New classification of nodes cooperation in Delay Tolerant Networks

New classification of nodes cooperation in Delay Tolerant Networks

Salah Eddine Loudari[1], Maria Benamar [1], Nabil Benamar [1],

[1] University Moulay Ismail Meknes Morocco

{salaheddine.loudari@gmail.com,
mariabenamar@gmail.com, benamar73@gmail.com}

Abstract. Delay and Disruptive Tolerant Networks (DTNs) is a concept related to environments characterized by very long delay paths and frequent network disruptions. DTN is nowadays a recognized area in networking and communications research, due to its suitability and practical experiences with mobile ad-hoc networks especially in situations where continuous end-to-end paths may not be always guaranteed. In DTNs, nodes store carry and forward messages, called bundles, to other nodes. The forwarding mechanism can occur opportunistically. However, some nodes may show some selfish or malicious behavior, which leads to less cooperation in the network. Thus, one of the main challenges in DTN is to ensure the security and confidentiality within the Network and assure cooperation among nodes. In this paper, we classify some of the threats that have been considered and treated by researchers in the field of DTN, and we propose a new classification based on the degree of cooperation of nodes. We describe different incentive mechanisms used to enhance cooperation among nodes in DTN environment focusing on the strengths of these mechanisms and also their limitations and drawbacks.

Keywords: Delay Tolerant Networks, cooperation, bundle

1 Introduction

Delay Tolerant Network is a network of regional networks; it is an occasionally-connected network [1] that permits communication where connectivity issues like long and variable delay, high error rates, sparse and intermittent connectivity, highly asymmetric data rate and non-end-to-end connectivity exist [2]. The purpose of the DTN is to support interoperability among these underlying stressed regional networks. DTN concept was originally designed for communicating with spacecraft, to compensate for disconnections over interplanetary distances [3]. However, after several years of research in the field of DTN, numerous implementations and applications have appeared with a broad variety of performance and application domains [4] (inter-planetary networks [3], underwater networks [5], wildlife tracking networks [6], military tactile networks [7]…). We regroup in table 1 the different examples of DTN application. A new work group has been created in the IETF to tackle DTN issues and application in terrestrial context [8].

The unit of information exchange in Delay Tolerant Networks is a bundle [9][10]. A DTN node is an entity with a bundle layer. A node may be a host, router, or gateway acting as a source, destination, or forwarder of bundles [4].

Fig.1 shows the bundle layer and its position with respect to the network layers when compared to the Internet layers. The DTN bundled layer is common across all the DTN regions while the lower layers are all region specific.

DTN utilizes the concept of store, carry and forward [11][12][13] (Fig.2) which is a long established form of postal system. Each node has a persistent storage system, which is used to store messages as backup just in case the network fails during transmission. The node stores bundle in its buffer for a certain time (can be minutes, hours or even days) and will be forwarded only when connection between the intermediate nodes is established.

DTN Applications	Purpose	DTN nodes	Delay
ZebraNet [6]	Track African zebras across large regions	Zebra, mobile base station	Hours or days
DakNet [14]	Digital communications for rural areas	Coaches, motorbikes, ox carts, kiosks, access points	Minutes or hours
KioskNet [15]	Digital communications for rural areas	Buses, kiosks, hand-held devices, desktop computers with a dial-up connection	Hours or days
Widernet [16]	To improve educational communication systems in Africa	Desktop computers with sufficient storage to store web sites with rich educational contents	Days or monhs

