International Journal of Research Studies in Science, Engineering and Technology
Volume 2, Issue 9, September 2015, PP 23-29
ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

Cooperative Caching in Disruption Tolerant Networks with Security

Nimmy Mary Rajan
P.G. Scholar, Dept. of ECE
Sree Buddha College of Engineering for Women
Pathanamthitta, India
nimmymaryrajan@gmail.com

Jisha Anu Jose
Assistant Professor, Dept. of ECE
Sree Buddha College of Engineering for Women
Pathanamthitta, India
jishaanujose@gmail.com

Abstract: *Disruption Tolerant Networks (DTNs) are considered to be a successful solution to allow communication between nodes in extreme networking environments. Cooperative caching is one of the best methods of data access in such conditions. One of the major challenges in this scenario is secure and efficient data transfer between nodes. Due to random nature of DTNs, harmful intruders can launch attacks, which may cause misrouting, drop or alteration of packets. Thus, it is imperative to detect such intruders and respond to these intruders in a timely and effective way. The traditional security mechanisms mainly focus on intrusion detection capability only. Incorporating a firewall based intrusion response scheme called smart intrusion blocker, along with the conventional detection method will reduce the complexity of overall security system. This response scheme can create a quick virtual barrier between the data nodes and the intruder, which blocks further communication with the intruder nodes.*

Keywords: *Disruption Tolerant Networks (DTNs), cooperative caching, intrusion detection, intrusion response*.

1. INTRODUCTION

Disruption Tolerant Networks (DTN) opens a new level of communication in adverse networking conditions. A customary internet like network assumes an end to end path between nodes for transferring data. But such a path or connectivity may not be available always. For example in space communication, the satellites or other data processing nodes are not always in range so that data transfer can occur rapidly. Disruption tolerant networks play a vital role in such a scenario. These networks are generally featured by their unpredictable node mobility and unstable network topology.

Since the contacts among nodes are opportunistic, it uses a store and forward mechanism for data access. It means that, nodes which receive data must be able to store them until they are ready to safely forward it to the next node in the network. DTNs can accommodate many kinds of wireless technologies, such as radio frequency, free-space optical, ultra-wide band, and acoustic (sonar or ultrasonic) technologies.

The most widespread notion of DTN is its custody transfer ability which enables communication in intermittently connected networks. A basic query is how to deliver the data securely to the destination. Different data accessing and forwarding schemes are available for DTNs, but which one is the best fit for routing depends on the characteristics of the network components. It is clear that traditional routing schemes cannot be adopted for DTNs because of its unstable nature. In [1], [2], and [3] some forwarding schemes have been presented, but they did not lay out efficient data access to mobile nodes. Caching is a prevalent technique used to improve the data access performance. The existing caching scheme can be upgraded by incorporating cooperative caching mechanism.

Cooperative caching has been widely adopted in both wired and wireless networks to enhance the performance of data access. In [4] cooperative caching based data accessing mechanism is demonstrated. In this scheme data is cached at some easily accessible nodes. This set of nodes is called as Network Central Location (NCL). Each NCL has a central node and this central node has the highest priority of caching the data. Since the central node has limited caching buffer, other nodes nearer to the central node may be involved in caching. Proper NCL selection, periodic cache replacement, selection of new NCL in case of central node failures, etc., are important steps involved in this scheme.

In recent years, several researches have been made on improving the performance of disruption tolerant networks. DTNs are more vulnerable to security attacks due to i) unpredictable location of mobile nodes; ii) lack of persistent network connectivity. Although cooperative caching improves the performance of DTN in terms of data accessing, chances of attacks by intruders still remain. These attacks cannot be negotiated because it can cause enormous data loss. Hence while designing a DTN; one should consider the security side also.

This paper investigates existing cooperative caching based data transfer mechanism in DTN and inspects the security issues in it. Then, proposes a security scheme to make the network safe and reliable. The main contributions of this work include 1) modeling a disruption tolerant network which uses cooperative caching as its data access scheme; 2) analyzing the effect of intruder nodes in this DTN model; 3) incorporate an intrusion detection system; 4) propose an efficient intrusion response scheme. The proposed intrusion response scheme is designed based on firewall, which effectively blocks the intruders.

