

# A Hybrid Approach for Misbehaviour Detection Based on Trust and Distance Management Scheme

S.Deepica<sup>1</sup> P.Brundha<sup>2</sup> N. Raja Priya<sup>3</sup>

<sup>1</sup>P.G Student <sup>2,3</sup>Assistant Professor

<sup>1,2,3</sup>Department of Computer Science & Engineering

<sup>1,2,3</sup>Francis Xavier Engineering College, India

**Abstract**— vulnerable nodes are the biggest threat in Disruption/Delay Tolerant Networks (DTN). The main objective of this paper is to find the vulnerable nodes. Vulnerable nodes means it may be act as Malicious or Selfish or Replica node. In this project the DTrust technique is used as misbehaviour detection scheme. The DTrust is offering a Trusted Authority (TA) to analyse the node's behaviour based on the collected claim evidences and the distance of each nodes. The malicious and selfish behaviours are detected based on the claim evidences. The replica node is found based on the distance of each node. From the distance we can identify the moving speed of each node. If the speed reaches the maximum threshold that node considered as the replica. The proposed method used in this project performs well than the other existing methods.

**Key words:** Trusted Authority; Delay Tolerant Network; Misbehaviour Detection Scheme; Vulnerable nodes

## I. INTRODUCTION

A DTN is a collection of sub networks. It is spread on top of the major purpose networks including the internet. DTNs maintain interoperability of alternative networks of taking long disruptions and delays between and within those networks, by converting between the communication protocols of those networks. In affording these functions, DTNs hold the mobility and finite power of growing wireless communication devices. DTNs have more diverse applications on globe, where disruption tolerance is the biggest commitment. The possible globe applications spread across the range of military, commercial, scientific and public service applications. The main aim of DTN is to have acceptable performance in the high delay/loss/disconnected environments. A DTN node is an entity with the bundle protocol agent spread on the secondary layer communication protocols. At any stage the specific node may act as a sender, receiver or mediator of bundles. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise. Trust management [1] is an ideal system that processes significant representations of social trust, normally to provide automated resulting process. Trust management [1] is an attractive management in applying the information security, and access control policies. In this view, actions are permitted if they express satisfactory authorizations, irrespective of their genuine individuality, unravelling symbolic illustration of trust from the genuine person. Node replication attack is the harmful attack in this section. Replication attack means that the affected nodes are positioned once more for further vulnerable deeds. So it is very important to judge the replica nodes and get well from the attack. Suppose any node cracks any of the protection values and is then below some attack". Such nodes show one or more of the subsequent deeds: Packet Drop- Just

absorbs or drops the data and does not transmit it. Energy weak- Sometimes a misbehaving node may misuse the energy by doing needless operations. Buffer run over- Actual updates cannot be stored further in a buffer when vulnerable node fills the buffer with false data. Malicious Node arriving- Without any verification a malicious node may get in to the network. Delay- A vulnerable node may intentionally delay the data transmit to it. Link smash- It means that a malicious node will block any two genuine nodes from sharing data. False Routing- A malicious node may transmit data in false routes to the valid nodes in order to get the data or to upset the operations. Node Not obtainable- An interloper can cut off the node from taking part in any action and it leads to produce delays when the sender node takes another substitute path. Stealing data- Any vulnerable node may steal the data like the content, position and progression numbers. By this the vulnerable node can employ the data for attacks. Session Capturing- A Vulnerable node may detain the communication session of two valid nodes to obtain the data from the nodes. A malicious node can act as the number of alternative ways.

## II. SYSTEM MODEL

The problem of finding misbehaving nodes in a network requires the efficient detection scheme which provides reduced transmission overhead. Suppose a node is under any attack means it braches any of the safety measures. Such nodes exhibit one or more of the behaviour. Some of the behaviours are packet drop, battery drained, delay, fake routing, stealing information and session capturing. Replication of nodes in the network is the most dangerous attack. According to replication attack in a network the infected nodes are situated once more. So for better security we have to find the best method to detect the replica nodes in the network. For that reason misbehaviour detection is greatly preferable to guarantee the secure DTN routing as well as the authorization of the trust among nodes in a network. Thus the proposed scheme is better in achieving perfect secure in DTN.

The DTrust [1] scheme is proposed in finding the misbehaving nodes in a network. This scheme is used for finding the selfish, malicious and replica nodes. Because the Malicious, Replica and selfish behaviours signify the severe hazard against routing in Delay tolerant networks (DTNs). This scheme is based on the location of nodes. Using claim generation and forwarding between all nodes we can get the exact location of each node. The fact is that for any reason an uncompromised node never moves at speeds in surplus of the system build speed. Speed is measured based on the time and claim location of a node.