Table 1 : Example of DTN applications

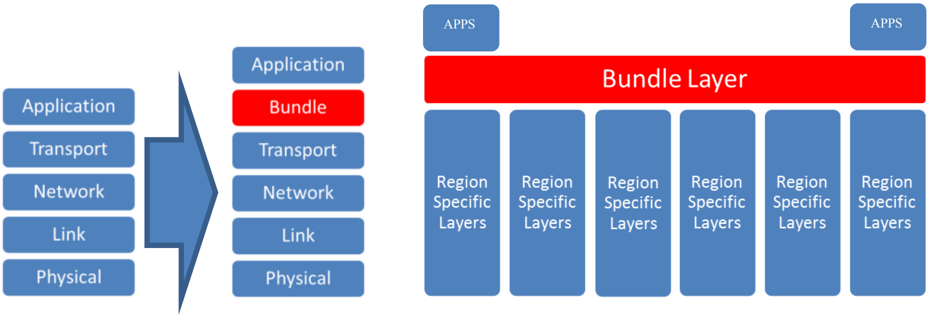

Fig. 1 Position of bundle layer

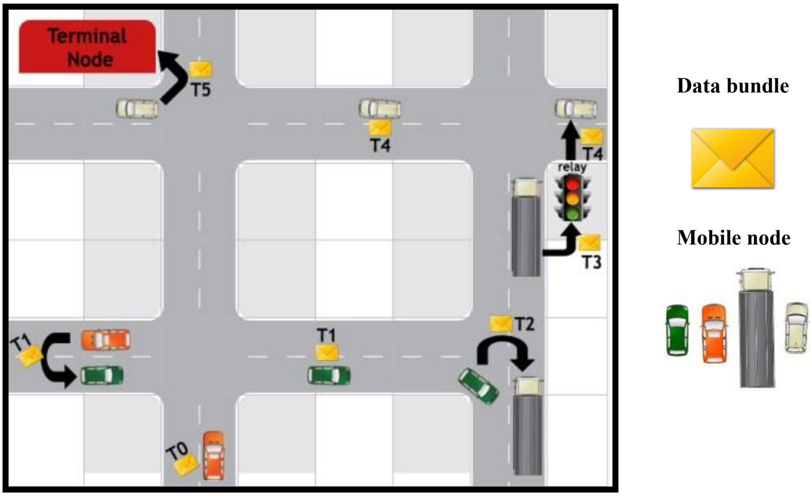

Fig. 2 Store-carry and forward paradigm

2 Security Threats: An overview

2.1 Non-DTN threats

The first series of threats to consider are those from the elements that are not directly part of the DTN, The network is an overlay network. Packets can traverse multiple underlying networks where the message might be edited or deleted.

An overlay network inherits all of the good and all of the bad of the underlying networks upon which it resides [17]. For example, if an overlay network passes over four or five different concatenated underlying networks, then the overlay network is vulnerable to all of the insecurities of any of the underlying networks. This makes overlay networks much more difficult to secure as one has to secure each underlying network in addition to applying proper security to the network overlay itself.

2.2 Resource consumption

Due to resource scarcity that characterizes DTN, unauthorized use of resources – particularly battery power and storage - can be considered as threats on the infrastructure of DTN [18]. For example, if an unauthorized application could control certain DTN infrastructures (through an attack on the routing protocol) resource consumption could be catastrophic for the network, which reduces its performance.

Limited resources challenge requires an efficient protocol design. In other words, nodes must utilize their limited hardware resources such as CPU, memory and battery efficiently. For example, in WSNs [19], nodes can be located in an open environment for years before data are collected, and hence it requires nodes to carefully manage their energy usage. Additionally, a good routing protocol will leverage the resources of multiple nodes. For example, nodes may choose to shift some of their stored bundles to other nodes to free up memory or to reduce transmission cost.

2.3 Routing attacks

Denial of Service

This type of attack must be considered in the DTN context because it is at the same position of other MANETs. So, all the problems with secure routing in ad-hoc networks exist for many DTNs too.

Denial of service is one of the major threats and among the toughest security issues in networks nowadays [20] because it attempts to limit access to a machine or service. The effect of Dos in Delay Tolerant Network is even more aggravated due to the scarcity of resources. Perpetrators of DOS attacks in DTN-like environments look beyond the objective of rendering a target node useless [21]. The aim of an attacker is to cause a network-wide degradation of resources, service and performance. This can easily be achieved by exhausting node or link resources and partitioning the network.

Black-Hole

This attack aims to destroy the network services, causing a sharp decline in delivery rate [22]. Malicious nodes involved in launching the black-hole attack disseminate false probable information delivery to increase -or decrease- their chances to be selected and attract the maximum number of messages to delete later.
Gray-hole It is an extension of the Black-hole attack where malicious nodes delete certain packets (as opposed to black-hole that remove all packages) [23].

Worm-Hole

Malicious nodes build a tunnel between each other using a low latency link to convince victims that it is the best path to send packets [24]. These nodes can manipulate the routing algorithm and control information that is shared by the honest nodes which disrupts the packet delivery operation.

Techniques	Objectives	Details
Bundle Authentication Block (BAB) [16]	Ensures bundle authenticity and integrity	Used to thwart DOS and to ensure routing information exchange between “neighboring” DTN nodes is authenticated.
Internet Security Association and Key Management Protocol (ISAKMP) [25]	Anti-clogging technique where a client is required to return a server generated cookie	Used to prove a client’s identity and is verified by the server before any costly authentication protocol is triggered.
Tackling the junk mail [20]	Tackle the problem of connection depletion attacks	Use cryptographic puzzles where a sender is required to compute a puzzle for very message sent. The cost of this technique is negligible for normal users when compared to mass mailers.

