ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

A Probabilistic Misbehavior Detection Scheme in DTN: Survey

Prerana S. Jagadale, PrashantJawalkar

PG Scholar, Department of Computer Engineering, JSPM'S BhivarabaiSawant Institute of Technology & Research, Pune, Maharashtra, India

Assistant Professor, Department of Computer Engineering, JSPM'S BhivarabaiSawant Institute of Technology & Research, Pune, Maharashtra, India

ABSTRACT: Delay/ Disruption Tolerant Networking (DTN) program is an emerging technology that can facilitate access to information when secure end-to-end paths cannot exist.Disruption tolerant network is a different type of wireless network. It is an intermittently connected mobile network. Delay tolerant network adopts a store carry-and-forward mechanism, of which all the participants are assumed to cooperate with one another in message delivery, to overcome the challenges of the intermittent connection and the time-varying network topology. Here, at maximum time there does not exist a clear way from source to the destination. It also has a limitation in network resources. The DTN allows communication only if it is in the communication range. Because of this constraint there is a chance of dipping the received packets by the selfish or malicious nodes. Finally this leads to attacks. Malicious nodes within a DTN may attempt to delay or destroy data in transit to its destination. Such attacks include dipping data, saturating the network with extra messages, humiliating routing tables, and imitating network acknowledgments. Misbehaving nodes consume network resources, plummeting its concert and accessibility; therefore they constitute an important problem that should be considered.Many approaches are proposed to solve the problems which are occurred in DTN.In this paper I am focus on delay tolerant network architecture and its working and also focus on malicious or selfish node behavior.

KEYWORDS: Delay tolerant network; malicious node; detection; mitigation; security

I. INTRODUCTION

Delay tolerant networking is a networking architecture that is designed to provide communications in the most unstable and stressed environs, where the network would generally be topic to regular and long lasting disruptions and high bit error rates that could severely degrade normal communications. Delay tolerant networks are frequently used in disaster relief assignments, peace-keeping assignments, and in vehicular networks. DTN is based on a new experimental protocol called the Bundle Protocol (RFC 5050). Delay tolerant networks utilize the mobility of nodes. The nodes can move anywhere at any time. In a delay tolerant networks all devices search for nearer visible devices. Due to the intermittent connectivity it is very difficult to maintain end-to-end connections. This consents the furthering of data, only if it is in dealings with other nodes. So many traditional protocols and conventional routing schemes are failed under this long propagation delay. The basic idea behind DTN network is that endpoints aren't always unceasinglylinked. In order to aid data transfer, DTN usages a store-and-forward methodologyathwart a router that is more disruption-tolerant than TCP/IP. A delay tolerant network (DTN) is a network designed so that temporary or intermittent communications evils, restrictions and incongruities have the smallestpossible adverse impact. There are several aspects to the effective design of a DTN, containing:

- The usage of fault-tolerant techniques and technologies.
- The superiority of agiledilapidationunderhostilesituations or great traffic loads.
- The capacity to preclude or rapidlyrecuperate from electronic attacks.
- Capability to function with negligibledormancy even when routes are unclear or unpredictable.

Fault-tolerant systems are designed so that if a component fails or a network route turns out to beimpracticable, a backup module, process or path can immediately take its place without forfeiture of service. At the software level, an

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

interface consents the administrator to continuously monitor network traffic at multiple points and locate evilsinstantaneously. In hardware, fault tolerance is achieved by component and subsystem redundancy. Graceful degradation has always been important in large networks.

However, the DTN approach doesn't necessarily mean that all DTN routers on a network would require large storage capacity in order to maintain end-to-end data integrity. For establishing routing between the sender and receiver flooding related technique is used. In flooding linkedtechniqueenormous energy will be wasted. It reduces the delay tolerant networks performance. Packet Transfer ratio will be condensed by the selfish or malicious nodes. In the DTN security model nodes are classified as two types such as misbehaving nodes and normal nodes. Delay Tolerant Networks getting disconnection because of low node density and mobility. In the Department of Defense's wireless tactical networks, connectivity is often disrupted by terrain, weather, jamming, movement, or destruction of nodes. Such disruption makes it impossible to determine a path, halting the flow of data. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to flooding attacks. Based on the infrastructure and application security related problems may arise in the Delay Tolerant Networks such as authorization and data confidentiality obstacles.

In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Selfish nodes misbehave by showing unwillingness to spend resources such as power and buffer on forwarding packets of others while the malicious nodes that drop packets to launch attacks. These will result in routing misbehavior in DTNs. There are several techniques proposed to detect and mitigate this routing misbehavior in network.Several techniques have been proposed to detect and alleviate the effects of such selfish nodes in MANETs [5]. In [5], two techniques were presented, i.e., watchdog and path rater, to detect and mitigate the belongings of the routing misbehavior, respectively. The watch- dog technique identifies the misbehaving nodes by overhearing on the wireless medium. The path rater technique countenances nodes to avoid the use of the misbehaving nodes in any future route selections.The watchdog procedure is founded on inactive overhearing. In order to mitigate the adverse effects of routing misbehavior, the misbehaving nodes want to be identified so that these nodes can be avoided by all well-behaved nodes.

