Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Identification, Detection, Elimination of Selfish & Malicious Nodes with Buffer Level Monitoring For Secured Data Communication In DTN

Dr.C.Nalini, Aakansha, Abhilasha
Department of Computer Science and Engineering ,
Bharath University, India

Abstract— Delay Tolerant Networks (DTNs) face extremely lengthwise latency, frequent disconnection while communicating. The drawback in existing system is that no energy level is maintained within the network. Moreover there was a packet loss between the networks once the node attempt to transfer the information. In this paper we detect stingy & Malicious Nodes as well as we observe buffer level of every node to spot packet loss for secured information transfer. Stingy Nodes are harmless however it'll transmit/receive information to and from their friends list. Malicious Nodes are the ones that drop or add additional packets once they are attacked. We are using RSA algorithm to perform encryption and decryption of the messages transferred.

Keywords— Delay Tolerant Network (DTN), Selfish, Malicious, Nodes, RSA algorithm.

I. INTRODUCTION

A Delay Tolerant NETWORK (DTNs) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. DTNs comprises mobile nodes (e.g., humans in a social DTNs) experiencing distributed connection, opportunistic communication, and frequently changing network topology. Because of lack of lengthy connectivity, routing in DTNs adopts a store carry- and-forward scheme by which messages are forwarded through a number of intermediate nodes leveraging opportunistic encountering, hence resulting in higher lengthwise latency. In this paper, we propose dynamic trust management for DTNs to deal with both malicious and selfish misbehaving nodes etc.).

In this paper we have discussed about the related work, the proposed work, the architectural diagram, the modules present in the paper, the algorithm used to implement the idea and its application in the near future.

II. RELATED WORK

Paper [1] proposes a probabilistic routing protocol in intermittently connected networks wherever there's no guarantee that a totally connected path between supply and destination exist at any time, rendering ancient routing protocols unable to deliver messages between hosts.

Paper [2] proposes epidemic routing techniques to deliver messages in case where there is never a connected path from source to destination or once a network partition exists at the time a message is originated.

Paper [3] proposes an efficient approach termed as a Repetitive Trust Management (RTM) and adversary detection to handle the Byzantine attacks in DTNs.

Paper [4] takes into consider the reputation values among the nodes participated in the data transmission by presenting the Trust Based Management classifier.

Paper [5] proposes protocol for secure routing optimization in DTN environments in the presence of well-behaved, stingy and malicious nodes.

Paper [6] proposes calculation of trust values between every node to push confidence between cooperating nodes conjointly determining malicious nodes that may cause significant problems to such networks.

Paper [7] proposes a Social Stinginess Aware Routing (SSAR) rule to address user stinginess and supply smart routing performance in an economical manner.

Paper [8] proposes a sensible incentive protocol referred to as Pi, such that once a supply node sends a bundle message, it conjointly attaches some incentive on the bundle to encourage the node to forward the packet.

Paper [9] proposes forwarding choices based on collected information regarding node behaviour (e.g., past contacts between nodes) to predict future contact opportunities.

Paper [10] proposes a distributed theme to find packet dropping in DTNs. In this scheme, a node is required to keep a few signed contact records of the nodes it had previously contacted with, based on which the next contacted node can detect if the node has dropped any packet.

IV. SECURED DATA COMMUNICATION IN DTN

This paper proposes the monitoring of buffer level of every node in addition to identification and deletion of selfish and malicious nodes for secured data communication in Delayed Tolerant Network. It proposes to combine social trust

deriving from social networks and traditional Quality of Service (QOS) trust deriving from communication networks into a composite trust metric to assess the trust of a node in a DTN. To cope with both malicious and socially selfish nodes, considering "healthiness" and "unselfishness" as two social trust metrics. It is detecting Selfish & Malicious nodes so that an alternative best route is chose. Selfish nodes are harmless but it transmits/receives data from their friends list. Malicious node drops/ redirects packets once they are attacked. It monitors buffer level of every node to identify whether packet loss is due to incapability of the node or they are malicious. Incapability is considered as normal. Packets are encrypted using RSA algorithm.