Table 2 Some solutions proposed to protect against attacks

3 Cooperation in Delay Tolerant Networks

Due to the uncertainty of transmission opportunities between nodes, Delay Tolerant Networks adopts a store–carry–forward method [26]. This method requires nodes to store and forward messages in a cooperative way. However, threats mentioned in the previous chapter directly affect the cooperation between nodes in the DTN and implicitly affect the performance of DTN.
The authors in [27] define three types of nodes behavior: cooperative nodes, partly-cooperative and uncooperative.

Cooperative nodes: stock and forward messages to another node without restriction.

Partly-cooperative: Agree to forward the messages coming from other nodes, but on condition that transmits messages directly to the destination.

Uncooperative: DTN are resource-constrained networks. The selfish behaviors may occur among the nodes to preserve its own resources (energy, storage space, CPU…) by ignoring the packet from other nodes and will forward only its own message [28]. Another type of uncooperative nodes is that malicious nodes provide forged metrics to other nodes that come in contact with and attract packets from them [29]. After receiving these forwarded packets the malicious node can either drop or modify them [30].
On the basis of types mentioned above, we propose a classification of node behavior (Fig. 3):

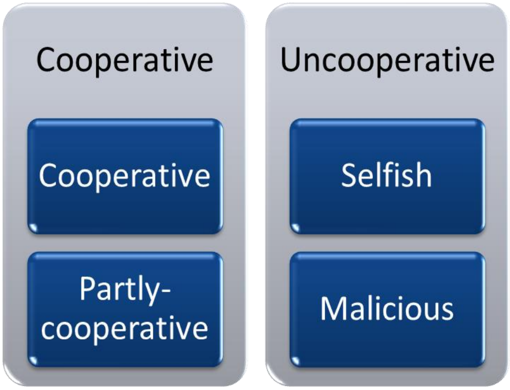

Fig. 3 Classification of node behavior

3.1 Impact of uncooperative behavior

The existing research works, based on theoretical analysis models and simulations, demonstrate two characteristics of the performance degradation caused by uncooperative behavior, Firstly, the routing performance (i.e., delivery ratio, delivery cost and delivery latency) is seriously degraded, if a major portion of the nodes in the network is selfish [31]. Secondly, the impact on the routing performance is related to the uncooperative behavior (i.e., non-forwarding of messages and dropping of messages). The behavior of non-forwarding of messages reduces the delivery cost, while the behavior of dropping of messages increases the delivery cost. However, both of them decrease the delivery ratio, and prolong the delivery latency, even if messages are eventually delivered.

3.2 Strategies for preventing uncooperative behavior

In order to reduce the impact of uncooperative behavior on routing performance, a number of studies focus on stimulating uncooperative nodes to be cooperative. The existing incentive strategies can be classified into three categories [27]: Barter based, Credit based and Reputation based, table 3 summarizes these strategies. In the following sections, we present a comprehensive discussion about these different strategies.

Barter-based strategies

Barter-based or pair wise Tit-For-Tat strategy is the simplest strategy and one of the most popular motivations to tackle the problem of uncooperative behavior [32]. It is based on the fact that every node forwards as much traffic for a neighbor as the neighbor forwards for it. In [33], the authors divide the message into two types: primary messages and secondary message. A message is a primary message for a given mobile

node, if the mobile node is interested in the content of the message and secondary if the mobile node is not. It is worth for the users collecting messages even if they are not interested in them to exchange them later for messages that they are interested in.
However, the requirement of exchanging the same amount of messages is a two-edged sword. The problem is when the node has no enough messages to exchange; the message should not be delivered to destination even if the destination is in connection [32], which reduces routing performances.

Credit-based strategies

Due to disadvantages of barter-based, Credit-based strategies are proposed to avoid these disadvantages. This strategy encourages nodes to be cooperative by paying reward for cooperative nodes. The concept is that if a node cooperates to forward a message for others nodes, it receives an amount of credit as a reward that it can later explore for its own benefit.
Credit-based strategies can be subdivided into two models [31]: **Message Purse Model**: the source node pays credits to nodes which participate in delivering the message to the destination. **Message Trade Model**: the source node do not pay for the message forwarding, contrary to message purse model, the receiver pays credits to the sender of a message until the message reaches the destination, which finally pays for the message forwarding. Because the source nodes do not pay for the message forwarding, the network can be flooded by the source node. For this reason, most of the credit-based works utilize the message purse model.

Reputation-based strategies

In Reputation-based strategies, each node observes the behavior of other nodes and assigns each of them a reputation, which measures how well a node is behaving. Reputation is calculated from the opinion of neighbor. The routing of messages is done on the basis of the reputation: the lower the reputation the lower the probability that a node is chosen as next hop for forwarding a message [34].

