International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209989 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

CETA: Cooperation Enforcement and Trust Algorithm to Handle Selfish Attack in Delay Tolerant Network

Hanane ZEKKORI
Department of computer Science of Faculty of Sciences and Techniques, University of Moulay Ismail, Errachidia, Morocco.
hananzekkori06@gmail.com

Said AGOUJIL
Department of computer Science of Faculty of Sciences and Techniques, University of Moulay Ismail, Errachidia, Morocco.
agoujil@gmail.com

Youssef QARAAI
Department of computer Science of Faculty of Sciences and Techniques, University of Moulay Ismail, Errachidia, Morocco.
qaraai_youssef@yahoo.fr

Received: 21 August 2021 / Revised: 01 October 2021 / Accepted: 05 October 2021 / Published: 27 October 2021

Abstract – Nobody can deny that a 'Delay Tolerant Network (DTN)' is a wireless mobile network capable of withstanding intermittent connectivity and long delays. Furthermore, DTN is a partitioned network that ensures data delivery via the Store and Forward strategy. However, due to resource scarcity (limited storage capacity, limited power, and energy...), DTN can be vulnerable to various types of attacks that can pose a serious threat. Among these types of attacks is selfish behavior, which can potentially ruin the network's integrity, authenticity, confidentiality, and availability. A selfish node tries to maximize its own assets by refusing to transfer other nodes' messages and only forwarding its own. We attempt to investigate the impact of selfish behavior on the existing flooding and forwarding-based routing DTN protocols in this paper. Following that, a comprehensive overview of existing solutions to the selfish attack is presented. To address this threat, we proposed a security mechanism called CETA, which is based on an effective proposed novel algorithm (COOPERATION ENFORCEMENT and TRUST ALGORITHM). The proposed mechanism involves encouraging DTN nodes to collaborate in message forwarding in order to improve delivery probability. Using the ONE simulator, we assessed the performance of our proposed algorithm CETA in DTN under selfish attack. Through simulation tests, CETA efficiency was demonstrated, resulting in promising selfish behavior in terms of delivery probability, overhead ratio, Latency average, and hop count.

Index Terms – DTN, Security, Selfish Node, Algorithm, Trust, Cooperative, Attack.

1. INTRODUCTION

Wireless technology has now infiltrated the mobile network market. MANET (Mobile Ad hoc Network) [1] is a wireless network that does not use pre-existing infrastructure. In contrast, this traditional mobile network does not support packet transfer in an environment characterized by intermittent connectivity between the transmitter and the receiver. As a result, the DTN (Delay Tolerant Network) was born to meet these challenges. The delay tolerant network (DTN) [2] is a mobile wireless network comprised of multiple regional networks (Partitions or areas). And, as the name implies, DTN allows for long delays and intermittent connectivity by employing a novel layer called 'Bundle' that sits on top of lower protocols such as Internet protocols. Through a sublayer known as the Convergence Layer Adapter (CLA), the bundle layer ensures interoperability between the lower layers of the various heterogeneous regions.

To avoid data loss if the upstream path is interrupted, DTN employs the store-carry and forward paradigm [2] . When a source node creates a bundle (a bundle means a message in DTN network), it stores it in its persistent buffer until it can make contact with an intermediate node. The two nodes exchange bundles hop by hop, and the process is repeated until each bundle reaches its destination.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209989 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

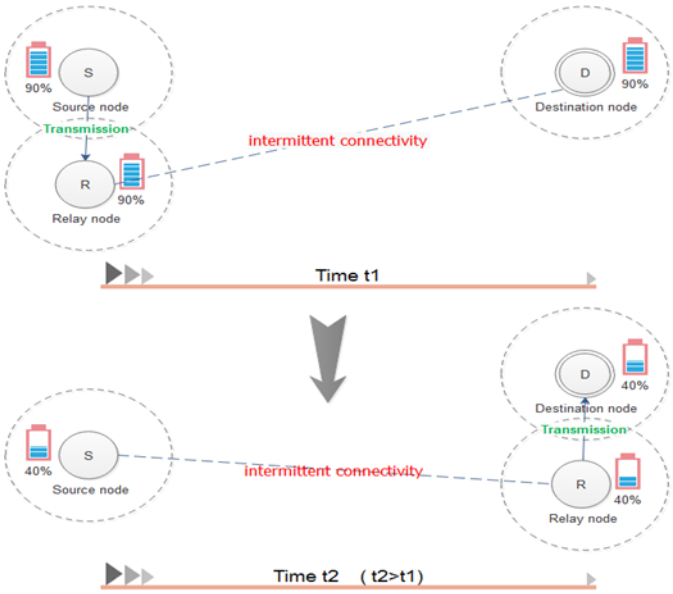

Figure 1 The Communication Process Between DTN Nodes

When there is no direct path between the source and destination nodes. The intermediate nodes (relay nodes) work together to deliver data. In this case, the source node sends the message to the nearest relay node (see Figure 1), and if the destination of the message is not within the communication range of this relay node, it sends it to another relay node (hop by hop manner) until it reaches the destination.

1.1. DTN Security Issues

Security is concerned with protecting measures regardless of undesired behaviors. Compared to wired networks, security is a critical parameter in DTN, especially with its specific and unique features that present a big challenge (see the Figure 2).

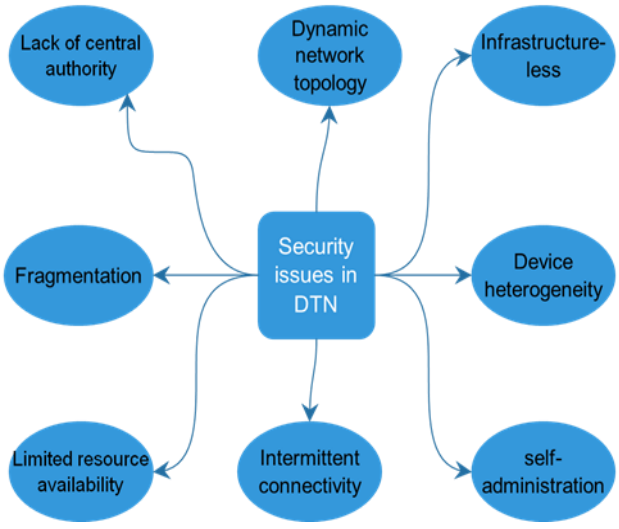

Figure 2 Various DTN Security Issues

Mobile nodes in DTN [3] [4] are autonomous. They are free to move everywhere in the network and to leave at any time, which can lead to dynamic network topology. In addition to that, DTN works without any pre-existing infrastructure and without a central control authority that can manage mutual trust between nodes. And because of the intermittent connectivity in DTN, it is hard to get feedback between the sender and the receiver. Therefore, the existing security solutions for conventional (traditional) networks are ineffective and unsuitable for DTN because of its unique features. So, ensuring security in DTN is problematic. Recently, in the last few years researchers have been working on developing new security solutions or changing the current ones to be applicable to DTN network.

