a denser network. In a sparse network, contacts are fewer, therefore, not as many opportunities for exchanging messages. But, with less messages, node's buffers are not as saturated and can carry

messages longer without having to drop them. For dense networks, the exact opposite happens. More contact opportunities, more messages exchanged, and so, more dropped messages. Having in mind the Helsinki map size, it was decided that 50 nodes would be a good representation for a sparse network and 200 nodes for a dense network.

As in the case of the number of nodes in the network, the profile of the network also has an impact in how the messages are transmitted. Considering as vehicles, cars, pedestrians and trams, the quantity of each one of these in each simulation has an impact on the different metrics. Since each group moves at a different speed and are confined to certain areas. For the initial simulations, the decision was made to include the three types of vehicles, to better represent the diversity that a VDTN might have. Maintaining the number of trams constant in every simulation and trying three different combinations for the number of cars and pedestrians. The first combination includes more pedestrians, roughly double the number of cars. The second has an equal number of cars and pedestrians and the last has more cars than pedestrians, also roughly at double the quantity. To study the number of nodes to use, once the profile of the network was not already decided, the three different profile combinations were tested for 50, 106 and 206 nodes. In a total of nine different scenarios. Each node generates messages in a time range between one hour and forty minutes and two hours.

The protocol chosen to study was Prophet, since was one of the most commonly used in the studies analyzed. The overall simulations settings are presented in Table I. Ten simulations were made for each scenario with different seeds to guarantee non-deterministic results in each run. Furthermore, the corresponding 95% confidence intervals are also presented with the results.

To decide on the number of nodes and the profile of the network the delivery ratio was evaluated. Because, the objective is to see when black-hole nodes' impact is more prominent. The results to understand the impact of the number of nodes are presented in Fig.1.

It is clear that the impact of black-hole nodes is more extreme when using 206 nodes in the simulations. Settling the number of nodes for the simulations as 206.

To choose the profile of the network composed of 206 nodes, the same simulations were used. But to observe the effect of the nodes' profiles, the graphs are presented in a different manner, as it is depicted in Fig.2.

There are some distinctions regarding the three profile networks, however, none big enough to be considered relevant. Knowing that fact, it was established that for the next simulations, an equal number of pedestrians and cars would be used, to have a middle ground between the two other profiles. Concluding, thereby, the decisions in relation to the first part of the approach to the problem.

D. Detection Phase

The detection part of the reputation system in each node has the purpose of identifying black-hole nodes in the scenario. For this reason, to classify the detection schemes, only three metrics were used, the detection rate, false positive rate and false negative rate.

Various strategies can be used to identify malicious nodes, as seen in section Background. For this work, some considerations were deemed necessary. First, it is imperative that the detection phase is decentralized, allowing each node to have its own reputation rating for other nodes in the network. Second, the reputation rating should be achieved in the most independent manner possible and when necessary, exchanged information between nodes should be done carefully. Also, it was of higher importance to achieve the best metric possible and a fast convergence ratio in the false positive rate than in the false negative and the detection rate. This decision was made because of the impact that the false positive and false negative rate have in the action phase of the scheme. In a worst-case scenario where a reputation system has a detection ratio of 0%, the impact in the network would be approximately the same as if no reputation system were applied. The same goes for the false negative ratio. If a system has a false negative ratio of 100%, then all black-hole nodes are considered good and it is basically the same scenario as if no reputation were applied. However, a high false positive rate classifies a lot of good nodes as malicious. This is a bigger problem, since the goal of the whole reputation system is to improve the delivery ratio of good nodes. Classifying good nodes as bad, having into account that a punishment will be applied to these nodes, will probably decrease the good nodes' delivery ratio, which is the opposite of what is desired.

Assumptions are made in accord to some aspects of the VDTN in general. It is assumed that every node has a unique identifier that allows other nodes to distinguish them in the network. Also, messages carry the list of the nodes' identifications they have passed by. Starting with the source, each node adds its identification upon receiving a message that it is not destined to itself. As in RCAR [18]. Moreover, it is assumed that nodes, when receiving a message, are able to know its source. These detection schemes only focus on single black-hole attacks. This means that, a node that is malicious maintains its behavior during the whole simulation and does not collude with other black-hole attackers.

Finally, each node has a black-hole node list and a good node list. The black-hole node list saves the identification of nodes that are classified as bad and the good node list saves the identification of nodes that are classified as good.

