A Study of Black Hole Attacks in Delay Tolerant Network

Puneet and Anamika Chauhan

Abstract DTN is the latest growing technology having unique characteristics such as longer delays, intermittent connectivity and limited resources or constrained resources. Delay tolerant networks is a store and forward method which delivered the messages to the nearest potential forwarder by replicating copies of the original messages. DTN is created to handle long delays in wireless networks and handle the intermittent connectivity. An information at particular node is delivered only if it has higher particular than the current node. DTN is studied and implemented in opportunistic network environment (ONE) simulator. DTN is having characteristics like disconnected paths, long delays, higher mobility, uplinks, and downlinks, which leads to network vulnerabilities. These vulnerabilities lead to the compromisation of nodes and can cause security threats as these compromised nodes can disrupt the routing protocols in the network. DTN is exposed to different network layer attacks. Attacks on network layer like gray hole and black hole attack can destroy the topology of the network resulting in loss of data and damage to the network. This paper discusses about the black hole, type of black hole attacks, and different detection techniques in delay tolerant networks.

Keywords Delay tolerant network (DTN) · Wireless networks · Network connectivity · Opportunistic network environment (ONE) · ONE simulator

1 Introduction

A DTN is an ad-hoc network which tries to resolve various issues of heterogeneous networks such as facing failures in point to point and continuous\ connectivity. DTN is extremely useful in various applications areas such as: providing connectivity in remote areas where providing an infrastructure connection is costly, wireless sensor

Puneet (✉) · A. Chauhan
Department of Information Technology, Delhi Technological University, New Delhi, India
e-mail: puneetbisarwal@gmail.com

A. Chauhan
e-mail: anamika@dce.ac.in

M. Chakraborty et al. (eds.), *Trends in Wireless Communication and Information Security*,
Lecture Notes in Electrical Engineering 740,
https://doi.org/10.1007/978-981-33-6393-9_2

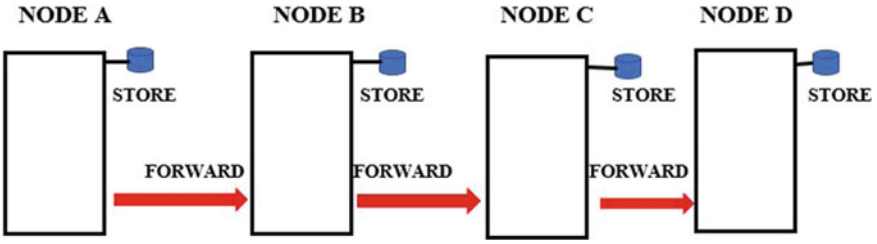

Fig. 1 Store and forward message

network for tracking wildlife animals and birds, military communications and control sensors, and equipment. DTN networks are highly desirable for use in war-prone areas, remote places in relief efforts, and in disaster scenarios. DTN which is also known as delay and disruption-tolerant network is used where there is a lack of connectivity in the network which results in spontaneous end-to-end paths being insufficient for communication. In such cases where there are no network infrastructures, a critical mode of communication can be given by DTNs network. DTN is a complete wireless network as there is no base station as compared to an existing wireless network.

DTN is a type of architecture in which it can forward, store, or carry the messages. It stores information in the node buffer until a possible forwarder is found and forward it to the next node's buffer which is available in the network [1].

In DTN protocol stack, there is a bundle layer, and in this layer, the messages are stored as "bundles." These bundles are sent as soon as they come across with a receiver node. The requirement for DTN network is due to node disconnection by equipment failure (Fig. 1).

In DTN, message transmission through intermediate nodes is difficult because the intermediate nodes can act as a malicious node, a malicious node either drop the message or not forward the message to the destination.

In DTN, in scenarios where nodes have intermittent and opportunistic communication connectivity, networks are established. DTN does not have a very large storage space, very limited power supply, and battery-operated devices may be used. One of the challenges of DTNs is the intermittent connectivity while another challenge may be handling misbehaving nodes. Misbehave means acting badly or improperly. Misbehave node in a network does not perform its task properly. It is possible to classify misbehaving nodes into two types: malicious and selfish. A selfish node is one which drops all messages to save its own energy and prefers not to contribute to the network while forwarding only its own packets or messages. Malicious nodes acts as a forwarder and sends copies of the original message to as many nodes as possible. These nodes attempt to hamper various parameters of the network. Malicious nodes attack routine network operations and are not concerned about their gains in the process. To handle these types of nodes, DTN security protocols must be more invulnerable and powerful. The existence of such nodes in vehicle DTNs

results in the loss of crucial data or messages that may trigger more road accidents or may cause resource wastage in resource constraints DTNs.