1.2. Classification of Attacks

The unique and challenged characteristics of DTN have made it vulnerable to various security threats [5] such as:

Bundle modification, changing a bundle's blocks (control fields or payload fields), unauthorized access to DTN resources, intercepting, dropping, injecting unwanted and forged (fake) bundles into the network...

The attacks can be classified into four classes [6] [7]: internal and external, active, and passive attacks as it is shown in the Figure 3.

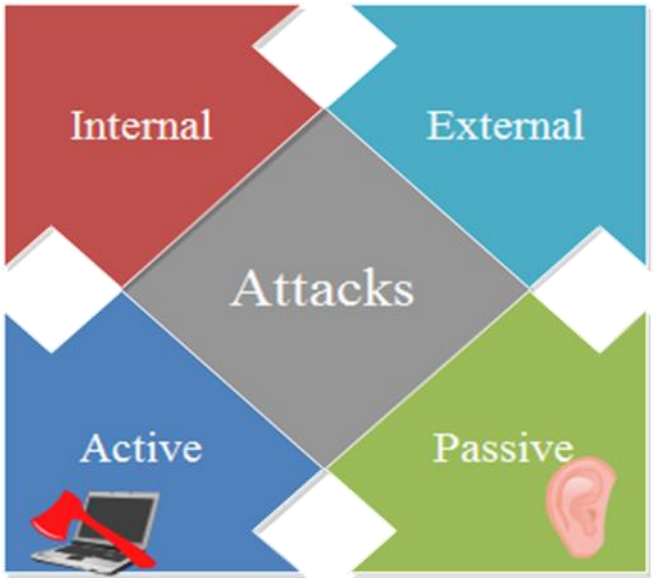

Figure 3 Classification of Attacks

Passive attacks are more common on mobile wireless networks, particularly on delay-tolerant networks, because malicious nodes can listen to traffic simply by being close to the neighbors' transmission range. To obtain information, nodes listen to the network. Active attacks, on the other hand, disrupt the network's normal operations.

RESEARCH ARTICLE

When the source of the attack does not belong to the same region (area) in DTN, we refer to it as an external attack. Internal attacks, on the other hand, are carried out by a legitimate node from the same region.

Internal attacks appear to be more severe than external attacks, and active attacks appear to be more destructive than passive ones.

1.3. DTN Security Requirements

Security is based on five several services that can manage the security issues [4] [8]:

- Confidentiality: prevents unauthorized viewing of private information, and the data (bundles) sent by the sender must only be understandable by the intended receiver.
- Integrity: information should not have been changed since it was sent, and data sent by the source node should reach the destination node undamaged (No modification of the data along the transmission path).
- Availability: means that authorized nodes can access network resources whenever they want, and the network should be always operational.
- Authentication: each node must know the identity of the peer node with which it is communicating (verifying the validity of a specific attribute provided by the peer node).
- Non-repudiation: whoever sent or received the data cannot deny it later. It is a mechanism that ensures that the sender of a message cannot later deny sending it, and that the receiver cannot deny receiving it.

1.4. Problem Description and Motivation

Traditional routing protocols fail in opportunistic networks due to long delays, frequent disconnections, and resource scarcity. The Delay Tolerant Network (DTN) was created to address these issues. Mobile DTN nodes replicate bundles and collaborate to improve delivery probability in the absence of a connected link between the sender and the receiver. However, selfish nodes may refuse to collaborate with other network nodes in order to protect their resources. Traditional mechanisms are ineffective and unsuitable for detecting and controlling selfish attacks due to the unique characteristics of DTN networks. As a result, new mechanisms for forcing selfish nodes to cooperate are being developed.

1.5. Objectives

The primary goals of this research are to force non-cooperative nodes to participate without restrictions in order to deliver the greatest number of bundles possible while also ensuring mutual trust between DTN nodes. As a result, we proposed a CETA-based mechanism that first identifies selfish nodes in the network based on their degree of selfishness and then assigns penalties to uncooperative nodes as an example for every node that refuses to collaborate with its neighbors in data forwarding.

1.6. Organization of the Paper

The rest of this paper is structured as follows: Section 2 begins by presenting related work. Selfishness in Delay Tolerant Network, how selfish behavior affects the performance of DTN routing protocols, this section then discusses the existing security solutions in DTN against selfish behavior. Section 3 focuses on the proposed modeling of our proposed work. Section 4 then presents our proposed cooperative mechanism to combat selfishness, which is based on the proposed CETA (COOPERATION ENFORCEMENT and TRUST ALGORITHM). Before concluding the paper in section 6 with a final summary of the research. Section 5 goes over the simulation settings, performance metrics, and results obtained by evaluating our proposed algorithm using the Epidemic routing protocol.

2. RELATED WORK

In DTN, when a mobile node enters in the communication range of another neighbor node, they start exchanging bundles according to the algorithm of the used protocol. This operation of transferring messages in addition to the mobility of nodes consumes resources such as: Energy, Storage space, CPU capability, bandwidth...