Reputation-based strategies can work even if a major portion of the malicious nodes. However, this kind of strategy mistakenly considers the collaboration of intermediate nodes as selfish behavior, which results in the decrement of the delivery probability of the messages generated.

Strategies	advantages	Limitations
Barter-based	Requirement of exchanging the same amount of message	When the node has no enough messages to exchange
Credit-based	Encourage nodes to be cooperative by paying reward	Cannot work in an environment in which the nodes have a high probability of being selfish to other nodes
Reputation-based	Work well even if a major portion of the nodes are uncooperatives	Consider the collaboration of intermediate nodes as selfish behavior

Table 3 Advantages and limitations of preventing strategies

4 Conclusion

In this paper, we presented an overview of the various security threats in Delay Tolerant Networks such as non-DTN threats, resource consumption and routing attacks. We focused on threats related to nodes behavior and cooperation and their effects on DTN performances. Thus, we proposed a new cooperation degree classification: Cooperative node (Fully cooperative and partly cooperative), and uncooperative node (Malicious, selfish and misbehaving). We pointed out the negative impact of uncooperative behavior on the network, and we presented the existing strategies aiming to solve or at least to reduce the impact of this issue. We discussed their strengths and we made a special focus on the limitations of these strategies and their drawbacks.
Due to the importance and the utility of Delay Tolerant Networks, especially in their terrestrial applications, further work should take into consideration security threats in order to solve the problems encountered in these networks and reduce the negative impact of threats.

5 References

[1] K. Scott and S. Burleigh, “Bundle Protocol Specification,” RFC 5050, November 2007.

[2] P. Rog, A. Casaca, S. Member, J. J. P. C. Rodrigues, V. N. G. J. Soares, S. Member, J. Triay, and C. Cervell, “From Delay-Tolerant Networks to Vehicular Delay-Tolerant Networks,” IEEE Commun. Surveys Tuts. , vol. PP, no. 99,pp. 1–17, 2011.

[3] S. Burleigh, A. Hooke, L. Torgerson, B. Durst, K. Scott, and T. M. Corporation, “Delay-Tolerant Networking : An Approach to Interplanetary Internet,” IEEE Communications Magazine, pp. 128–136, 2003.

[4] A. G. Voyiatzis, “A Survey of Delay- and Disruption-Tolerant Networking Applications,” Journal of Internet engineering vol. 5, no. 1, pp. 331–344, 2012.

[5] J. Partan, J. Kurose, and B. N. Levine, “A survey of practical issues in underwater networks,” Proc. 1st ACM Int. Work. Underw. networks - WUWNet ’06, p. 17, 2006.

[6] P. Juang, H. Oki, and Y. Wang, “Energy-Efficient Computing for Wildlife Tracking : Design Tradeoffs and Early Experiences with ZebraNet,” Proc. ASPLOS, Oct 2002.

[7] R. Krishnan, P. Basu, J. M. Mikkelson, C. Small, R. Ramanathan, D. W. Brown, J. R. Burgess, A. L. Caro, M. Condell, N. C. Goffee, R. R. Hain, R. E. Hansen, C. E. Jones, V. Kawadia, D. P. Mankins, B. I. Schwartz, W. T. Strayer, J. W.

Ward, D. P. Wiggins, and S. H. Polit, “The SPINDLE Disruption-Tolerant Networking System,” MILCOM 2007 - IEEE Mil. Commun. Conf., pp. 1–7, Oct. 2007.

[8] DTN Work Group, http://datatracker.ietf.org/list/wg/

[9] N. Benamar, K. D. Singh, M. Benamar, J. Bonnin and D. El Ouadghiri,, “Routing protocols in
Vehicular Delay Tolerant Networksm: A comprehensive survey,” Elsevier, Computer Communication (Com Com), vol. 48, pp. 141–158, 1 April 2014.

[10] Benamar, N.; Benamar, M.; Bonnin, J.M., "Routing protocols for DTN in vehicular environment," Multimedia Computing and Systems (ICMCS), 2012 International Conference on , vol., no., pp.589,593, 10-12 May 2012

[11] N. Benamar, M. Benamar, S. Ahnana, F.Z. Saiyari, M.D. el Ouadghiri, J.-M. Bonnin, Are VDTN routing protocols suitable for data collection in smart cities: a performance assessment, J. Theor. Appl. Inf. Technol. 58 (3) (2013) 589–600.