The structure of the paper is defined below. Architecture of DTN is discussed in Sect. 2. While challenges in DTN are discussed in Sect. 3. In Sect. 4, we had discussed AODV protocols, black hole attacks, and different detection techniques. In Sect. 5, conclusion and future work is discussed.

2 DTN Architecture

In extreme and challenging environmental conditions, continuous connectivity is not feasible. DTN research group [2] developed the architectural and protocol design principles required to address this problem and provide interoperable communications in such environments. Example-space network (SN), deep space network (DSN), military equipment, underwater submarines, forms of disaster response, and ad-hoc sensors/actuator networks.

Initially, Kevin Fall proposed the challenged network in delay tolerant networks in 2003, but it was properly documented and standardized by the DTN research group as RFC 4838 in 2007 [3, 4]. Message switching abstraction is a key component in the DTN network and is developed to work as an overlay network. It works on top of protocol stack for the various types of networks to make provision for the gateway feature between them, also called 'bundle layer' [5].

The DTN architecture requires a small re-vamp of the design of the Internet protocol layer that had already been developed. Depending on their appropriateness for each region in the network, the transport layer below the bundle layers is chosen. Figure 2 gives us an idea or an overlay of how the bundle layer looks like compared to the Internet protocol layers.

3 Challenges in DTN

We discussed various challenges during data transmission in DTN in this section. These are the following areas:

i. Capacity to Store: The capacity to store message of every node is limited or confined. Due to this, at whatever point an experience happens to the node, the node attempts to swap each and every information they have in their storage or buffer. If the nodes have an unlimited storage capacity, the node will flood it with similar kind of information or messages, and adversity will arise [6].
ii. Battery or Power Constraints: The battery or power constraint is limited to the node. So, the node have to perform their operations in that limited battery.
iii. Network Capacity: Limiting the basic system is also a crucial element in determining the measure of information that can be transmitted. On the off chance

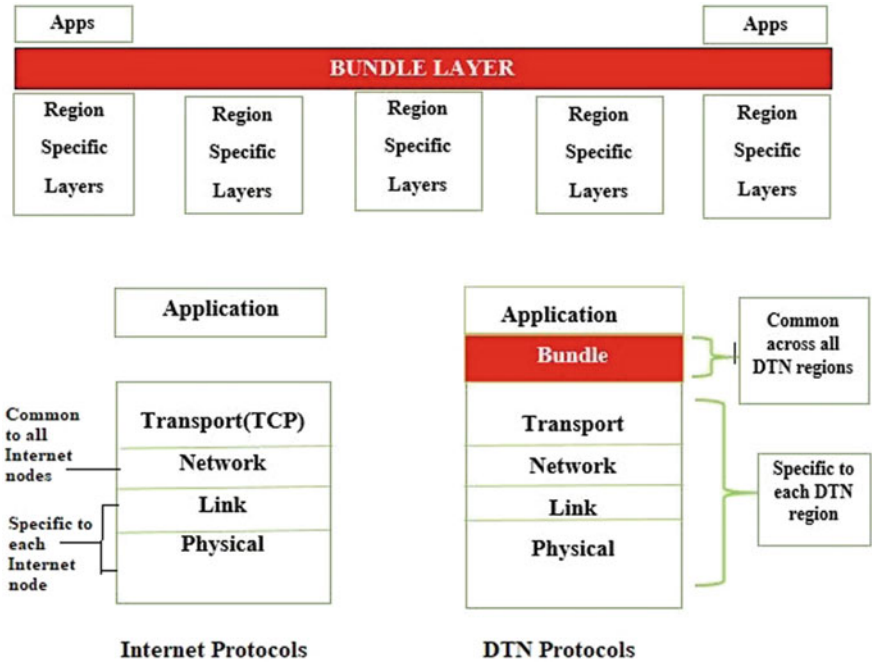

Fig. 2 DTN bundle layer architecture

that, in the mid of experience, different nodes are trying to forward information, and the system may be congested. Therefore, this component decides whether or not to divide a message or data packets with a specific end goal of transmitting it from source to target node.

iv. Encounter Schedule: Every node has a specific end goal of sending the data from the transmitter to the destination node, the node will not transmit if the receiver's node is unreachable and immediately transmit the message to the receiver's node if it becomes reachable.