2.1. Behavior of Selfish Nodes

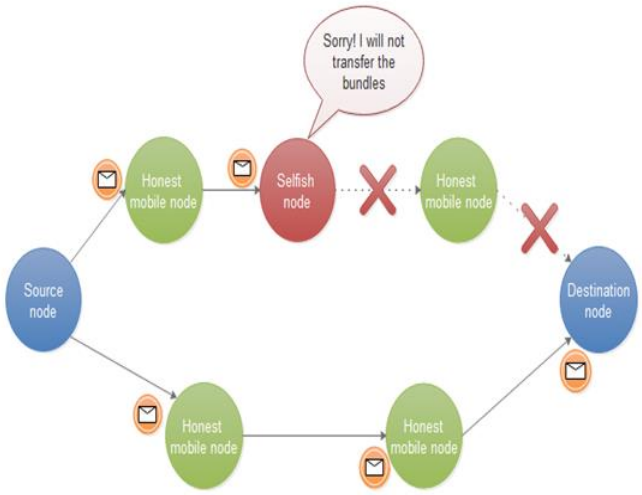

Figure 4 Communication Process of DTN Nodes in the Presence of a Selfish Node

Because of the limited resources, some mobile nodes refuse to cooperate and to collaborate with the other nodes in the network. What's more, they choose to conserve their own assets and to behave selfishly instead of forwarding data. These nodes are called selfish nodes and their behavior named

RESEARCH ARTICLE

individual selfishness [5]. On the other hand, when a group of mobile nodes chooses to interact only with nodes belonging to the same group, because they have mutual interests and social ties, for this situation we are discussing social selfishness [9].

According to section 1, we conclude that selfish behavior is an active internal attack that threatens the availability and the authentication services of the network.

In the present work, we are interested in individual selfishness (see Figure 4).

In the presence of a selfish node, the paths shown above represent how a bundle was relayed from the source node to the destination node. This selfish node clearly drops the bundle instead of transferring it to its destination.

In [10] [11] the authors classify mobile nodes in three main classes according to the degree of cooperation in DTN:

- Cooperative nodes: nodes that participate in the transfer of bundles, storing, carrying, and forwarding bundles without restriction.
- Non-cooperative nodes: mobile nodes refuse to accept bundles that are not intended for them. They only send and receive bundles that are intended for them. They are self-centered and do not contribute to the community for fear of depleting their resources.
- Partially cooperative nodes: nodes accept bundles from other nodes in the network that are not destined for them in exchange for delivering them directly to the destination (Two hop forwarding). Nodes contribute in part based on their resources.

2.2. Effects of Selfish Nodes on DTN Routing Protocols

- Epidemic protocol [12] is a flooding-based routing algorithm without any prior knowledge about the network. So, to increase the delivery probability, each mobile node must be cooperative in a way that each node must have all the set of its neighbors' bundles in its buffer. But, when the nodes are showing the selfish behavior [13], they refuse to participate in forwarding bundles, and each selfish node keeps bundles in its buffer until their Time to Live expires, which degrade the performance of the network.
- S&W protocol [14] is a limited flooding-based protocol without any prior knowledge about the network, and it does not use the history of encounters. Each mobile node in the network replicates each bundle which it had in its buffer space to L different relay nodes. This process is called as the spray phase. If the destination is not met in the spray phase, then each node of these L relay nodes keeps the single copy in its buffer until it meets the destination node to transmit it directly (Wait phase). In the presence of selfish nodes that refuse to store relay's bundles to preserve their own resources, and as the resources are limited, the performance of the algorithm decreases.
- Prophet protocol [15] is based on a probabilistic routing algorithm. The algorithm's process is that mobile nodes, instead of flooding the network by replicas in a randomly manner, they use the history of encounters with certain probabilities equations (delivery predictabilities). In the presence of selfish behavior [16], the selfish node announces itself-having a high delivery predictability to make relay nodes to transferring their bundles to it. Then, when it receives bundles, it drops them which degrades the delivery probability of bundles(messages).
- MaxProp protocol [17] is a probabilistic DTN routing protocol. MaxProp is based on the encounter's history of DTN nodes based on the observation of their past activities. When two mobile nodes meet, they first exchange a list of the recorded probabilities of meeting with relay nodes, then each DTN node calculates the probability of meeting, and it must also calculate the cost of reaching the destination node. These parameters are represented and updated by the equations defined in MaxProp algorithm. But, in the presence of selfish behavior, the performance of the protocol degrades [16].

2.3. Security Mechanisms Against Selfish Attack

Most recent research has concentrated on creating security mechanisms that encourage DTN nodes to participate and collaborate with each other[18] in order to successfully transfer bundles. In the literature there are three main existing mechanisms to mitigate selfish attack.

2.3.1. Barter Based Mechanism

To encourage selfish nodes in the DTN network to collaborate with other nodes, the authors of [19] [20] proposed a mechanism to prevent selfish nodes from exploiting the services of honest nodes. The process of this mechanism is as follows: when two nodes establish a contact, they first start exchanging the list of messages stored in their buffers. Then, they mutually agree on the messages they would like to exchange with each other on the condition that these messages must have the same size and the transmission must be message by message.

However, it was later discovered that the nodes exhibited selfish behavior when exchanging messages. As a result, two types of messages appeared, primary and secondary. If one of the parties cheated (one of the two nodes refused to accept messages from the other), then the transmission would be interrupted.

RESEARCH ARTICLE

2.3.2. Reputation Based Mechanism

The authors of [21] proposed a protocol called MobiGame for the DTN network, which is based on the reputation of nodes. Each DTN node is committed to maintain its own reputation in order to be available for verification. In this context, the authors of [22] proposed a reputation management system called (RTM). In this suggested strategy, the reputation of each mobile node is calculated by a Trust Authority (TA) based on the transmission's history of this node. The node with the highest number of messages from neighboring nodes concerned having a high reputation value. But if the Trusted Authority is infected by a malicious node the network performance decreases.

2.3.3. Incentive Based Mechanism

Table 1 shows the Description, Limitations, and Challenges of the Existing Mechanisms against Selfish Behavior

Mechanism	Description	Limitation
Barter based[20]	Equal exchange of services and goods between pairs.	One of the two nodes may refuse to accept messages from the other node.
Reputation based[26]	Each node evaluates the behavior of its neighbors by a trust metric.	Trusted Authority (TA) may be infected by a malicious node.
Incentive Based[27]	Helpful nodes earn rewards.	Scarcity of resources especially the battery.