V. ARCHITECTURE AND MODULES DETAILS

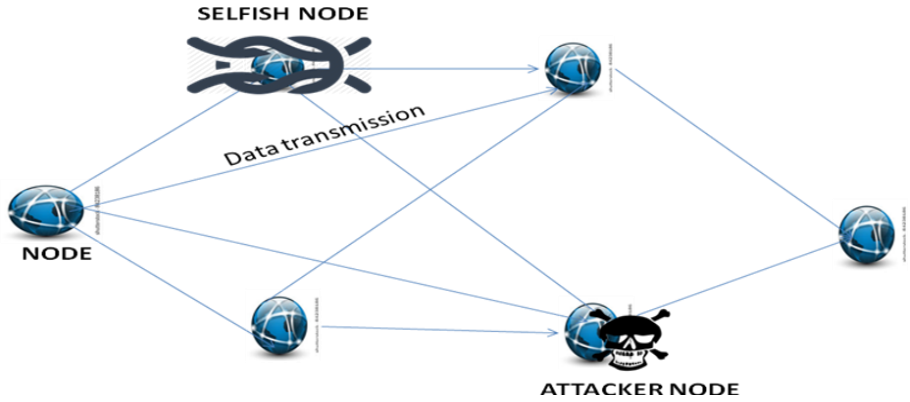

FIG 1: ***Presence of selfish & attacker node in a network***

Network Deployment:
To implement the thought, initial a network is made that consists of 'n' range of nodes. So nodes will request information from different nodes within the network. Multiple networks square measure created for our implementation. So these networks can have multiple nodes. For every node it's required to form a node frame that contains the node data, destination node field to transfer the information and therefore the browse button to transfer the information from node's directory.

Route/Path Construction:
In this the network can confirm the versatile path to transfer the information from the supply node to the destination node. There'll be several ways are going to be out there from supply node to the destination node. In order that the information are going to be transfer via the trail that has the best property in order that the information can reach the destination node in reliable manner.

Assaulter Node:
In the module its characteristic the attackers conferred within the network. If the node transmits or receives the information quite the mounted rate then it's thought-about that node as associate degree As assaulter node. Conjointly the node tries transmits the malicious content to the destination nodes we tend to conjointly known as associate degree assaulter node and send they're going to be eliminated from the network.

Ungenerous Node Activity:
In this module the discussion is regarding the ungenerous node that this sort of node perpetually sends the information to their neighbour nodes in order that the packet won't reach the destination and it'll tends to drop the packet. A result of the ungenerous nature and energy overwhelming nature, ungenerous nodes aren't willing to forward bundle for others while not decent reward.

Malicious Node Activity:
As associate degree individual, the malicious nodes at random drop others' bundles (black hole or gray hole attack), which frequently occur on the far side others' observation during a thin DTN, resulting in serious performance degradation.

Best Route Identification:
The best route is taken by the packet from source to destination. The malicious and selfish nodes are identified. The energy level and buffer level of each node is checked before forwarding a packet. Thus the packet is sent to the destination through several intermediate nodes by selecting the best route available.

VI. ALGORITHM

The RSA rule is employed for each public key encoding and digital signatures. It's the fore most wide used public key encoding rule. The premise of the safety of the RSA rule is that it's mathematically impossible to issue sufficiently giant integers. The RSA rule is believed to be secure if its keys have a

length of a minimum of 1024-bits.

Key Generation rule

1. Opt for any to terribly giant random prime integers: p and Q
2. Calculate n and φ (n): n = pq and φ(n) = (p-1)(q-1)
3. Opt for associate degree whole number e, one < e < φ(n) such that: gcd(e, φ(n)) = 1(where gcd suggests that greatest common denominator)
4. Compute d, one < d < φ(n) such that: erectile dysfunction ≡ one (mod φ(n))

• the public key's (n, e) and therefore the personal key's (n, d)
• the values of p, Q and φ(n) are personal
• e is that the public or encoding exponent
• d is that the personal or decipherment exponent

Encryption

The cipher text C is found by the equation ('C = American state mod n') wherever M is that the original message.

Decryption

The message M can be found form the cipher text C by the equation

'$M = C^d \bmod n$'.

EXAMPLE

This is an extremely simple example and would not be secure using primes so small, normally the primes p and q would be much larger.