4 AODV Protocol

4.1 Ad-hoc on Demand Distance Vector Protocol (AODV)

Route Discovery

It uses route request (RREQ) packet which is broadcasted by the sender's node for the discovery of the route in the network. After that, the participating nodes continuously look over the routing table to get the path for the receiver's node [7]. In the end, the route reply packet (RREP) is transmitted to the sender's node, if it discovers a better and updated route in the network. When multiple route requests are received, then the

node chooses the shortest route for data transmission. Figure 3 indicates the details in RREQ and RREP.

Maintenance of Route

The nodes in mobile ad-hoc network (MANET), as the name suggests have mobility. The routes are being divided into sender and receivers if there is any change in the topology [8]. At this point, the route error (RERR) packet will be produced if there is any breakage in the route.

4.2 Black Hole Attack

The malicious node can provide a manipulated metrics to other nodes that comes into contact with the malicious nodes and attracts packets from the attacks which is done by black hole. In this attack, most of the data packets of the participating nodes are attracted by the malicious nodes. The node forcefully tries to create a path by its own. When the path is created, then instead of forwarding packets the malicious node drops them, thus creating a black hole.

The effect of black hole is that it exploits routing protocols like AODV, and its functionality in the network is degraded.

Black hole types [9].

Single node black hole

There is only one malicious node present between the transmitter and the destination (Fig. 4).

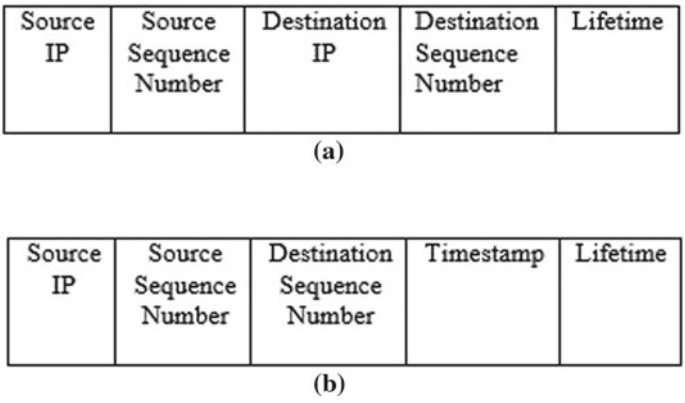

Fig. 3 Packet in AODV **a** RREQ, **b** RREP

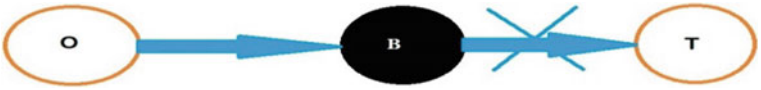

Fig. 4 Single node black hole

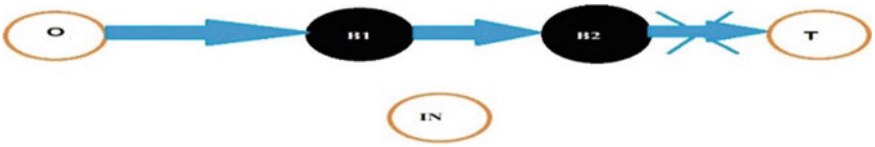

Fig. 5 Multiple black hole node

Multiple Black Hole

There are many malicious node present between the sender and the receiver (Fig. 5).

Origin node '*O*' tries to find a path for data transmission to the target node '*T*' as shown in Fig. 6. It begins the process of route discovery by transmitting the packet of RREQ across the entire network. From Fig. 6, we can see that nodes '*B*' and '1' accept the RREQ data packet from origin 'O'. Black node is a hostile node, and hence, it immediately produces RREP data packets without examining its routing tables.