Table 1 Describing Description, Limitations, and Challenges of the Existing Mechanisms against Selfish Behavior

In incentive/credit-based mechanism, [23] the authors proposed a payment distribution system to encourage nodes to cooperate in the network. However, the problem of intermittent connectivity and dynamic topology makes the distribution more difficult. The authors of [24] developed a mechanism that consists of distributing rewards to relay nodes to stimulate their cooperation into the DTN network. In this strategy, the source node proposes the following offer to the relay nodes: "I will offer an attractive reward to the first relay node that accepts a message transfer and successfully transmits it to its final destination." However, each relay node can accept or reject the source node's offer depending on the state of its battery and the capacity of its buffer. In this context, Sweta Jain and Ankit Verma [25] have proposed a scheme whose basic idea is to encourage relay nodes to cooperate by offering them rewards or virtual money. They noted this reward by C, and it is proportional to the ratio between the message size and Time to Live (TTL) of the message. Whenever a cooperative node encounters a Trusted Authority TA, it requests it to cash its reward in virtual money that will be useful in its future missions in the network.

3. PORPOSED MODELLING

There is no guarantee that there is an end-to-end path between two nodes in a DTN network, and they must rely on each other to carry messages across the network. As a result, cooperation is essential for the network to function properly. This section aims to describe the network states that a mobile node in a DTN network can adopt, as well as how to model them.

We consider a DTN network of N mobile nodes, noted by n_i, where i ∈{1,……..N}.

We consider a scenario in which honest nodes want to transfer bundles along a path that includes a selfish node (Uncooperative node). The selfish node receives messages that are only intended for itself (see Figure 5).

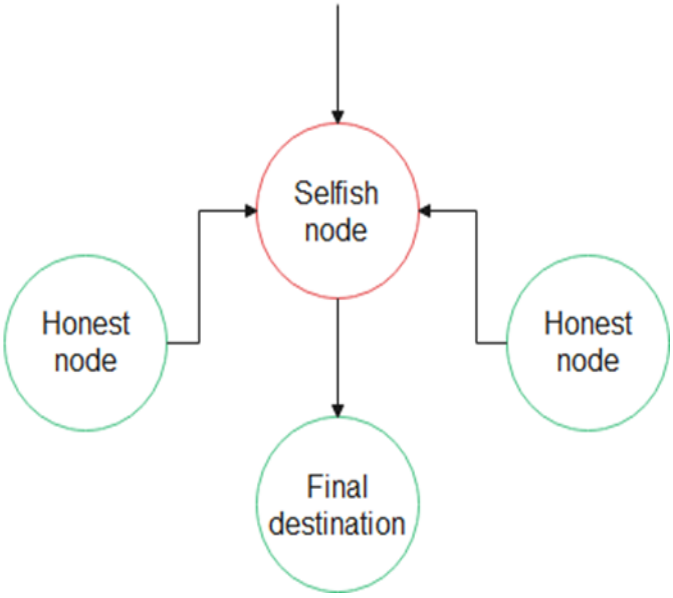

Figure 5 DTN Communication in the Presence of Selfish Behavior

As shown in Figure 5, the selfish node drops all bundles that are not destined for it, and it transfers just its own bundles to the destination. Table 2 shows the various notations used in this work.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2021/209989 Volume 8, Issue 5, September – October (2021)

RESEARCH ARTICLE

Notation	Signification
N	The set of mobile DTN nodes in the network.
H	The number of the existing Honest nodes into the network.
S	The number of the existing Selfish nodes into the network.
Phs	The probability that an honest node becomes selfish.
Psh	The probability that a selfish node becomes honest.
d	Degree of selfishness, vary between 0 and 100.
TTL	Time To Live (lifetime).

Table 2 Table of Notations Used in our Proposed Work

In the DTN network, each mobile node can be in one of two states: selfish or honest.

3.1. DTN Node in an Honest State

We considered that at time t=0, there are H mobile nodes that are honest in the network, and the other nodes (N-H) are selfish. Over time, each honest node's resources begin to degrade. So, to preserve the rest of its resources, this node may turn into a selfish node (behave with selfishness) after an exponential time of parameter λ.

The probability that an honest node becomes selfish at time t+1, is Phs (0 <= Phs<=1), whereas if the node is selfish at t=0, the probability that it will be honest at t+1 is zero, (Psh=0).

Honest nodes: mean normal nodes. They function without any selfish behavior, and they are cooperative.

3.2. DTN Node in a Selfish State

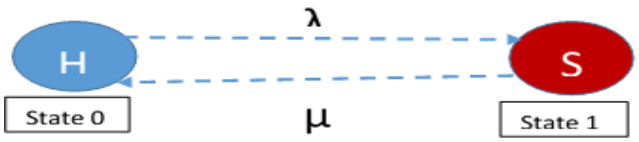

Figure 6 Honest/Selfish States of a Mobile DTN Node

When a mobile node can communicate freely with every node in the network in a cooperative manner, we say that this node is cooperative, and it is in the honest state (H). When it refuses to cooperate with the other nodes in the network, it becomes selfish. In this case, we say that the node is in the selfish state (S). The periods in which the node is honest (the node is in state 0) (see Figure 6), respectively the node is selfish (the node is in state 1), follow exponential laws of parameter respectively λ, μ.

A DTN node is characterized by the following parameters:

1/λ: Average time for a node to be honest.

1/μ: Average time for a node to be Selfish.

The following Q-matrix is the generator of the Markov chain [28] representing the evolution of the states of a mobile node in the network. In the following representation, the first state is the H state (when the node is honest) and the second is the S state (when the node is selfish).

$$Q=\begin{pmatrix} -\lambda & \lambda \\ \mu & -\mu \end{pmatrix} \quad (1)$$

After solving the system PQ=0, the probabilities associated with the generator Q are:

The stationary probability that the node n_i will be selfish (in state S) is Phs=λ/λ+μ. A node transmits bundles only if it is honest and its buffer is non-empty. A node can become selfish when it refuses to transmit bundles in order to conserve its own resources. The stationary probability that node n_i will be honest is Psh=μ/λ+μ with Phs+ Psh =1 and Psh, Phs are scaled in [0,1].