The reputation scheme is as simples as possible, to not add much computing and processing time so that message exchanges can still occur. Fundamentally, if a node receives a message in which the sender was not the source, the sender is classified as good and put on the good node list.

TABLE I

Simulation Time	24 hours
Movement Model	Shortest Path Map-Based Movement Model
Nodes' speed	Pedestrians 1.8-5.4 km/h Cars 10-50 km/h Trams 25-36 km/h
Nodes' buffer size	5MB
Nodes' wait time	0-120 seconds
Message size	500kb-1MB
Message TTL (Time to Live)	5 hours

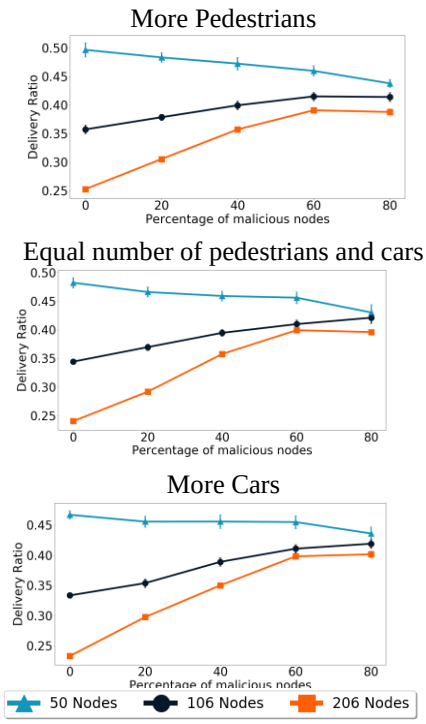

Fig. 1. Delivery ratio for Prophet in different profile networks when comparing different number of nodes

.

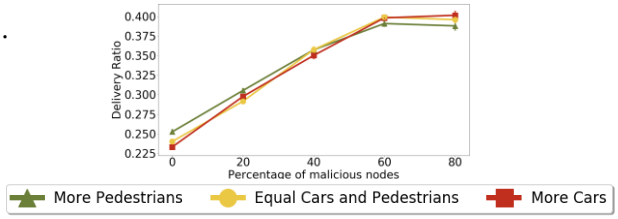

Fig. 2. Delivery ratio for 206 nodes when comparing different profile networks

Contrarily, if the sender of the message is the source of the message, the node is considered malicious and put on the black-hole list. Since nodes' behavior does not change during the simulation, every node that forwards a message in which it is not the source, is in fact a good node and will never change its status from the moment that is classified. Therefore, this detection scheme always leads to a 0% false negative rate because not a single malicious node will be classified as good.

Furthermore, since nodes have access to the list of nodes the message has passed by, every node that is listed in the message that is not the source of the message is also classified as good. Also, so that nodes can have information about nodes they did not met before, when a node sends a message, with it, sends also its good node list. To prevent accepting wrong information from malicious nodes, good node lists are used only if nodes have been classified as good, being deleted otherwise. This means that, since nodes firstly can only classify other nodes as good if they have a message proof and this proof is always accurate, the information will always come from a good node and used exchanged information will never be erroneous. A scheme exemplifying the detection process is presented in Fig. 3. The results simulated in the ONE, for the same settings presented in Table I, for Prophet for 20% of malicious nodes are presented in Fig. 4.

The results show that the detection scheme is working effectively, the detection rate increases as time goes by and false positive rate decreases. False positive rate is 0% as early as the fourth hour of the simulation, and by the end of the simulation the detection rate is about 97%, which is a very good result.

E. Action Phase

The action part of the reputation system in each node has the purpose of punishing black-hole nodes in the scenario. For this part, the metrics used to check the performance were the delivery ratio for good nodes, false positive rate for good nodes and detection rate for good nodes.

For the action phase, it is not only important the type of punishment done, but also at which point should nodes start to apply the punishment. Having into account the detection scheme chosen, if a punishment is applied to soon, nodes might not have time to reach the false positive rate of 0% and by this, good nodes will be wrongly penalized. On the other hand, if punishment is applied to late, it might not affect the nodes exchanges enough to significantly change the delivery ratio of good nodes.

For punishment, firstly, three principal and independent schemes were considered, an action related with the creation of messages, an action regarding connection between nodes and an action associated with deleting messages.