The rest of the paper is organized as follows. Section 2 provides an infrastructure for efficient data access in DTNs. Section 3 describes the security issues in DTNs. Section 4 explains an effective security mechanism called smart intrusion blocker. Details of the simulation and obtained results are presented in section 5. Finally, the paper is concluded in section 6.

2. INFRASTRUCTURE FOR EFFICIENT DATA ACCESS IN DTN

One of the most widely accepted data accessing technique in disruption tolerant network is cooperative caching scheme [4]. The main reason for the extensive popularity of this method is its efficient utilization of available resources in mobile nodes [5], [6]. The important concern of this schema is creation of Network Central Location or NCL.

2.1. Selecting NCL

NCL can be defined as a set of nodes which can be easily accessed by other nodes in the network. Each NCL has a central node which has the highest priority of caching the data. The central node is selected based on a NCL selection metric, which is given by,

$$C_i = \frac{1}{|V \setminus \mathbb{N}_C|} \sum_{j \in V \setminus \mathbb{N}_C} p_{ij}(T) \quad (1)$$

In this equation, V indicates the nodes and N_C is the set of selected central nodes (initially, N_C will be a null set). $V \setminus N_C$ ensures exclusion of current central nodes while selecting new ones. Term p_{ij} (T) is the weight of shortest opportunistic path between i and j within the time T. Let K be the required number of NCLs.

Caching of data involves mainly four steps:

- Calculate C_i for all nodes in the network.
- Choose K central nodes with highest C_i value.
- Cache the newly generated data at central nodes of NCLs.
- If buffer of central node is full, data are cached at another node nearer to central nodes.

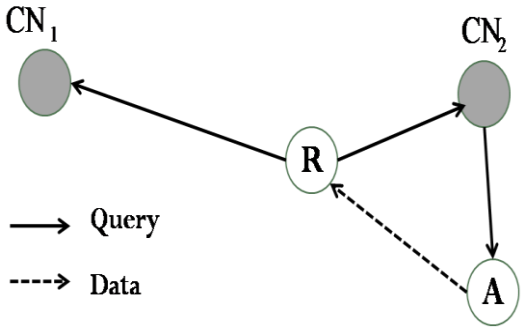

Fig1. *Accessing data from the NCLs*

Figure 1. Shows a requester accessing cached data from the central node. Here CN_1 and CN_2 are two central nodes. R is the requester. Buffer of CN_2 is assumed to be full and hence node A is responsible for caching the excess data. R multicasts a query to the two central nodes. Which CN should respond to the query depends on the distance between the requester and the CNs, which is determined probabilistically. From the figure it is clear that CN_2 is the nearby central node. Since data actually resides in A, A will respond when it receives a query from CN_2.

2.2. Cache Replacement

Data cached at particular nodes should be replaced so that available buffer space can be reused for new data. For that, a probabilistic cache replacement strategy is used which replaces least used data. It also limits number of cached copies of a particular data, since excess copies of same data are unnecessary. The cache replacement strategy makes use of the query history maintained by the caching nodes at NCLs.

2.3. Selection of New Central Nodes

The main components in a caching based data accessing scheme are central nodes. Any damage to these central nodes may cause loss of cached data and may result in poor data access performance. So a new central node should be selected when the current one fails. The new central node should be the node with higher NCL selection metric. It should also be noted that the newly selected central node is not too far from the previous one.

3. SECURITY ISSUES IN DTN

Even though disruption tolerant networks are well noted for their performance in adverse conditions, some security attacks can degrade its performance. Nodes in this network have limited resources such as reduced battery life, limited caching buffer, etc. Hence, any attacks that attempt to exhaust the network resources may cause permanent damage of the network. Since DTN is infrastructure less, an intruder can easily enter the network and can participate in routing protocols. Thus, it can launch severe attacks such as dropping or misrouting of packets, changing the contents of a packet, flooding the network with unnecessary information so that the authorized users cannot access the services, and so on.

Hence the main requirements of a security framework for DTN are: 1) attacks from both inside and outside malicious nodes must be ceased 2) overhead of implementing the security scheme must be minimized. It is more crucial to meet these requirements because DTNs do not have a stable topology [7].