4. POLICY OF THE PROPOSED MECHANISM

If it is demonstrated that a mobile node is not participating in packet forwarding for self-interest, it is identified as a selfish node. To ensure the network's proper operation, all DTN nodes must work together to forward data. To encourage cooperation among mobile nodes in the DTN network, we proposed an efficient mechanism that takes into account each node's available resources (energy, buffer space, contact duration, etc.). The proposed algorithm employs a punishment-based mechanism that penalizes selfish nodes (we proposed a cooperative mechanism by means of punishment).

4.1. Description of Our Mechanism

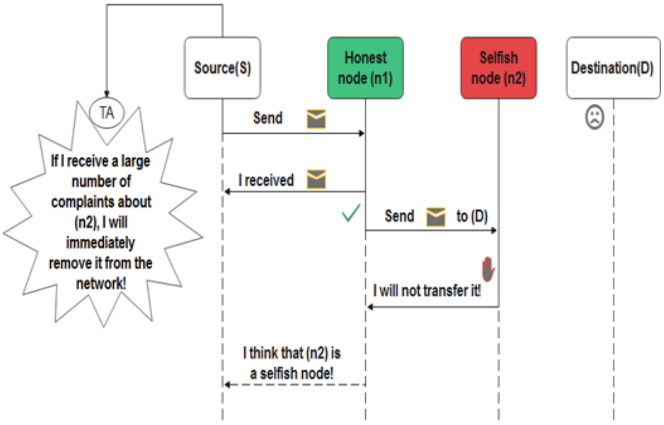

Figure 7 Communication Process in the Presence of a Selfish Node

RESEARCH ARTICLE

We intend to force uncooperative nodes to participate without restriction in order to deliver the greatest number of bundles possible. Our CETA-based mechanism begins by detecting each uncooperative node based on its degree of selfishness as determined by a trust authority (TA). Then, this trust authority punishes every selfish node by rejecting it from the network, forcing the other nodes to cooperate in order to improve network performance. Figure 7 shows an example of this.

4.2. Flowchart and Pseudocode of CETA Algorithm

Our mechanism begins by assigning a level of selfishness to each node. The selfish degree of a node ranged from 0 to 100, with 0 indicating no selfishness and the node being considered honest, 100 indicating a fully selfish node, and degrees between 0 and 100 indicating that the node is partially selfish. When a node's selfishness is greater strictly than 0 (0<d<=100), the node will suffer a penalty, which is to be rejected from the network. ($\lim_{t \to TTL} n(t) = 0$, TTL à 0) (punish the selfish nodes by rejecting them out of the network). See the below Figure 8.

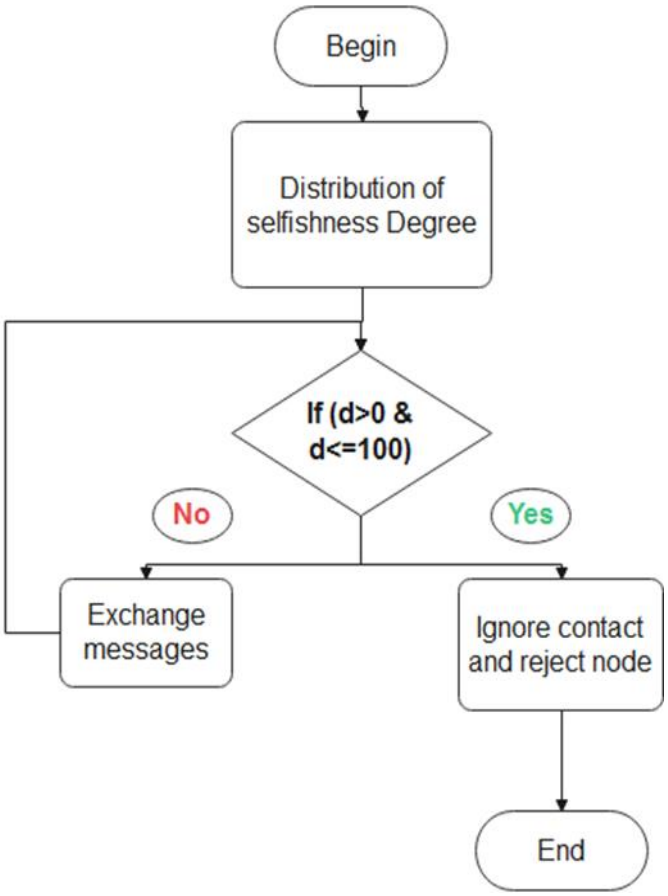

Figure 8 Flowchart of the Proposed Mechanism

The pseudocode of CETA (COOPERATION ENFORCEMENT and TRUST ALGORITHM) is provided in Algorithm 1 and the flowchart of CETA is provided in Figure 8.

Algorithm: CETA

Data (inputs):

N: Total number of nodes in the DTN network.

d: Selfish degree of a DTN node.

TTL: Time to Live of a DTN node.

selfishBehavior: indicates whether the node will take selfish behavior into consideration or not.

Begin

//Step 1: Parameters Initialization.

N = {1,……,n}

d = {0,……,100}

SelfishBehavior = {true,false}

//Step 2: Check whether current node is selfish or not.

4. For (i := 1 to N)
5. If (d<=100 & d>0)
6. Then
7. Node is considered selfish node
8. Else
9. Node is considered honest/trusted node
10. Next i
11. End for

//Step 3: If selfish then reject node out of the network.

12. For (i:= 1 to N)
13. If (d<=100 & d>0)
14. Then do
15. Give a penalty to selfish node
16. TTL:= 0 //expire lifetime of a node
17. End do
18. Else
19. Exchange packets
20. Next i
21. End for

End.

Algorithm 1: Pseudocode of CETA Algorithm

RESEARCH ARTICLE

5. RESULTS AND DISCUSSION

5.1. Simulation Setting and Performance Metrics

The ONE simulator [29] (Opportunistic Network Environment simulator) is an opportunistic networking simulator whose main goal is to improve the realism of Delay Tolerant Network simulations. ONE supports a wide range of node movement models and simulates a wide range of DTN routing algorithms. The ONE simulator was written in Java using the open-source paradigm and allows for the addition of routing algorithms by extending the built-in routing classes. By default, the Helsinki map data is used in ONE to set the scenario and node groups, which are used to model a wide range of independent node activities and capabilities. The ONE was designed to work at the network layer and does not implement lower layers (Physical and Data Link) as other more complex simulators do. The ONE also does not account for physical obstacles that may cause transmission interference.