From now on, they will be referred to as Creation, Disconnect and Delete action and are explained below.

Creation Action: Nodes do not create messages for nodes that they have in the black-hole node list.

Disconnect Action: When a node connects to other, if the met node is in the black-hole node list, the node disconnects and proceeds without exchanging messages.

Delete Action: All messages from nodes in the black-hole list are deleted from buffers.

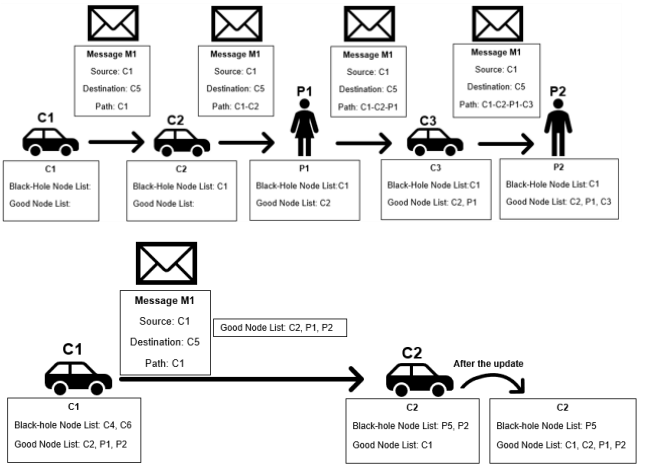

Fig. 3. Scheme exemplifying update of black-hole and good-nodes lists.

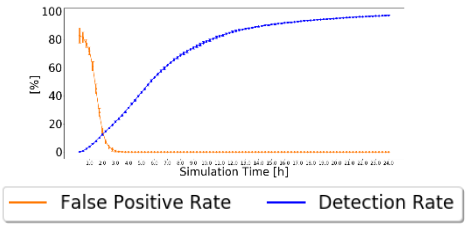

Fig. 4. False Positive and Detection Rate for Prophet with 20% malicious nodes

These were the principal actions taken to punish the black-hole nodes. Since one should not assume which scheme will

perform better or even if all actions together provide a better result, all possible combinations of actions were tested. To decide when to start applying punishment the results from the detection scheme were observed. Prophet reaches a false positive rate of 0% around the the fourth hour of the simulation. For this reason and for study purposes, it was decided to test the action scheme starting at the beginning, at the second, fourth and eighth hour of the simulation. The simulations use the defined settings in Table I for an equal number of pedestrians and cars. In a first instance for selecting the best options for the action scheme, only the metric of the delivery ratio for good nodes is evaluated. A case called "No Action" is used, representing the delivery ratio for good nodes if no action was taken to punish the black-hole nodes. From the results, three action schemes were chosen to analyze in more depth and the results are presented in Fig. 5.

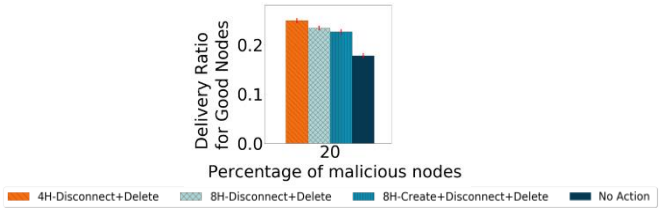

Fig. 5. Comparing best performance action schemes' Delivery Ratio for Good Nodes for Prophet with 20% malicious nodes

Since the most important part of a detection scheme is to increase the number of messages exchanged between good nodes, They have the best delivery ratio for good nodes performance. By best performance, is meant that, these protocols overperform the "No Action" case the most times when compared to others. Not that they have the best delivery performance overall. Only looking to the delivery ratio for good nodes numbers, the action scheme that provides the highest delivery ratio more times is the 4H-Disconnect+Delete. However, this can-not be the only indicator to choose an action scheme, since it is still necessary to observe the impact of the action scheme in the detection of nodes. It is expected that changes for either metric will only start appearing once the action scheme starts. If a false positive ratio for good nodes of 0% is reached before the action phase starts, the action scheme should not have an impact on this metric. Whilst if not reached, the false positive ratio will be higher than if no action was taken. This is mostly because, in any of the three action schemes, the Disconnection action prevents nodes from exchanging messages with nodes that they consider bad, making the detection process more difficult. For protocols in which the false positive rate of 0% is not reached, this metric will be higher the earlier the action scheme is applied. For the detection rate for good nodes, is also expected that the performance will decrease once the action takes place. Because, in any action scheme, there is a disconnect from the nodes that are considered malicious. Thus, no longer having an exchange of messages with malicious nodes. The messages from these nodes no longer circle the network, which prevent some nodes to be identified as malicious, also preventing some nodes to prove themselves as good.