[12] M. Benamar, S. Ahnana, F.Z. Saiyari, N. Benamar, M.D. El Ouadghiri, J.-M.Bonnin, Study of VDTN routing protocols performances in sparse and dense traffic in the presence of relay nodes. J. Mob. Multimedia, 10 (1&2), 2014, 78– 93.

[13] M. Benamar, N. Benamar, K. D. Singh, D. El Ouadghiri. Recent study of Routing protocols in VANET: Survey and Taxonomy. WVNT 2013 : 1st International Workshop on Vehicular Networks and Telematics, May 2013, Marrakech, Morocco. 2013

[14] http://www.unitedvillages.com/

[15] S. Guo, M. H. Falaki, E. A. Oliver, S. U. Rahman, A. Seth, M. A. Zaharia, and S. Keshav, “Very Low-Cost Internet Access Using KioskNet.”, ACM Computer Communication Review, Oct. 2007.

[16] http://www.widernet.org/

[17] W. D. Ivancic, “Security analysis of DTN architecture and Bundle Protocol Specification for space-based networks,” 2010 IEEE Aerosp. Conf., pp. 1–12, Mar. 2010.

[18] DTN Research Group - www.dtnrg.org/

[19] T. V. Prabhakar, A. U. Nambi S.n, H. S. Jamadagni, K. Swaroop, R. V. Prasad, and I. I. M. M. Niemegeers, “A novel DTN based energy neutral transfer scheme for energy harvested WSN Gateways,” ACM SIGMETRICS Perform. Eval. Rev., vol. 38, no. 3, p. 71, Jan. 2011.

[20] P. S. Ardra, “A Survey On Detection And Mitigation Of Misbehavior In Disruption Tolerant Networks,” vol. 2, no. December, pp. 656–660, 2012.

[21] G. Ansa, H. Cruickshank, and Z. Sun, “A Proactive DOS Filter Mechanism for Delay Tolerant Networks.” ICST PSATS, Conference, Malaga Spain, February 2011

[22] S. Jain, “Black Hole Attack in Delay Tolerant Networks : A Survey,” no. 4, pp. 172–175, 2014.

[23] M. Nogueira, H. Silva, A. Santos, and G. Pujolle, “A Security Management Architecture for Supporting Routing Services on WANETs,” IEEE Trans. Netw. Serv. Manag., vol. 9, no. 2, pp. 156–168, Jun. 2012.

[24] Y. Ren, M. C. Chuah, J. Yang, and Y. Chen, “Detecting wormhole attacks in delay tolerant networks,” IEEE Wireless Commun. Mag., vol. 17, no. 5, pp. 36–42, Oct. 2010.

[25] M. Onen and R. Molva, “Denial of service prevention in satellite networks,” 2004 IEEE Int. Conf. Commun. (IEEE Cat. No.04CH37577), pp. 4387–4391 Vol.7, 2004.

[26] R. S. Mangrulkar and M. Atique, “Procedia Computer Science Heterogeneous Highly Dense Mobile Environment,” vol. 00, pp. 1–13, 2013.

[27] A. Keranen, M. Pitkanen, M. Vuori and J. Ott, “Effect of Non-cooperative Nodes in Mobile DTNs.” In Proc. 2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), pp.1-7, Jun. 2011.

[28] D. Mishra and M. Chawla, “Minimax Theory Based Scheme to Detect Selfish Node and Reduce Latency in Delay Tolerant Network,” vol. 2013, no. Cac2s, pp. 78–82, 2013.

[29] S. Ahnana, F.Z. Saiyari, N. Benamar, M.D. el Ouadghiri, “Study of DTN routing protocols in vehicular environment in the presence of misbehaving nodes” Proc. - WINCOM, 2013.

[30] F. Li, J. Wu, and A. Srinivasan, “Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets,” Proc. - IEEE INFOCOM, pp. 2428–2436, 2009.

[31] J. Miao, O. Hasan, S. Ben Mokhtar, L. Brunie, and K. Yim, “An Analysis of Strategies for Preventing Selfish Behavior in Mobile Delay Tolerant Networks,” 2012.

[32] L. Liu, “A survey on barter-based incentive mechanism in opportunistic networks,” 2013 2nd Int. Symp. Instrum. Meas. Sens. Netw. Autom., pp. 365–367, Dec. 2013.

[33] L. Buttyan, L. Dora, M. Felegyhazi, and I. Vajda, “Barter trade improves message delivery in opportunistic networks,” Ad Hoc Networks, vol. 8, no. 1, pp. 1–14, 2010

[34] G. Dini and A. Lo Duca, “Ad Hoc Networks Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network,” Ad Hoc Networks, vol. 10, no. 7, pp. 1167–1178, 2012.