The below-mentioned performance metrics are considered to evaluate the efficacity of our proposed mechanism to thwart selfishness when using the Epidemic protocol [30]:

- Delivery_prob: This metric represents the number of successfully delivered messages to the destination. One of the primary goals of the DTN network is to maximize this value. This metric's value is scaled in [0,1]. It is computed using the following formula: (NumberOfDeliveredMessages/NumberOfCreatedMessages).
- Overhead_ratio: It measures how many transfers were needed for each successful message delivery. The DTN network's primary goal is to reduce the value of this metric. It is defined by 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. The DTN network's primary goal is to reduce the value of this metric.
- Hopcount_avg: It is an important metric that counts the average number of hops which were needed between source and destination node.

Parameters	Values
Simulation Area Size	1000m x 1000m
Simulation time	86400 seconds (one day)
Number of nodes	500
Mobility Model	Random Walk
Routing protocol	Epidemic
Speed of Mobility	0.5 m/s, 1.5m/s
Size of Packet	500kb,1M
Buffer Size	5MB
TTL	300 min
selfishDegree	[0,30,60,90,100]
selfishBehavior	[true,false]

Table 3 Simulation Settings and Parameters

5.2. Performance Evaluation

The ONE Simulator[29] (Opportunistic Network Environment Simulator) was used, as shown in the figure below (Figure 9). see the above Table 3 for more information on the simulation parameters that were used.

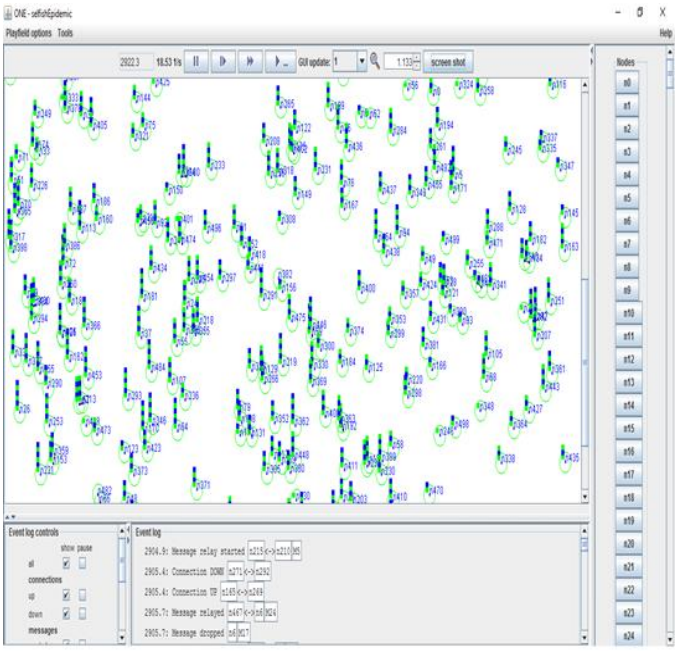

Figure 9 The Screenshot of Our Scenario on the ONE Simulator's GUI. The Green Circles Represent the Range of the Respective Node, Denoted by n(i) where i is the Sequence Number

5.2.1. Delivery Probability Analysis

We vary the percentage of selfish nodes in the network and evaluate the effect on delivery probability. Figure 10 depicts the outcomes.

Figure 10 shows that as the percentage of selfish nodes increases, the delivery probability decreases significantly

RESEARCH ARTICLE

when using the Epidemic routing protocol (SelfishEpidemic) because selfish nodes did not collaborate in the routing process. However, we can see an improvement in delivery probability values when we implement our proposed algorithm CETA in the Epidemic routing protocol (TrustEpidemic). This is due to the fact that the selfish degree is controlled when CETA is used.

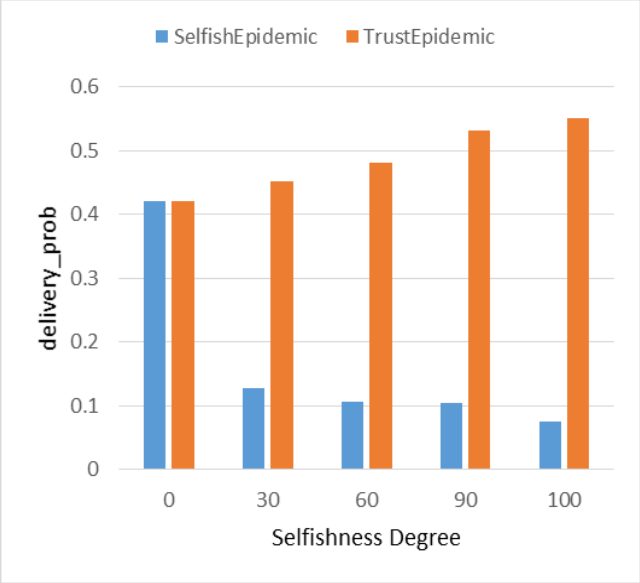

Figure 10 Delivery Probability Vs. Selfishness Degree

5.2.2. Overhead Ratio Analysis

We vary the percentage of selfish nodes in the network and examine the effect on the overhead ratio. Figure 11 depicts the results.