The results for these metrics were simulated using the defined settings in Table I for an equal number of pedestrians. The 95% confidence interval is very small, showing great trust in the achieved results presented in Fig.6.

The results concur with the expected. Furthermore, it does not appear to be a difference between the action schemes in which the action scheme starts at 8H.

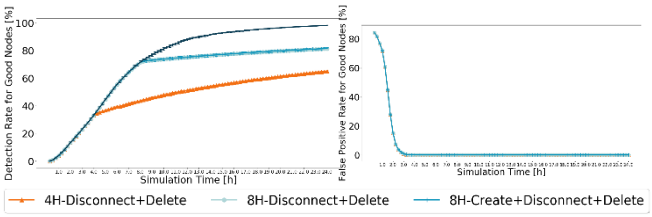

Fig. 6. Comparison of Detection Rate for Good Nodes and False Positive Rate for Good Nodes, between best performance action schemes, for Prophet, with 20%.

Furthermore, it limits the messages created to only some good nodes. Ending up excluding all nodes that are good but have not been yet identified as such. After analyzing the scenarios, the best combination for an action scheme is 8H-Disconnect+Delete. It is the second action scheme with the best delivery ratio for good nodes, not being overperformed by the 4H-Disconnect+Delete action scheme by a long value. But overperforming 4H-Disconnect+Delete action scheme by long in terms of detection and false positive rate.

Due to how the nodes are classified, in a binary way, being always good or bad, not having any "status" in between, the reputation scheme was named Binary Reputation System, or for short, BiRep.

IV. Robustness Results and Analysis

In the previous sections, the results were studied in order to aid the development of the BiRep algorithm. This section has as an objective to test the reputation system against several different scenarios in order to determine BiRep's robustness. Since the most important factor for the success of this Reputation system is the number of messages relayed between nodes, the first group of scenarios use different message creation intervals and transmission rates in order to see how these differences impact the results. The second group of scenarios that are tested have a major focus on the type and quantity of nodes in the simulation. Most of the parameters for the scenarios are equal to the ones described in Table I of section II. Note that the base scenario, corresponds to the exact settings of Table I and serves as a comparison for the other scenarios. In Less message scenario a node creates a message each two to four hours. In More messages scenario each node generates messages in an interval from thirty minutes to an hour. Bigger transmission rate scenario maintains the message generation rate from the base scenario, but the transmission rate from the nodes' interfaces increases in double. The second group of scenarios related to type and quantity of nodes. The 50 and 106 nodes scenario uses the simulation parameters presented in Table I, except for the nodes, as does All cars scenario except for the profile of the network, which now has 200 cars. To evaluate the results, only metrics for good nodes will be judged once they are the most relevant to evaluate the usefulness of the whole scheme. Firstly, looking at the node classification metrics, it would be expected that, for Less messages scenario, less black-hole nodes would be identified and for More messages and Bigger transmission rate more. For Less messages, less messages would be created, therefore, less messages are circulating the network and less opportunities for nodes to prove themselves as good exist. The exact opposite happens with More messages. In Bigger transmission rate scenario, the message transmission rate is the double, allowing nodes to exchange more messages and having more and faster information to classify nodes as good or as bad. The results for Prophet are presented in Fig. 7 for