Origin node '*O*' immediately receives RREP from the black node, so it initiates data transfer to the black node, presuming it generates the shortest route to target node '*T*'. Malicious black node discards the data packets, instead of sending those to the target node 'T', thus the decrease of overall throughput in the network can be seen (Table 1).

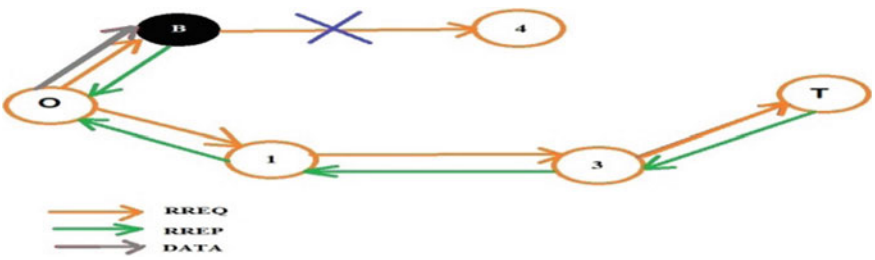

Fig. 6 Black hole attack in AODV

Table 1 Comparative analysis of black hole attack

Sr. no.	Techniques	Routing protocol	Simulator	Results and remark
1	Reply based on destination and next hop information scheme [10]	AODV	NS-2	Throughput is increased in ADOV, and the overhead is minimized. Malicious node is not found which act in group
2	Scheme based on shared hop and sequence number [11]	AODV	NS-2	Verify routes from 80 to 99% due to long delays, the last sequence number can be put in the table by the attacker
3	2-ACK scheme [12]	Dynamic source routing (DSR)	NS-2	Packet delivery ratio (PDR) is achieved up to 91% even if the node is malicious at 40% challenging to derive triplet information
4	Ignorance scheme [13]	ADOV	NS-2	Minimize additional overhead, PDR increased by 19% node packet loss in the network increased by 4%
5	Sequence number and voting scheme based on neighbors [14]	AODV	–	False detection rate is reduced, and malicious node was not found in the group
6	Neighbors opinion scheme [15]	AODV	–	With minimal delay and overhead, better security is achieved, and PDR is high with few additional delay
7	Packet delivery information scheme [16]	PROPHET	NS-2	100% is the detection rate, false positive rate is less, More independent examination method
8	Sequence number scheme [17]	AODV	NS-2	More packets delivered, data packet drops are dependent on the number of nodes and speed
9	Ranks given to nodes [18]	Modified AODV	–	Can judge new nodes as a black hole, energy efficient

(continued)

Table 1 (continued)

Sr. no.	Techniques	Routing protocol	Simulator	Results and remark
10	Using 'NTT' & 'PB' for Neighbor trust values [19]	AODV, TSDRP	NS-2	Present in large network, robustly built, overhead increased additional node calculations
11	NHBADI [20]	AODV	NS-2	Delay decreased, packet delivery fraction (PDF) increased
12	Using threshold levels for secure route discovery (SRD) [21]	AODV, SRDAODV	NS-2	Increase in packet delivery fraction (PDF) and overhead
13	Using 'fm' and 'rm' for Neighbor trust values [22]	Modified AODV	NS-2	Increase in PDF and overhead. Nodes must perform additional calculations
14	Base node sends bogus RREQ packets [23]	AODV	NS2-2.34	Increase in throughput, packet delivery ratio and slight increase in delay. Cannot protect against black hole node without base node

5 Conclusion and Future Work

The paper describes, various attack in DTN, its architecture, and its challenges that are presented. This review paper also describes about malicious and selfish nodes which is a major security challenges. This paper also compare black hole attack detection schemes with results, and limitations have been provided. In future, it is intended to propose a new methodology that detects black hole nodes and prevent network from black hole node attack.