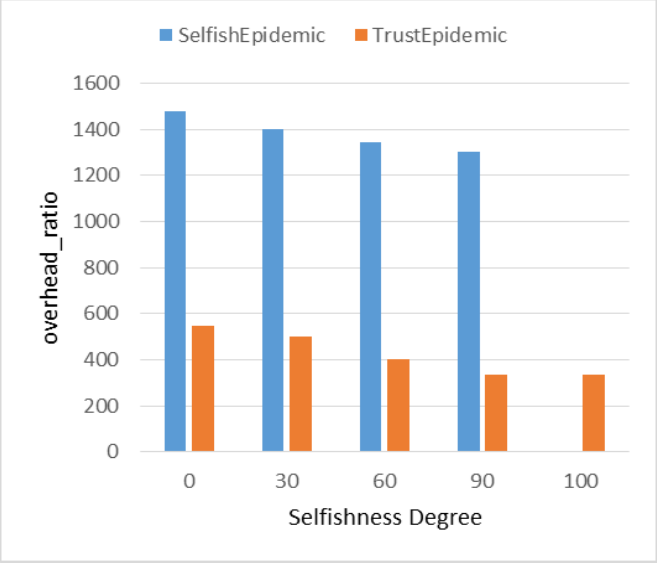

Figure 11 Overhead Ratio Vs. Selfishness Degree

Figure 11 shows that as the percentage of selfish nodes increases, the overhead ratio decreases significantly when using the Epidemic routing protocol (SelfishEpidemic) until it disappears because selfish nodes transfer only their own messages. Also, when we use our proposed algorithm CETA in the Epidemic routing protocol, we see a decrease in overhead ratio values that are small compared to when we used SelfishEpidemic. CETA identified and then isolated selfish nodes in our proposed mechanism, increasing the delivery probability and lowering the overhead ratio.

5.2.3. Latency Average Analysis

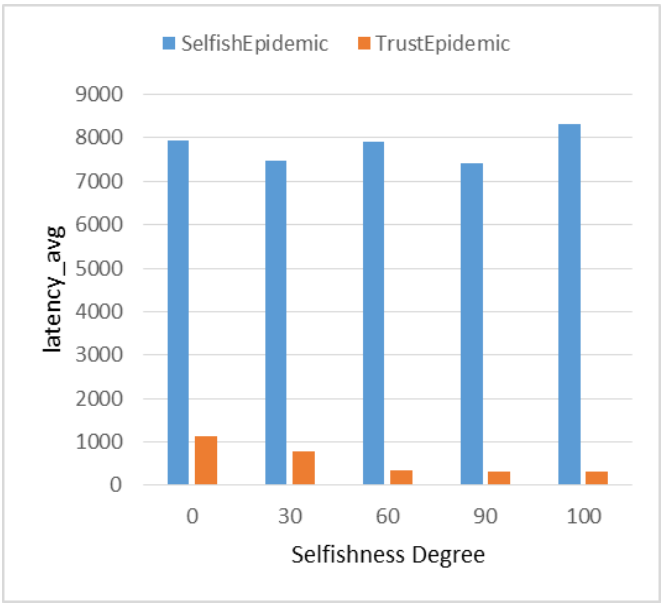

Figure 12 Latency Average Vs. Selfishness Degree

We vary the percentage of selfish nodes in the network and evaluate the effect on latency average. Figure 12 depicts the outcomes.

Figure 12 shows that as the percentage of selfish nodes increases, the average latency decreases significantly when using our proposed algorithm CETA in the Epidemic routing protocol (TrustEpidemic) versus the Epidemic routing protocol (SelfishEpidemic) because selfish nodes do not collaborate in the routing process and take a long time to find their destinations. As a result, low trusted nodes have high average latency values.

5.2.4. Hop Count Analysis

We vary the percentage of selfish nodes in the network and evaluate the effect on hop count. Figure 13 depicts the outcomes.

Figure 13 shows that as the percentage of selfish nodes increases, the hop count decreases significantly when using the Epidemic routing protocol (SelfishEpidemic) until it

RESEARCH ARTICLE

equals one, because selfish nodes only transfer their own messages. However, when we implement our proposed algorithm CETA in the Epidemic routing protocol, we see an improvement in hop count values (TrustEpidemic). This is because the nodes become more interactive and cooperative with each other. As a result, our proposed algorithm has a positive effect on the epidemic routing protocol.

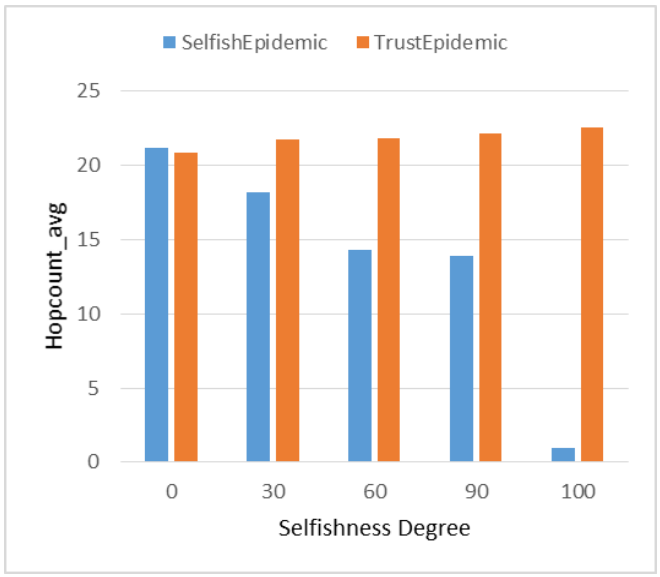

Figure 13 Hop Count Vs. Selfishness Degree

6. CONCLUSION

The utilization of DTN security forces computational expenses on DTN nodes. There might be limits regarding the amount of CPU that can be given to security mechanisms and the measure of calculation will rely upon the algorithms utilized and their parameters. Our proposed Cooperation Enforcement and Trust Algorithm (CETA) uses the fewest parameters and combines detecting selfish nodes with dealing with this threat by penalizing each selfish node in order to enforce cooperation in the DTN network and improve its performance. The simulation results show that our proposed mechanism outperforms other mechanisms in terms of improving network performance. We would like to test our proposed algorithm CETA over probabilistic routing protocols for DTN networks in the future, as well as implement it in heterogeneous network.

REFERENCES

[1] F. Hamza and S. M. C. Vigila, "Cluster Head Selection Algorithm for MANETs Using Hybrid Particle Swarm Optimization-Genetic Algorithm," Int. J. Comput. Netw. Appl., vol. 8, no. 2, pp. 119–129, 2021.

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

[3] 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.

[4] 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.