20% of malicious nodes. Analyzing the results, the expected is confirmed, and it is clear that the detection rate for good nodes is increasing in all scenarios, with a range from 70% to 90%, depending on the scenario, and that the false positive rate is always zero for most of the simulation. For the routing protocol metrics, it was decided to test the reputation system also with various percentages of malicious nodes, to test to how BiRep would respond. Without a reputation scheme, the delivery ratio, average latency and overhead ratio for good nodes performance decreases as the percentage of black-hole nodes increases. Having more black-hole nodes in the network makes it harder for good nodes to deliver messages, hence lower delivery rate. When they do deliver the messages, it takes longer, so more latency and in general in more hops. Overhead ratio is also bigger because with the increase of malicious nodes in the network, the same number of messages are relayed but less are delivered. It is desired that all scenarios have a better performance than if no reputation scheme was used. The results for the same sets of simulation used for Fig. 7 are presented in Fig. 8. Prophet, for all scenarios show better results for the delivery rate for good nodes than if no reputation scheme was used. This proves the usefulness of the reputation scheme. Furthermore, overall the performance of the other metrics also improves. Looking now to the second group of scenarios that are tested, having a major focus on the type and quantity of nodes in the simulation, it is not easy to predict the results. While it is plausible to assume that 50 nodes will have less contacts than 106 or 206 nodes, and thus less opportunities to exchange messages, the initial location and further movement of the nodes is random. So, it is possibly to end up with nodes moving very close to each other in the simulation, increasing the contact opportunities. Furthermore, with fewer nodes, less messages need to be exchanged before all malicious nodes are identified. It is not an easy scenario to predict results, because they depend immensely on nodes' behavior and on the simulation scenario in general. For the situation of the scenario with all cars, is not easy to predict results as well. Having more cars, and therefore more vehicles moving at a larger speed, increases the encounter possibility but also can decrease the time available for message exchange. Once again, the detection and false positve rate behave as expected, reaching high levels of detection and 0% of false positive rate. Also, overall, the assumption of a better detection rate related to a bigger number of contacts and therefore more message exchange, thus having more and faster information seems to be related. Although not a big difference is noted. This means that BiRep does not seem to be greatly affected by the profile or number of nodes.Evaluating the routing protocol metrics, the results appear in Fig. 10. The results show a big increase in the delivery ratio and overhead ratio for all scenarios. The latency does not change in such a significant matter but it does not get worse either.

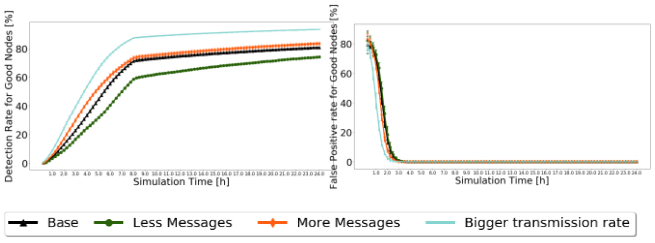

Fig. 7. Comparison of Detection Rate for Good Nodes and False Positive Rate for Good Nodes for Prophet, with 20% of malicious nodes to test robustness of scenarios with different message generation and transmission settings

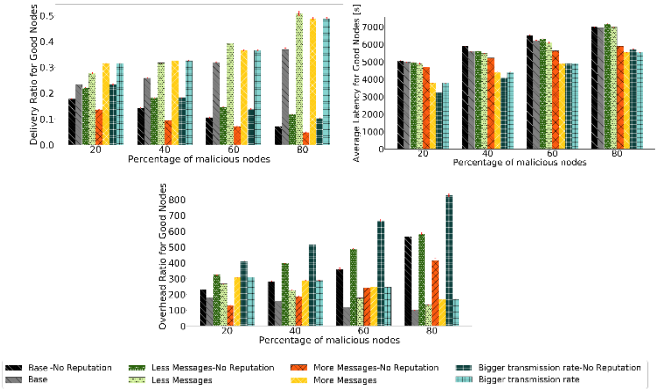

Fig. 8. Comparison of Delivery Ratio for Good Nodes, Overhead Ratio for Good Nodes and Average Latency for Good Nodes for Prophet to test robustness of scenarios with different message generation and transmission settings

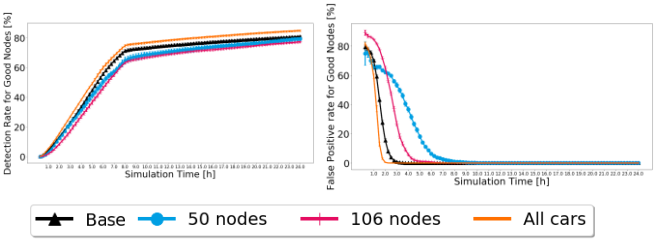

Fig. 9. Comparison of Delivery Ratio for Good Nodes, Overhead Ratio for Good Nodes and Average Latency for Good Nodes for Prophet to test robustness of scenarios with different node numbers and profiles