4. SMART INTRUSION BLOCKER

DTNs are more vulnerable to security threats. Hence a proper security mechanism should be adopted in this network so as to keep it safe. In this section, we describe a smart tracking firewall [8] based intrusion blocking scheme, called smart intrusion blocker. It incorporates an intrusion detection and intrusion response techniques [9]. This scheme effectively tracks intruders and constantly blocks attacks from such nodes.

Before moving into the actual procedure, consider the following points:

- At each node i, an intrusion detection scheme is enabled by utilizing key verification technique, which can detect unauthorized accesses.
- Each node i in the network maintains a blacklist and a greylist. Blacklist consists of nodes which are detected as malicious by i itself, and greylist includes set of malicious nodes detected by the neighbors of i. It means that, the nodes in the greylist are not within the direct communication range of i.
- Node i always blocks communication with nodes in the blacklist of i. It also blocks communication with nodes in the greylist when they come in range.

4.1. Procedure

- When a node detects attacks from a malicious node, it blocks communication with that node, and adds that attacker in its blacklist. Further, it reports about this attacker to the neighboring nodes during their opportunistic contacts. These neighboring nodes will record the attacker in their greylist. All nodes which have attacker in their greylist will form a warning zone.
- Similarly, when the central node receives the report on the attacker, it also enters the attacker in its greylist. We consider the central node as a decision node, because it decides whether an intruder shall be registered into the blacklist. So when a central node receives a report on the attacker from a certain number of nodes (i.e., a threshold value), it moves the attacker from greylist to blacklist and blocks further communication with it.
- This blacklist information is then broadcasted from central node to all other nodes, which are in contact range of this central node. Since the central node is the one which is easily accessible to all other nodes, this broadcast report can reach almost all nodes in the network. Nodes which didn't get this broadcast message will learn about the attacker, during their opportunistic contact with other nodes. So the nodes with attacker in their blacklist will form a safe zone, as the communication with the attacker is blocked in this region.

5. SIMULATION RESULTS

In this section we study the performance of smart intrusion blocker. Simulations are performed using NS-2. The model is composed in a 500m x 500m development area, where 37 nodes are randomly deployed. All nodes in the network are mobile and we use CBR connections between source-destination pairs. The source and destination are chosen randomly. The buffer size of each node is set to 600 messages. An intruder is generated which launches attacks at 25 s after simulation starts. This intruder node is also mobile and it moves randomly in the network area.

The metrics used for evaluating the performance of the system include (a) packet delivery ratio, which indicates the percentage of the transmitted data packets that are successfully received (b) throughput, which gives the amount of data transmitted from the source to the destination in a unit period of time (second), and (c) packet drop.