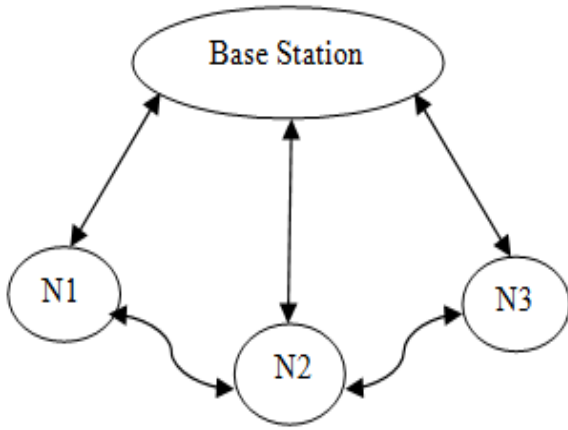


Fig. 1: Claim Generation and Forwarding

### III. IMPLEMENTATION

In this segment we are going to converse about the methods of the proposed system. DTrust has two important sections. First one is selfish, malicious node detection and the other one is replica node detection.

#### A. Node Initialization:

Consider a DTN shaped by certain nodes. Each node  $k$  is supposed to have a distinct nonzero identifier  $N_k$  and a equivalent private/public key pair. We interchangeably use node  $k$  and  $N_k$  here after.

#### B. Malicious and Selfish Node Detection:

Each node in a network is rational and a rational node's target is to benefit it is own profit. Because of the selfish character and energy absorbing, that nodes are not agreeable to transmit data for alternative nodes with no satisfactory benefits. Malicious nodes randomly drop others packets which often take place away from others surveillance, resulting to severe performance degradation. Here our base station acts as Trusted Authority [1]. The main work of TA is to monitor the network importantly the locations of all the nodes. By the claim generation and forwarding TA will get the locations of all nodes. As being selfish the selfish node will not send any claim to TA and the malicious nodes will send the claim lately. So by this TA will detect the particular selfish and malicious node.

#### C. Replica Node Detection:

The Trusted Authority validates the genuineness of the claim [2] with the public key and throw-outs the claim if it is not genuine. The base station (TA) collects the location information and time information from the claim. Let  $d_i$  denote the distance from location  $L_i$  at time  $T_i$ . Let  $O_i$  denote the measured speed at time  $T_i$  and  $V_{max}$  is the assigned maximum speed of a node in a particular network.  $O_i$  can be defined as

$$\text{Speed } (O_i) = \text{Distance} / \text{Time difference} \quad (3.1)$$

Let  $S_i$  denote a flag variable defined as

$$S_i = \begin{cases} 0, & \text{if } O_i \leq V_{max} \\ 1, & \text{if } O_i > V_{max} \end{cases} \quad (3.2)$$

Suppose for any node the variable  $S_i = 1$  means that particular node exceeds the maximum limit of the speed. So it's decided as replica node.

### IV. CONCLUSION

In this paper we have projected misbehaviour detection scheme (DTrust) for delay tolerant networks (DTNs). This scheme could decrease the detection overhead effectively. Our results sure that DTrust will reduce transmission overhead and increase the performance level of the nodes. Our future work will focus on the extension of DTrust to other types of networks.

### V. ACKNOWLEDGMENTS

My first sincere thanks to the lord almighty who has been with me throughout this project. As far as concerned to the management, my sincere thanks to Dr.D.C.Joy Winnie Wise ME., Ph.D., Professor and Head, Department of Computer Science and Engineering, Francis Xavier Engineering College. I also extend my gratitude to my guide Mrs. P.Brundha ME., Assistant Professor, Department of Computer Science and Engineering for her valuable guidance and support.

### REFERENCES

- [1] H. Zhu, S. Du, Z. Gao, M. Dong and Z. Cao "A Probabilistic Misbehaviour Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks" IEEE Transaction on Parallel and Distributed Systems, Vol. 25, PP 22-32, 2014.
- [2] M. Wright, J.W. Ho, et al "Fast Detection of Mobile Replica Node Attacks in Wireless Sensor Networks using Sequential Hypothesis Testing" IEEE Transaction on Mobile Computing, Vol. 10, PP 767-782, 2011.
- [3] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.
- [4] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.
- [5] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay- Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.