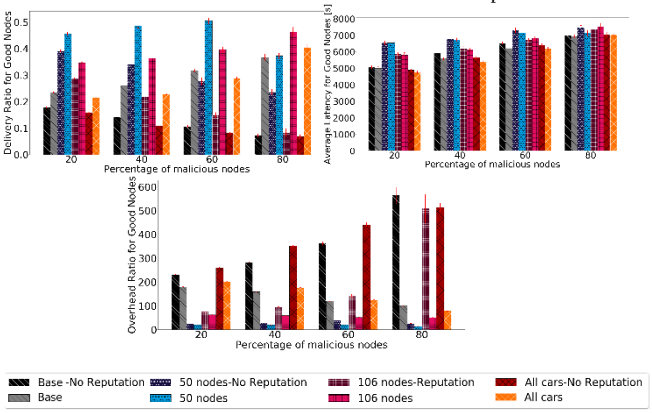

Fig. 10. Comparison of Detection Rate for Good Nodes and False Positive Rate for Good Nodes for Prophet, with 20% of malicious nodes to test robustness of scenarios with different node numbers and profiles

Overall, BiRep performs very well in all scenarios, in some cases even having 10 times more delivery ratio than if no reputation is used, such as in the scenario of More Messages. Comparing with the reputation schemes in section II, for [13], the overall conclusion was that for the Prophet routing protocol, the false positive rate was kept between 2%-5% and that the percentage of malicious nodes detected was around 80% at best.

Although a straight comparison cannot be made since nor the simulator nor the simulation parameters are the same, the scenario with 50 cars is similar enough to try and make a fair comparison. Fig. 9 shows that for the Prophet protocol, the detection rate sets around 70%-80% and 0% for the false positive rate. The results are not much different, but BiRep has the benefit of not having a single point of failure since there it is not a centralized system and nodes are capable of making decisions by themselves. For MUTON [14], the simulation results are better, 1%-2% false positive ratio and 95% detection rate. This scheme has 10%-30% of malicious nodes

in the simulation and for that scenario again comparing with 50 nodes scenario for 20% of malicious nodes, BiRep has 0% of false positive rate and at least 80% of detection ratio. MUTON has a better detection rate, but the problems associated with having a centralized detection scheme. When compared with the MDS in [15], for Prophet, the MDS scheme has a detection rate higher than 90% reaching 97%, and 0% false positives. To make a fair comparison, since the simulator used in [15] is the same used in this work and the authors provided the simulation settings, a test was made. The detection scheme of BiRep were applied but using the simulation settings of [15]. Action started being applied at 10000s, as in [15], and using the Disconnect Action scheme. The results are presented in Fig. 11. As the simulation results prove, at least the detection scheme part of BiRep, works very well, overperforming the results of MDS [15] for black-hole nodes, and for the most part, reaching a perfect result in terms of detection. For [17], again, only the Prophet protocol is analyzed. A fair comparison cannot be made since the simulator and movement models are not the same. The results, in general, are worse than the ones this work presents. When comparing, BiRep does standout as a good option. But to make a completely fair comparison further simulations should be made. That would require access to the other works' source code, so its left for further work. Our solution also assumes that nodes do not change behavior, so there are no grey-hole nodes and that nodes do not collude. Even when looking only to a scenario where black-hole nodes do not change behavior and do not collude, there are still flaws. Such as if Direct Delivery routing were to be used, all nodes would be considered malicious, since they are always the source of the messages they carried. But this can also be considered a non-problem since Direct Delivery performance is not affected by black-hole nodes.

V. Conclusions

The main objective of this work was to develop an effective reputation scheme for VDTNs, adaptable to various network scenarios to diminish the effects of black-hole nodes in the network. In that regard, BiRep offers a solution to deal with black-hole nodes that has very low false positive rate and high values of detection rate. The results for different scenarios prove BiReps versatility, achieving in all scenarios an improvement in delivery ratio and overhead ratio helping to a greater performance of the overall network.

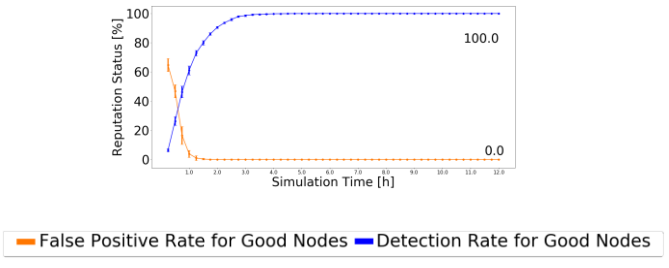

Fig. 11. Detection Rate for Good Nodes and False Positive Rate for Good Nodes for Prophet with simulation settings of [15] and BiRep.

