Secured Routing in DTNs: Threats & Counter-measures

Sujoy Saha[1], Satadal Sengupta[2], Subrata Nandi[3]
PhD Student[1], Undergraduate Student[2], Assistant Professor[3]
Dept. of Computer Science & Engineering
National Institute of Technology, Durgapur, India-713209
{sujoy.ju, satadal.sengupta.nit, subrata.nandi}@gmail.com

Abstract. Our work deals with the aspect of secured routing in Delay Tolerant Networks. DTNs depend entirely on the honesty and integrity of individual nodes for performance as well as data security. Therefore, security is of utmost concern when it comes to DTN routing. However, although there has been appreciable advancement on routing in DTN, security has seen limited work globally. In this technical write-up, we present a concise description of the work done so far by us on this field and results achieved, as well as indications for future study.

1 Introduction

The concept of Disruption Tolerant Network (DTN) was introduced to combat problems of high node mobility, low node density & short radio ranges. These networks use store-forward approach to deal with challenging networking scenarios, e.g., sparse node density, battlefield situations, deep-space communication, etc. However, it is a challenging task to verify the integrity & trustworthiness of transmitted information, due to network constraints, thus rendering them vulnerable to attacks & compromises.

In this paper, we present the motivation for our pursuing this area of research. Next we present the status of our work so far by describing the proposed algorithm and corresponding results obtained. Finally, we conclude the paper and indicate important areas for future research.

2 Motivation

Control in a DTN is distributed amongst individual nodes, and therefore integrity of information transmitted relies entirely on the trustworthiness of each node in the network. Therefore, compared to any infrastructure-based network, a DTN is more susceptible to malicious activities arising from foreign intrusion and/or insider attacks. As such, study of the effect of various types of malicious activities on the performance as well as integrity of a DTN is relevant as well as important. However, research on *Secured Routing in DTNs* is confined to few research groups globally. To the best of our knowledge, 3 schemes have been proposed till date with the aim of detecting malicious nodes in a DTN. A ferry based detection method FBIDM [1] was first introduced. The strategy was to detect malicious nodes by employing a trusted examiner - a ferry node. It was improved upon by a scheme known as MUTON [2] which uses mutual correlation values. Later on, a detection scheme using packet exchange recording [3] was proposed. All these schemes are based on the PRoPHET [4] routing protocol. Certain key security issues were addressed and schemes suggested in [5].

In most practical cases of DTN implementation, where there are hardly any periodicity in node mobility, the *Spray & Focus* [6] routing protocol works better than the *PRoPHET* protocol. Consequently, we have chosen this protocol and have effected certain algorithmic modifications in it to ensure that *Spray & Focus* routing is secure and free of malice. According to the best of our knowledge, this is the first such attempt at making this specific protocol secure. In a broad sense, the importance of ensuring security in a challenged networking environment, as well as the limited amount of research performed so far in this field, form the motivation for our research work.

3 Status of Our Work

We have conducted an elaborate survey on the types of malicious activities that can take place in a DTN environment. The types that have been identified are: eavesdropping, trespassing, circumstantial denial of service, lack of integrity, individual selfishness, denial-of-service attacks under influence of foreign force, false report of presence, false report of absence, misdirection of traffic, exploitation of node maintenance feature, foiling of malicious activities, incorrect detection, deliberate alteration & redundancy.

As stated earlier, we have chosen the *Spray & Focus* routing protocol and effected certain algorithmic modifications in it to facilitate detection and elimination of malicious nodes.

Algorithm: We propose a table based scheme where each node maintains a table with entries corresponding to each encounter in the network. We call this table the *Network Records Table (NRT)*. Additionally, each node stores a *Malice Identification List (MIL)* which stores the node IDs of all those nodes which have been found to be malicious. Whenever two nodes (say A & B) encounter each other, they perform the following actions, in the specified order:

1. Node A checks its *Malice Identification List* to see if node ID of B is present in it. Node B performs the same MIL check for A. If any of the two nodes test positive, no further interaction takes place. If both test negative, they move on to the next step.
2. Node A and node B exchange their respective *Network Records Tables*.
3. Node A performs a *Maliciousness Test* on node B by matching its own *NRT* entry by entry with that of node B. Node B does the same for node A.
4. If one of the nodes (say, node A) finds the other node (node B) to have engaged in malicious behavior, then A appends the node ID of B to its MIL. No further interaction takes place under this circumstance.
5. If each node passes *Maliciousness Test* performed by the other node, they update their *Network Record Tables* by inserting entries corresponding to latest information about the network. So, the entries in the NRT of A which are not present in NRT of B, are inserted into NRT of B and vice versa.
6. Also, the nodes exchange and update their *Malice Identification List* in the same way that they do in case of the $NRTs$ in order to have the latest information about detected nodes.
7. Finally, they will exchange messages according to the $Spray$&$Focus$ protocol and then generate and exchange corresponding entries to be stored in their respective $NRTs$.

For our scheme, we shall consider the Black Hole Denial-of-Service (DoS) attack, i.e., the malicious nodes will drop all packets they receive. Each such node will, therefore, participate in the routing of the message but is not going to forward the packet any further. The malicious nodes are divided into *Spray Malicious* and *Focus Malicious*. The first type only drop packets while the latter declare attractive metrics to suck packets from the network and then drop those.

Simulation Results: We have performed simulations using the *ONE simulator* (www.netlab.tkk.fi/ tutkimus/dtn/theone) by customizing the code of *Spray & Focus* protocol to suit our detection methodology. Corresponding details have been provided below.

***Setup*:** In our simulation setup, we used the following setup: Simulation area = 4500m X 4500m, movement: customized *Cluster Mobility Model*, no. of clusters = 6, no. of nodes = 156, transmission range = 10m, packet size = 50KB to 1MB, transmission speed = 250KBps, buffer size = 500MB, simulation time = 86,400s. Scenarios considered: (1) Percentage of malicious nodes varied among 10%, 20%, 30% & 40% of the total no. of nodes; (2) Total no. of nodes varied among 94, 110, 124, 140, & 156 nodes. In each case, an appropriate number of nodes have been made to behave as malicious, half of which are *spray malicious* while the rest are *focus malicious*.

***Metrics Observed*:** We have studied various metrics to ascertain the performance of our detection mechanism: *average number of detections*, *total delivery probability*, & *cumulative delivery probability*.

***Results*:** The results & corresponding analysis follow:

Efficiency: Fig. 1 presents the graph obtained by plotting average number of detections against time in seconds. We have plotted values obtained against all four cases, i.e., 10%, 20%, 30% & 40% malicious nodes respectively out of the 156 nodes. From the graph, we can conclude that the detection algorithm works effectively as it detects all malicious nodes in the network if allowed to run for sufficient simulation time. As expected, the more the number of malicious nodes in the network, more is the time required to detect & eliminate all of them from the network. It is also noteworthy that detections occur very quickly when the simulation time is at lesser values, whereas as higher values of time, detection slows down. Detection in NRT anomalies is easier initially when network is less congested compared to later.

Impact on Delivery Probability: Fig. 2 depicts the impact of malicious activity in the network & its subsequent detection & elimination from the network on the metric of cumulative delivery probability. Cumulative delivery probability starts from a low value & remains so for some initial thousands of seconds. This is the initial phase of the network where delivery probability suffers a setback due to packets being dropped by malicious nodes throughout the network. However, with the detection algorithm in place, the malicious nodes get gradually eliminated & hence there is a steady increase in the delivery probability. This is the second phase where the network is slowly recovering from previous message drops & hence the graph shows a steady increase at a decreasing rate. However, this increase in delivery probability does not carry on beyond a certain point in time. Beyond this, the graph becomes almost parallel to the horizontal axis. This is the third phase of the graph where the network has entered its steady state,