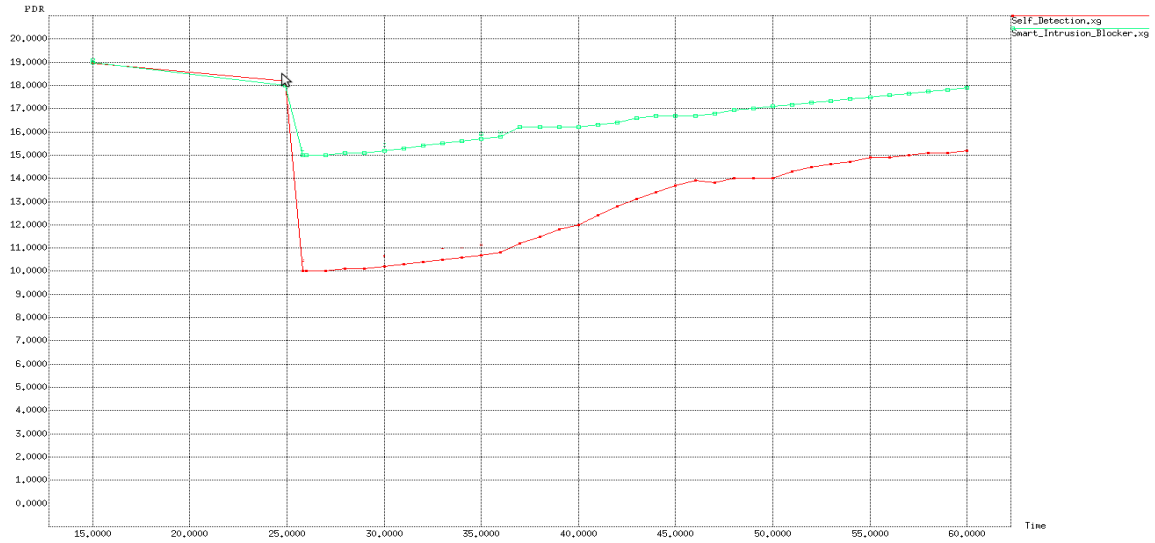

Fig2. *Packet delivery ratio under two different scenarios*

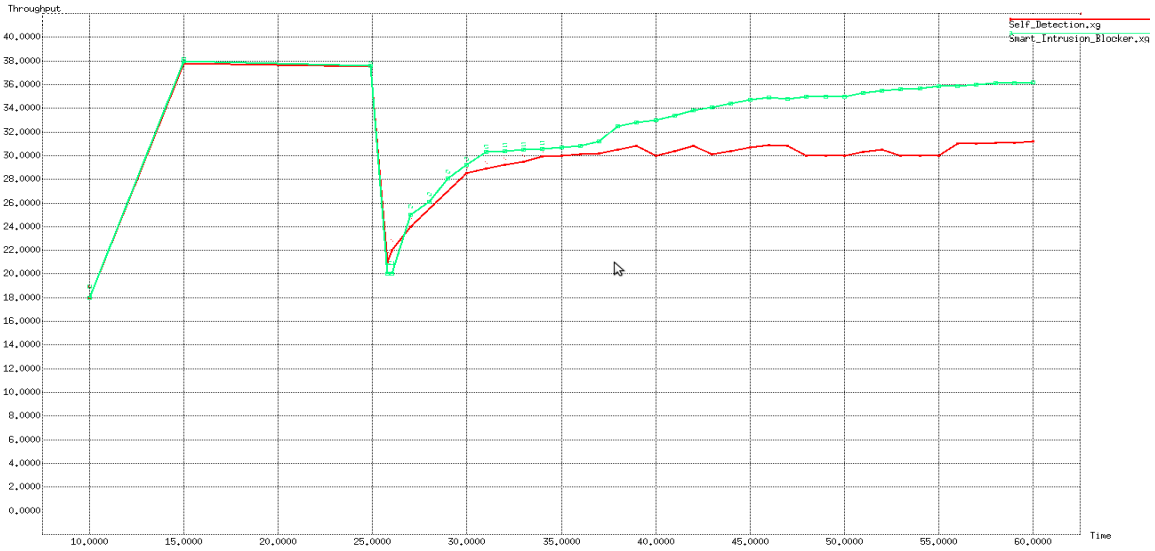

Fig3. *Throughput under two different scenarios*

In order to justify the effectiveness of the proposed system, we consider two cases. First one is, DTN security model with self detection, in which each node performs intrusion detection independently, and they do not implement a smart blocking. i.e., when a node detects an intruder, it blocks the attacks individually. Second one is the security model which executes smart intrusion blocking. The experimental results of both cases, in terms of packet delivery ratio, throughput, and packet drop are shown in Figures. 2, 3, and 4 respectively. The intruder launches attacks at 25 s, and hence the network performance degrades at this point. In the case of self detection, each node individually detects and responds to the intruders and hence it takes more time to safeguard against attackers. But smart intrusion blocking efficiently tracks the attacker and blocks it quickly and constantly. Hence the network can regain its normal performance within a short duration.