References

[1] F. Warthman. Delay- and Disruption-Tolerant Networks (DTNs) - A Tutorial, Version 3.2. The InterPlaNetary (IPN) Internet Project. InterPlanetary Networking Special Interest Group (IPNSIG), 2015.

[2] P.R. Pereira, A. Casaca, Joel J.P.C. Rodrigues, V.N.G.J. Soares, J. Triay and C. Cervelló-Pastor,"From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks", IEEE Communications Surveys & Tutorials, vol. 14, n. 4, pp. 1166-1182, 4th Quarter 2012.

[3] V. Cerf et al., "Delay Tolerant Network Architecture", IETF, RFC 4838, April 2007.

[4] K. Scott and S. Burleigh, "Bundle Protocol Specification", IETF, RFC 5050, November 2007.

[5] K. Fall, "A delay-tolerant network architecture for challenged Internets", In Proceedings of SIGCOMM'03, August 2003.

[6] Veniam, The Internet of Moving Things [Online; accessed August 2020]. Available: https://veniam.com/

[7] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Single-copy Routing in Intermittently Connected Mobile Networks," in First IEEE Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON 2004), Santa Clara, USA, October 4-7, 2004, pp. 235-244.

[8] S. Jain, K. Fall, and R. Patra, "Routing in a Delay Tolerant Network," in ACM SIGCOMM 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Portland, Oregon, USA, August 30 - September 3, 2004, pp. 145-158.

[9] A. Vahdat and D. Becker, "Epidemic Routing for Partially Connected Ad Hoc Networks", Tech. Rep. CS-200006, Department of Computer Science, Duke University, Durham, NC, 2000.

[10] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks", in Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking, pages 252–259. ACM, 2005.

[11] A. Lindgren, A. Doria, E. Davies, S. Grasic,, "Probabilistic routing protocol for intermittently connected networks", RFC 6693, August 2012.

[12] G. Dini, A. Lo Duca, "A reputation-based approach to tolerate misbehaving carriers in delay tolerant networks", in Computers and Communications (ISCC), 2010 IEEE Symposium on, pp. 772–777, June 2010.

[13] M. Chuah, P. Yang and J. Han, "A ferry-based intrusion detection scheme for sparsely connected ad hoc networks," in Mobile and Ubiquitous Systems: Networking Services, (MobiQuitous), pp. 1-8, August 2007.

[14] Y. Ren, M. Chuah, J. Yang, and Y. Chen, "MUTON: Detecting malicious nodes in disrupt-tolerant networks," in Proc. IEEE Wireless Commun. Netw. Conf. pp. 1–6, 2010.

[15] Y. Guo, S. Schildt, and L. Wolf, "Detecting blackhole and greyhole attacks in vehicular delay tolerant networks," in Proc. IEEE 5th Int. Conf. Commun. Syst. Netw., pp. 1–7, January 2013.

[16] Y. Guo, S. Schildt, T. Pögel, and L. C. Wolf, "Detecting Malicious behavior in a Vehicular DTN for Public Transportation," in Global Information Infrastructure and Networking Symposium 2013 (GIIS'13), Trento, Italy, pp. 1–8, October 2013.

[17] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, "Detecting blackhole attacks in Disruption-Tolerant Networks through packet exchange recording," World of Wireless Mobile and Multimedia Networks (WoWMoM), 2010 IEEE International Symposium on a, Montreal, QC, Canada, pp.1-6, 2010.

[18] G.Dini and A.L.Duca, "Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network", Ad Hoc Networks, vol.10, no.7, pp.1167-1178, September 2012.

[19] J. Dede, A. Förster, E. Hernández-Orallo, J. Herrera-Tapia, K. Kuladinithi, V. Kuppusamy, P. Manzoni, A. bin Muslim, A. Udugama, and Z. Vatandas. Simulating opportunistic networks: Survey and future directions. IEEE Communications Surveys Tutorials, 20(2):1547–1573, Secondquarter 2018.

[20] The ONE. The Opportunistic Network Environment simulator. [Online; accessed August 2020]. Available: https://akeranen.github.io/the-one/