[5] S. Farrell, S. Symington, H. Weiss, and P. Lovell, "Delay-Tolerant Networking Security Overview," Internet Engineering Task Force, Internet Draft draft-irtf-dtnrg-sec-overview-06, Mar. 2009. Accessed: Aug. 19, 2021. [Online]. Available: https://datatracker.ietf.org/doc/draft-irtf-dtnrg-sec-overview-03

[6] 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.

[7] P. Goyal, S. Batra, and A. Singh, "A literature review of security attack in mobile ad-hoc networks," Int. J. Comput. Appl., vol. 9, no. 12, pp. 11–15, 2010.

[8] 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.

[9] Q. Li, S. Zhu, and G. Cao, "Routing in socially selfish delay tolerant networks," in 2010 Proceedings IEEE Infocom, 2010, pp. 1–9.

[10] A. Keränen, M. Pitkänen, M. Vuori, and J. Ott, "Effect of non-cooperative nodes in mobile DTNs," in 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, 2011, pp. 1–7.

[11] S. E. Loudari, M. Benamar, and N. Benamar, "New classification of nodes cooperation in delay tolerant networks," in International Symposium on Ubiquitous Networking, 2015, pp. 301–309.

[12] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks." Technical Report CS-200006, Duke University, 2000.

[13] 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.

[14] 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, 2005, pp. 252–259.

[15] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," ACM SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 19–20, 2003.

[16] C. C. Sobin, "Analyzing the impact of selfishness on probabilistic routing algorithms in Delay Tolerant Networks," in 2015 International Conference on Computing and Network Communications (CoCoNet), 2015, pp. 186–190.

[17] J. Burgess, B. Gallagher, D. D. Jensen, and B. N. Levine, "MaxProp: Routing for Vehicle-Based Disruption-Tolerant Networks.," in Infocom, 2006, vol. 6.

[18] A. Waqas, "Interference Aware Cooperative Routing Algorithm for Wireless Ad Hoc Networks over Nakagami Fading and Lognormal Shadowing," Int. J. Comput. Netw. Appl., vol. 3, no. 4, p. 78, Aug. 2016, doi: 10.22247/ijcna/2016/v3/i4/48568.

[19] L. Buttyán, L. Dóra, M. Félegyházi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," Ad Hoc Netw., vol. 8, no. 1, pp. 1–14, 2010.

[20] L. Liu, "A survey on barter-based incentive mechanism in opportunistic networks," in 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013, pp. 365–367.

[21] L. Wei, Z. Cao, and H. Zhu, "Mobigame: A user-centric reputation based incentive protocol for delay/disruption tolerant networks," in 2011 IEEE Global Telecommunications Conference-GLOBECOM 2011, 2011, pp. 1–5.

[22] F. Gai, J. Zhang, P. Zhu, and X. Jiang, "Trust on the ratee: a trust management system for social internet of vehicles," Wirel. Commun. Mob. Comput., vol. 2017, 2017.

[23] B. B. Chen and M. C. Chan, "Mobicent: a credit-based incentive system for disruption tolerant network," in 2010 Proceedings IEEE INFOCOM, 2010, pp. 1–9.

RESEARCH ARTICLE

[24] S. A. Ezzahidi, E. Sabir, S. Koulali, and E.-H. Bouyakhf, "Robust fully distributed file caching for delay-tolerant networks: A reward-based incentive mechanism," Int. J. Distrib. Sens. Netw., vol. 13, no. 4, p. 1550147717700149, 2017.
[25] S. Jain and A. Verma, "Bubble rap incentive scheme for prevention of node selfishness in delay-tolerant networks," in Smart innovations in communication and computational sciences, Springer, 2019, pp. 289–303.
[26] P. Nagrath, S. Aneja, and G. n. Purohit, "Taxonomy of reputation-based defending mechanisms against types of attacks in delay tolerant networks," Int. J. Secur. Netw., vol. 16, no. 2, pp. 77–91, Jan. 2021, doi: 10.1504/IJSN.2021.116772.
[27] A. Sharma, N. Goyal, and K. Guleria, "Performance optimization in delay tolerant networks using backtracking algorithm for fully credits distribution to contrast selfish nodes," J. Supercomput., vol. 77, no. 6, pp. 6036–6055, Jun. 2021, doi: 10.1007/s11227-020-03507-4.
[28] C. Ş. Şahin, S. Gundry, and M. U. Uyar, "Markov chain analysis of self-organizing mobile nodes," J. Intell. Robot. Syst., vol. 67, no. 2, pp. 133–153, 2012.
[29] https://www.netlab.tkk.fi/tutkimus/dtn/theone/pub/the_one.pdf
[30] R. S. Mangrulkar and M. Atique, "Routing protocol for Delay Tolerant Network: A survey and comparison," in 2010 International Conference on Communication Control and Computing Technologies, Oct. 2010, pp. 210–215. doi: 10.1109/ICCCCT.2010.5670553.

Authors

ZEKKORI Hanane received her master's degree in computer science at Hassan 1er University, Morocco in 2014.Currently, PHD Student, Dept. of computer Science of Faculty of Sciences and Techniques, University of Moulay Ismail, Errachidia, Morocco. Field of research: DTN Routing, DTN Security.

AGOUJIL Said Full Professor in computer Science at Faculty of Sciences and Techniques Errachidia, University of Moulay Ismail, Errachidia, Morocco. His research work falls within the framework Numerical analysis, Mobile Network (adhoc and DTN), Signal and Image processing, speech coding.

QARAAI Youssef had his PHD thesis in Applied Mathematics, systems analysis, and control option, in 2008 at the faculty of sciences and techniques of Tangier Morocco. Currently he is a professor in computer Science at Faculty of Sciences and Techniques Errachidia, University of Moulay Ismail, Errachidia, Morocco. His research work falls within the framework of the routing and security of mobile networks, as well as the modeling and simulation of road traffic.

How to cite this article:

Hanane ZEKKORI, Said AGOUJIL, Youssef QARAAI, "CETA: Cooperation Enforcement and Trust Algorithm to Handle Selfish Attack in Delay Tolerant Network", International Journal of Computer Networks and Applications (IJCNA), 8(5), PP: 585-595, 2021, DOI: 10.22247/ijcna/2021/209989.