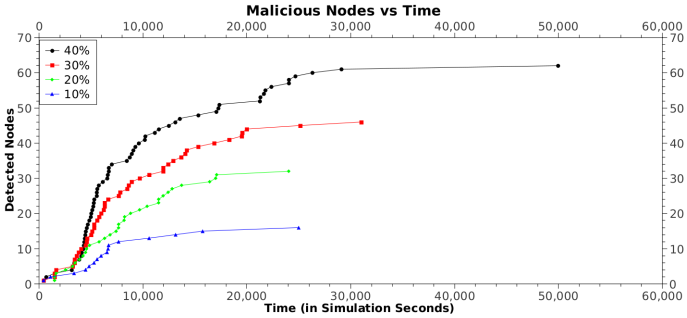

Fig. 1. Average Number of Detections v/s Time

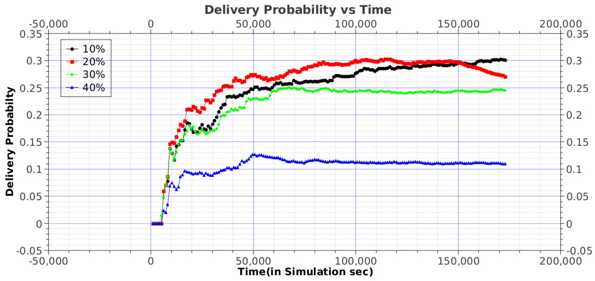

Fig. 2. Cumulative Delivery Prob. v/s Time

& the delivery probability has become virtually constant. This phase shall continue till the end of simulation time is reached.

Comparision between Normal Scenario & Maliciousness Inclusive Scenario: Fig. 3 focuses on a comparative study between equivalent malicious & non-malicious scenarios. It is easy to notice that in the normal scenario cases, delivery probability increases from 156 to 94 consistently, except the 110 case which yields maximum value. This is perhaps owing to the fact that the network consisting of 110 nodes is neither too sparse, nor too dense to drop too many messages.

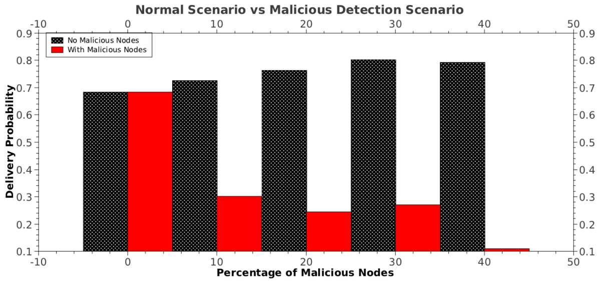

Fig. 3. Delivery Prob. v/s Percentage of Malicious Nodes

4 Conclusion & Future Work

In our work so far, we have performed a detailed survey of various types of malicious attacks possible in a DTN environment & have taken a look at detection schemes. We have proposed a modified *Spray & Focus* routing scheme, for detection of malicious nodes in the network. The intricacies of the mechanism have been studied in detail & described in brief in this write-up. Simulations using ONE simulator show us that the proposed scheme is effective in detecting malicious nodes & thereby ensures that they take no further part in the routing process. Furthermore, we have carried on our research in this field & we intend to look into certain other aspects with regards to performance analysis of our strategy as well in the recent future, one of them being the latency involved in informing all nodes in the network about the detection of a node. An important aspect of our srategy where we feel we should improve is the overhead incurred due to execution of a detection algorithm each time 2 nodes encounter. We believe that one way to reduce such high overheads is to introduce a special detection permission in a certain percentage of the nodes, instead of all, i.e., only certain trusted nodes in the network would have the ability to execute the detection algorithm as & when they encounter another node in the network. We are analyzying the effect of such a modification on the performance of our scheme & hope to come up with results in the recent future.

References

1. M.Chuah, et. al., *A Ferry based Intrusion Detection Scheme for Sparsely Connected Ad Hoc Networks*, in Proc. MOBIQUITOUS, August, 2007.
2. Y.Ren, et. al., *MUTON: Detecting Malicious Nodes in Disruption-Tolerant Networks*, in Proc. IEEE Wireless Communications & Networking Conference (WCNC), 2010.
3. Y.Ren, et. al., *Detecting Blackhole Attacks in Disruption-Tolerant Networks through Packet Exchange Recording*, in Proc. IEEE Int'l Symp. on World of Wireless, Mobile & Multimedia Networks, 2010.
4. A.Lindgreny et. al., *Probabilistic Routing in Intermittently Connected Networks*, in Proc. ACM SIGMOBILE Mobile Computing & Communications Review, Vol. 7, July 2003.
5. H. Zhu, *Security in Delay Tolerant Networks*, Thesis paper presented in Univ. of Waterloo, Canada, 2009.
6. T.Spyropoulos et. al., *Spray & Focus: Efficient Mobility-Assisted Routing For Heterogeneous & Correlated Mobility*, in Proc. Fifth IEEE Int'l Conf. on Pervasive Computing & Communications Workshops, 2007.