1. Select the prime integers q=11, q=3.
2. n=pq=33; φ(n)=(p-1)(q-1)=20
3. Choose e=3
    - Check gcd(3,20)=1
4. Compute d=7
    - (3)d ≡ 1 (mod 20)

Therefore the public key is (n, e) = (33, 3) and the private key is (n, d) = (33, 7).

Now say we wanted to encrypt the message M=7

- $C = M^e \bmod n$
- $C = 7^3 \bmod 33$
- $C = 343 \bmod 33$
- $C = 13$

So now the cyphertext C has been found. The decryption of C is performed as follows.

- $M' = C^d \bmod n$
- $M' = 13^7 \bmod 33$
- $M' = 62{,}748{,}517 \bmod 33$
- $M' = 7$

After the message has been encrypted and decrypted the final message M' is the same as the original message M. A more practical way to use the algorithm is to convert the message to hexadecimal and perform the encryption and decryption steps on each octet individually.

VI. EXPERIMENTAL SETUP

Software requirement of this project includes JAVA JDK as front end and SQL server 2008 as backend while hardware requirements include Windows OS, RAM 512 Mb and Pentium IV processor. In this paper we define a source node and a destination node and some intermediate nodes through which a file is send to the destination node. All the nodes are set to have the same energy level and buffer level at the beginning. So initially when the file is sent it takes any of the intermediate paths available. But as the energy and buffer level is changed, the packet takes the best route available. Additionally the malicious nodes and selfish nodes are discovered and an alternate path is taken by the packet. .

Datasets defined:

We have a table named ‘Infotable’ in which we define the following columns:

Nodez data defines the name of any arbitrary node created.

IP defines the IP of the respective node.

Passcode defines the password that is used to send and receive the files between

In the second table named 'links' we have the following columns:

Node and Destnode which shows the nodes that are connected to each other.

VII. CONCLUSIONS

The aim of this paper is to ensure the optimization of communication in a Delayed Tolerant Network so that even small drop in data packets can be discovered and the packets travel in a route that is best for the packets. In a world with new technologies trending every day we can't ignore communication and thus there are several possible areas of research in the future in which our design can be utilised.

Acknowledgment

This Work Was Supported By Our Faculties At Bharath University.

REFERENCES

[1] A. Lindgren, A. Doria, and O. Schelen(2003) "Probabilistic Routing in intermittently Connected Networks ", vol.7, no. 3, pp. 19-20.

[2] A. Vahdat and D. Becker (2000) "Epidemic Routing for Partially Connected Ad Hoc Networks", Duke Univ.

[3] C.Ashok Baburaj, DR. K. Alagarsamy (2014) "Repetitive Trust Management and Adversary detection for Delay Tolerant Network ".

[4] E. Ayday, H. Lee, and F. Fekri(2010) "Trust Management and Adversary Detection for Delay Tolerant Networks ", pp. 1788-1793.

[5] Ing-Ray Chen,Fenye Bao, MoonJeong Chang, and Jin-Hee Cho(2014) "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing", VOL. 25, NO. 5.

[6] I. R. Chen and T.H. Hsi, "Performance Analysis of Admission Control Algorithms Based on Reward Optimization for Real-Time Multimedia Servers," Performance Evaluation, vol. 33, no. 2, pp. 89- 112, 1998.

[7] J.H. Cho, A. Swami, and I.R. Chen(2011) "A Survey on Trust Management for Mobile Ad Hoc Networks" ,vol. 13, no. 4, pp. 562-583, Fourth Quarter.

[8] M.K. Denko, T. Sun, and I. Woungang, "Trust Management in Ubiquitous Computing: A Bayesian Approach," Computer Comm., vol. 34, no. 3, pp. 398-406, 2011.

[9] Qinghua Li, Guohong Cao(2012) "Mitigating Routing Misbehaviour in Disruption Tolerant Networks", VOL. 7, NO. 2, APRIL 2012.

[10] Q. Li, S. Zhu and G. Cao(2010) "Routing in Socially Selfish Delay Tolerant Networks", Proc. IEEE INFOCOM, pp. 1-9, Mar. 2010.