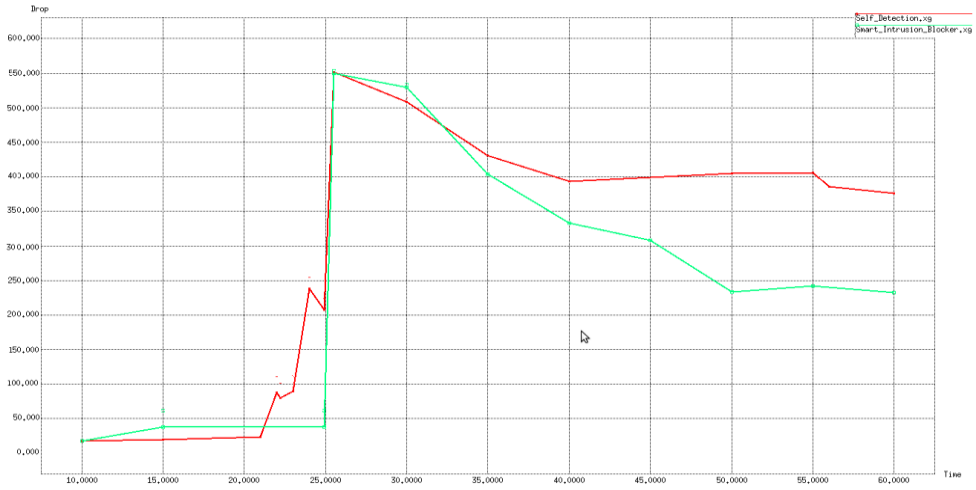

Fig4. *Packet drop under two different scenarios*

6. CONCLUSION

In this paper, a disruption tolerant network which supports cooperative caching is modeled. The security issues on this framework is then analyzed and presented a security scheme called smart intrusion blocker to deal with attacks launched by intruders. This scheme is actually developed based on traditional firewall mechanism. The simulation results verified the responsiveness of smart intrusion blocker in preventing the hackers.

The proposed security scheme includes both intrusion detection and intrusion response mechanisms. Potency of response scheme depends on how efficiently an intruder is detected. So in future, further investigation can be made to find more befitting intrusion detection techniques.

ACKNOWLEDGEMENT

This study was supported by the Department of Electronics and Communication Engineering, Sree Buddha College of Engineering for Women, Pathanamthitta, Kerala. I would like to express my gratitude to my guide, coordinator and my friends whose expertise, understanding, and patience, added considerably to my post graduate experience.

REFERENCES

[1] T. Spyropoulos, K. Psounis, and C. Raghavendra, ”Spray and Wait: An efficient routing scheme for intermittently connected mobile networks,” Proc. ACM SIGCOMM Workshop delay-tolerant networking, pp. 252- 259, 2005.

[2] Q. Yuan, I. Cardei and JieWu, ”Predict and Relay: An efficient routing in Disruption Tolerant Networks,” Proceedings of the Tenth ACM International Symposium on Mobile Ad hoc Networking and Computing, ACM, 2009.

[3] P. Costa, C. Mascolo, M. Musolesi, and G. Picco, ”Socially-aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks” IEEE J. Selected Areas in Comm., vol. 26, no. 5, pp. 748-760, June 2008.

[4] Wei Gao; Guohong Cao; Iyengar, A.; Srivatsa, M., ”Cooperative caching for efficient data access in disruption tolerant networks,” IEEE Trans. Mobile Computing, vol. 13, no. 3, pp. 611-625, March 2014.

[5] L. Yin and G. Cao,”Supporting cooperative caching in ad hoc networks,” IEEE Trans. Mobile Computing, vol. 5, no. 1, pp. 77-89, Jan. 2006.

[6] W. Zhang, L. Yin, and G. Cao, ”Secure cooperative cache based data access in ad hoc networks,” NSF International Workshop on Theoretical and Algorithmic Aspects of Wireless Ad Hoc, Sensor, and Peer-to-Peer Networks, pp. 11-16, 2004.

[7] J. Hur and K. Kang,"Secure data retrieval for decentralized disruption tolerant military networks," IEEE/ACM Transactions on Networking, vol. 22, no. 1, February 2014.

[8] X. Wang and Ping Yi, "Security framework for wireless communications in smart distribution grid," IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 809-818, Dec. 2011.

[9] Zhang, Yongguang, Wenke Lee, and Yi-An Huang, "Intrusion detection techniques for mobile wireless networks," Wireless Networks 9, no. 5 (2003): 545-556.

AUTHORS' BIOGRAPHY

Nimmy Mary Rajan received the B. Tech degree in Electronics and Communication Engineering in the year of 2013 and currently pursuing M. Tech in Communication Engineering at Sree Buddha College of Engineering for Women, Kerala, India. Her research interests include the areas of computer networking, and wireless sensor networks.

Jisha Anu Jose has 3 years of experience in teaching in India. She is currently an Assistant Professor in the Department of Electronics and Communication at Sree Buddha College of Engineering for Women, Kerala, India. Her research interests include the areas of image processing, wireless sensor networks, and computer networking, with several publications in refereed journals and conference proceedings.