II. LITERETURE SURVEY

A. DELAY TOLERANT NETWORK

A delay-tolerant network (DTN) is a network of regional networks. It is an overlayon top of regional networks, comprising the Internet. DTNs sustenanceinteroperability of regional networks by accommodating long delays between and within regional networks, and by decipheringamongst regional network communication characteristics. In providing these functions, DTNs ac-accommodate the mobility and limited power of evolving wireless communication devices. The wireless DTN technologies may be diverse, including not only radio frequency (RF) but also ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies.
There are several characteristics of DTN as follows:

- Intermittent connectivity
- Long or variable delay
- Asymmetric data rates
- High error rates

Store-And-Forward Message Switching

DTNs overcome the problems associated with intermittent connectivity, elongated or mutable delay, distorted data rates, and great error rates through store-and-forward message switching. As shown in Fig.1. whole messages (entire blocks of application program user data) or fragments of such messages are forwarded from a storage place on one node to a storage place on another node, beside a path that in timegrasps the destination. DTN routers need persistent storage for their queues because

– A communication connection may not be accessible for a long time
– One node may send or receive data much quicker or more reliably than the other node
– A message, once transmitted, may need to be retransmitted for some reasons

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

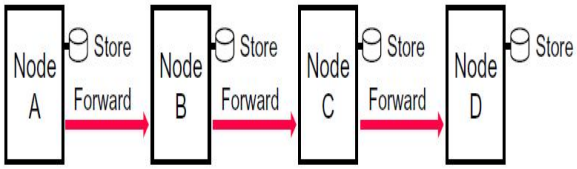

Fig.1.Store and forward message

Intermittent Connectivity

A growing number of communicating devices are in motion and operate on limited power. When communicating nodes are in motion, links can be obstructed by intervening bodies. When nodes must conserve power or preserve secrecy, links are shut down. These events cause intermittent connectivity. When no path exists to connect a source with a destination, a network partition is alleged to happen. On the Internet, intermittent connectivity basesdamage of data, whereas DTNs sequester delay by means of a store-and-forward technique.

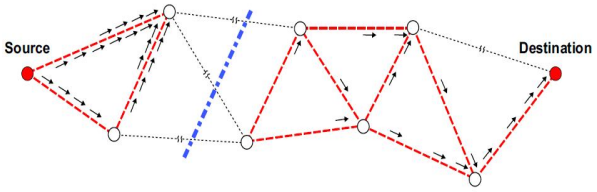

Fig.2. Intermittent connectivity (network partition)

Opportunistic Contacts

Network nodes mightessential to communicate during opportunistic contacts, in which a sender and receiver make contact at an unscheduled time.

Scheduled Contacts

Scheduled contacts may involve message-sending between nodes that are not in direct contact. They may also involve storing information until it can be forwarded, or up to the receiving application can catch up with the sender's data rate. Scheduled contacts entail time-synchronization throughout the DTN.

III. RELATED WORK

Disruption-tolerant networks (DTNs) provide communication in scenarios that challenge traditional mobile network solutions. DTNs use the inherent mobility of the network to deliver messages in the face of sparse deployments, highly mobile systems, and intermittent power. DTN routing differs from previous networking paradigms by assuming that connectivity will be fickle and poor, so information must be opportunistically routed towardthe final destination. In addition to those challenges, malicious adversaries may threaten connectivity in a DTN by inserting, flooding, corrupting, and dropping messages. In traditional, infrastructure based networks and MANETS, security is often provided by restricting participation to a specific set of authorized nodes, enforced with cryptographic keys and identity management. In such a system, an administrator certifies all nodes in the network and participants will only route messages through other authorized nodes.

IV. PROPOSEDSYSTEM

Proposed system consists of a packet dropping detection scheme and a routing misbehavior mitigation scheme. Fig. 3 illustrates our basic approach for misbehavior detection. The misbehaving node [N1 in Fig. 1] is required to generate a communication report during each contact and report its previous communication reports to the contacted node [N2 and

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

N3 in Fig. 3]. Based on the reported communication reports, the contacted node detects if the misbehaving node has dropped packets. The misbehaving node may misreport to hide its misbehavior, but fictitious records cause conflicts which make misreporting detectable.

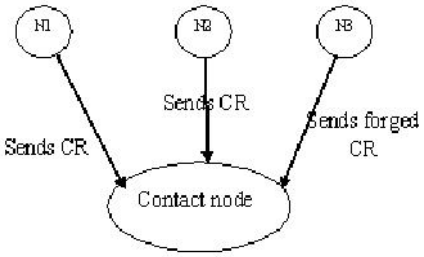

Fig.3. Packet dropping detection misbehaving node reports fictitious communication report which is inconsistence.