References

1. Goncharov V (2010) Delay-tolerant networks. Institut fur Informatik, Albert Ludwigs Universitat Freiburg, Lehrstuhl fur Rechnernetze und Telematik
2. IRTF (2009) Delay tolerant networking research group, https://www.dtnrg.org
3. Kevin F (2003) A delay-tolerant network architecture for challenged internets. In: Proceedings of the 2003 conference on applications, technologies, architectures, and protocols for computer communications. ACM, pp 27–34
4. IRTF (2007) RFC 4838— DTN Architecture, https://www.ietf.org/rfc/rfc4838.txt
5. Warthman F (2012) Delay-and disruption-tolerant networks (DTNs). A Tutorial. V.0. Interplanetary Internet Special Interest Group

6. Khabbaz MJ, Assi CM, Fawaz WF (2011) Disruption-tolerant networking: a comprehensive survey on recent developments and persisting challenges. IEEE Commun Surveys Tutor 14(2):607–640
7. Tamilselvan L, Sankaranarayanan V (2007) Prevention of blackhole attack in MANET. In: The 2nd ınternational conference on wireless broadband and ultra wideband communications (AusWireless 2007). IEEE, pp 21–21
8. Mandala S, Abdul HA, Abdul SI, Habibollah H, Md AN, Yahaya C (2013) A review of blackhole attack in mobile adhoc network. In: 2013 3rd ınternational conference on ınstrumentation, communications, ınformation technology and biomedical engineering (ICICI-BME). IEEE, pp 339–344
9. Su M-Y, Kun-Lin C, Wei-Cheng L (2010) Mitigation of black-hole nodes in mobile ad hoc networks. In: International symposium on parallel and distributed processing with applications. IEEE, pp 162–167
10. Deng H, Li W, Agrawal DP (2002) Routing security in wireless ad hoc networks. IEEE Commun Mag 40(10):70–75
11. Al-Shurman M, Seong-Moo Y, Seungjin P (2004) Black hole attack in mobile ad hoc networks. In: Proceedings of the 42nd annual Southeast regional conference. ACM, pp 96–97
12. Liu K, Deng J, Varshney PK, Balakrishnan K (2007) An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans Mob Comput 5:536–550
13. Dokurer S, Erten YM, Can EA (2007) Performance analysis of ad-hoc networks under black hole attacks In: Proceedings 2007 IEEE SoutheastCon. IEEE, pp 148–153
14. Deb, M (2008) A cooperative black hole node detection mechanism for ADHOC networks. In: Proceedings of the world congress on engineering and computer science, pp 343–347
15. Medadian M, Mohammad HY, Amir MR (2009) Combat with black hole attack in AODV routing protocol in MANET. In: 2009 First Asian himalayas ınternational conference on ınternet. IEEE, pp. 1–5
16. Ren Y, Mooi CC, Jie Y, Yingying C (2010) Detecting blackhole attacks in disruption-tolerant networks through packet exchange recording. In: 2010 IEEE ınternational symposium on" a world of wireless, mobile and multimedia networks (WoWMoM). IEEE, pp 1–6
17. Tseng F-H, Chou L-D, Chao H-C (2011) A survey of black hole attacks in wireless mobile ad hoc networks. Hum-Cent Comput Inf Sci 1(1):4
18. Biswas S, Tanumoy N, Sarmistha N (2014) Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In: 2014 applications and ınnovations in mobile computing (AIMoC). IEEE, pp 157–164
19. Chaubey, N, Akshai A, Savita G, and Keyurbhai AJ (2015) Performance analysis of TSDRP and AODV routing protocol under black hole attacks in manets by varying network size. In: 2015 fifth ınternational conference on advanced computing & communication technologies. IEEE, pp 320–324
20. Babu MR, Usha G (2016) A novel honeypot based detection and isolation approach (NHBADI) to detect and isolate black hole attacks in MANET. Wireless Personal Commun 90(2):831–845
21. Tan, S, Keecheon K (2013) Secure Route Discovery for preventing black hole attacks on AODV-based MANETs. In: 2013 IEEE 10th ınternational conference on high performance computing and communications & 2013 IEEE ınternational conference on embedded and ubiquitous computing. IEEE, pp 1159–1164
22. Siddiqua A, Kotari S, Arshad AKM (2015) Preventing black hole attacks in MANETs using secure knowledge algorithm. In: 2015 ınternational conference on signal processing and communication engineering systems. IEEE, pp 421–425
23. Jain S, Ajay K (2015) Detecting and overcoming blackhole attack in mobile Adhoc Network. In: 2015 ınternational conference on green computing and ınternet of things (ICGCIoT). IEEE, pp 225–229