To detect misreporting, the contact node collects the communication report. It finds out which node has dropped the packets. It reduces the data traffic that flows into misbehaving nodes in two ways: 1) If a misbehaving node misquotes, it will be boycotted and will not get any packet from other nodes; 2) if it reports its communication reports honestly, its dropping behavior can be monitored by its contacted nodes, and it will obtain much fewer packets from them.

V. SYSTEM ARCHITECTURE

The source sends data to the destination through the intermediate nodes. The intermediate node is acting selfish and misbehaves by dropping packets and it misreports it to the contact node. The contact node detects that node 3 has dropped packets and it sends the packet through node 4 to the destination. The contact node plays a vital role here in detecting the misbehaving node. Destination node on receiving the data sends the contact node an ack to intimate the receipt of data.

In Fig 4 (a) Node n misbehaves and drops packet that it receives from intermediate node. Node behaves selfish as it is unwilling to spend its resources to forward packets of other node. This moderates the packet delivery ratio and wastes system resources. The source on receiving requests provides response to the client. Source forwards packet to node 1, which in turn forwards the packet to the next intermediate nodes, Source and intermediate nodes send CR to the contact node. This CR is used by the contact node to detect misbehaving nodes that drop packets. Node n misbehaves and it drops packet.

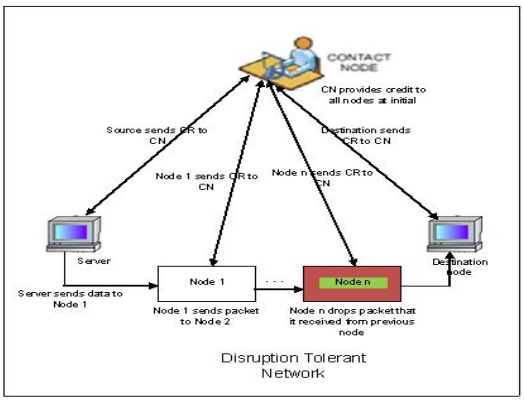

Fig. 4(a). System architecture with misbehaving node

In Fig 4 (b) Node n which misbehaved is now renovated to legitimate node. The contact node detects it and renovates to legitimate node. The contact node detects that node n has dropped packets using the CR. It provides credit to all

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014

nodes at the beginning. When a node misbehaves its credit value is decreased by CN. When a request is received from a client, its credit value is checked. If it's below a threshold value service to that client is rejected. In order to get service each node should maintain its credit value. Thus misbehaving node behaves as legitimate node and forwards data to the destination or next intermediate nodes.

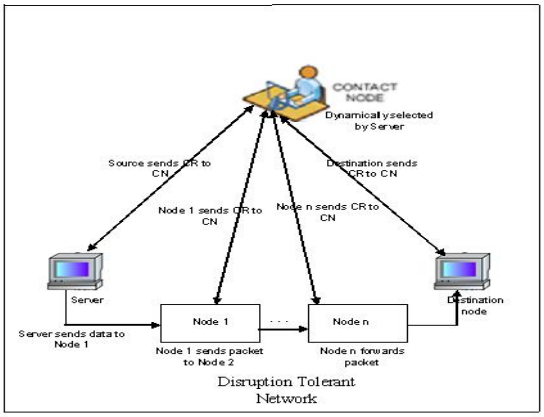

Fig. 4(b) .System architecture with misbehaving node renovated to legitimate node

VI. CONCLUSION AND FUTURE ENHANCEMENT

In this paper, I propose system which will consist of a packet dropping detection scheme and a routing misbehavior mitigation scheme. The detection scheme works in a disseminatedapproach; i.e., every node detects packet dropping nearby based on the collected information. Besides, the detection scheme can commendably detect misreporting even when some nodes conspire. Systematic results on detection probability and detection delay were also obtainable. Grounded on our packet dropping detection scheme, we then proposed a scheme to mitigate routing misbehavior in DTNs. The proposed scheme is very generic and it does not rely on any specific routing algorithm.

The further enhancement can be done by providing security to the contact node .This avoids the contact node being compromised by malicious node to avoid being detected. In future work, I am going to introduce a probabilistic misbehavior detection scheme by adopting the inspection game and also going to propose iTrust scheme for misbehavior detection in DTN.

REFERENCES

[1]RFC4838 2007 Delay-Tolerant Networking Architecture
[2]Warthman, F. 2003 Tutorial. Delay-Tolerant Networks (DTNs)
[3] Ms.Aarthy D.K., Mr.C.Balakrishnan ," Detecting Selfish Routing and Misbehavior of Malicious Node in Disruption Tolerant Networks"Volume 3, Special Issue 1, January 2013
[4] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.
[5] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks", in Proc. ACM MobiCom, 2000, pp.255-265.
[6] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012
[7] Delay Tolerant Networking Research Group http://www.dtnrg.org/wiki/Docs

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 11, November 2014