IJCAT International Journal of Computing and Technology, Volume 1, Issue 6, July 2014
ISSN : 2348 - 6090
www.IJCAT.org

# Trust and Reputation Management for Secure Communication in DTNs

[1] Vrinda A, [2] Arun Anoop M

[1] Mtech Student, Department Of CSE
MES College Of Engineering, Kuttippuram

[2]Assistant Professor, Department Of CSE
MES College Of Engineering, Kuttippuram

**Abstract -** Delay/Disruption Tolerant Networks (DTNs) have been identified as one of the key areas in the field of wireless communication, wherein sparseness and delay are particularly high. These characteristics pose several challenges to the security of DTNs. DTNs' links on an end-to-end path do not exist for a long time, and hence intermediate nodes may need to store, carry, and wait for opportunities to transfer data packets toward their destinations. Hence, DTNs are much more general than MANETs in the mobile network space. A security mechanism for DTNs is developed here which enables us to evaluate the nodes based on their behavior during their past interactions and to detect misbehavior due to Byzantine adversaries, selfish nodes, and faulty nodes. An approach to trust and reputation management is implemented which serves to ensure secure communication and isolates malicious nodes which may attack the network and reduces network performance in terms of reliability and security.

***Keywords*** **- Delay-Tolerant Networks, Trust, Reputation, Misbehaviour, Secure Communication**

## 1. Introduction

DELAY-TOLERANT Networks (henceforth referred to as DTNs) are a relatively new class of networks [12], where sparseness and delay are particularly high. In conventional Mobile Ad hoc Networks (MANETs), the existence of end-to-end paths via contemporaneous links is assumed in spite of node mobility. And if a path is disrupted due to mobility, the disruption is temporary and either the same path or an alternative one is restored very quickly. In contrast, DTNs are characterized by intermittent contacts between nodes. DTNs' links on an end-to-end path do not exist for a long time, and hence intermediate nodes may need to store, carry, and wait for opportunities to transfer data packets toward their destinations. Hence, DTNs are much more general than MANETs in the mobile network space. So MANETS are special type of DTNs[5].

Delay tolerant networks are self organizing wireless networks of large latency, limited resources and intermittent connectivity. In contrast to traditional mobile ad-hoc networks, DTNs forward message to the destination using a store, carry and forward manner and hence cope up with the short term connectivity. There is obviously a lack of centralized trusted entity in such a distributed network which can guarantee reliable transmission of data across the network. The open, distributed and dynamic nature of DTNs poses several security challenges.

Trust and security are two tightly interdependent concepts that cannot be separated. Trust is defined as "the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other party will perform a particular action important to the trustor, irrespective of the ability to monitor or control the party". Jøsang defines trust in a passionate entity (human) as the belief that it will behave without malicious intent and trust in a rational entity (system) as the belief that it will resist malicious manipulation. A trusted entity will not behave maliciously in certain situations. Trust is an important issue in distributed systems.

Transactions that occur in a distributed environment can cross domains and various organizations and not all can be trusted equally. Even within a domain the users trustworthiness can differ. A flexible trust management system can maintain current and consistent trustworthiness information for different nodes in a

distributed environment and the main work presented here highlights it.

## 2. Literature Survey

Sepandar D.Kamvar,Mario.T.Schlosser and Hector Garcia-Molina [10] proposed an efficient EigenTrust algorithm for reputation management in P2P networks. Though the algorithm ensures anonymity where the trust values cannot be increased or decreased by malicious peers, it relies on the existence of pre-trusted nodes in the network. Here the local and global trust is used to evaluate trust of a node. Sonja Buchegger and Jean-Yves Le Boudec[9] proposed a bayesian model approach for reputation systems. Though this approach finds false positives effectively it was found to be less applicable to DTNs due to their unique characteristics. Here less weight is given to evidence received in the past and more weight to recent evidence. It uses both reputation rating and trust rating to evaluate a node.

Rabin patra,Sonesh Surana and Sergu Nedevschi [8] proposed a hierarchical Identity based cryptography for End-to-End security in DTNs. This approach creates a secure channel for end-to-end connectivity and uses aymmetric key cryptographic technique. It provides protection against theft of information, modification and provides authenticated access. But since it requires a Private key generator (PKG) for key distribution, once it is compromised the system will not work.

Gianluca Dini and Angelica Lo Duca[7] proposed a reputation-based approach to tolerate misbehaving carriers in DTNs. Here local utility function is the value which decides whether a particular node has to be selected as a carrier for a message. It involves more communication overhead.

Zhaovu Gao,Haojin Zhu,Suguo Du,Chengxin Xiao and Rongxing Lu [4] suggested a probabilistic misbehavior detection scheme in DTNs which introduced a periodically available trusted authority which could launch the probabilistic detection for the target node and judge it by collecting and forwarding history evidence from its upstream and downstream nodes. Here a good node is inspected less times than a bad node. But since rare inspection of good node is done, the node can build reputation and start misbehaving. P Srilega and Nagajyothi M E [2] suggested a threshold based reputation management mechanism. Even though it is a very simple mechanism, it does not effectively identify the adversaries because approach depends on ACK to decide whether the packets reached destination or not. Ing-Ray Chen,Fenye Bao,Moon Jeong Chang and Jin-Hee Cho[1][6] developed dynamic trust management scheme which determines and applies the best operational settings at runtime in response to dynamically changing network conditions to minimize trust bias and to maximize the routing application performance. Though a combination of 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 is used here, it involves more overhead due to the increased number of parameters.

## 3. Trust and Reputation Management Scheme

Many attacks like routing attacks or attacks on packet integrity are not very big concern in DTNs. Due to the lack of end-to-end path and by efficient usage of authentication mechanisms, such attacks can be prevented in DTN. But since there is no centralized control, packet drop attacks are harder to withstand because node cooperation is fundamental requirement for delay tolerant networks.

The main aim of this trust and reputation management mechanism is to develop a security mechanism for DTNs which enables us to evaluate nodes based on past interactions and to detect misbehavior due to malicious nodes. This is hence a distributed malicious node detection mechanism for DTNs and it enables every node to evaluate every other nodes based on their past behavior without a central authority. A node in DTN cannot use watchdog mechanism to monitor another intermediate node after forwarding packets to it. This is due to the non existence of end-to-end path between source and destination. Similarly relying on ACK packets from destination for establishing reputation values will also fail due to the lack of a fixed common path from source to destination.

In DTNs usually direct observations are not very practical due to the opportunistic contacts for communication. Trusting a peers feedback and trusting a peers service quality are two different concepts taken care of in the existing mechanism. It is a graph based technique where the service providers are represented as bit vertices and raters are represented as check vertices of a bipartite graph as shown in figure. Every rater has some opinion of the service providers .The algorithm analyze the collection of these opinions to decide what values should be given to service providers under consideration. Once the values of service providers are almost estimated, the

next step deals with determining whether the raters are trustworthy or not.

A novel method for trust and reputation management is developed where TRj-Global reputation of jth service provider. TRij-Rating of SPj from peer i.Ri-Report of trustworthiness of ith peer as a rater. Raters, SPs and associated relationship interpreted as a bipartite graph. In this representation, each rater corresponds to a check vertex in the graph, shown as a square and each SP is represented by a bit vertex shown as a hexagon in the graph. If rater i has a rating about jth Service provider, an edge with value TRij from ith check vertex to jth bit vertex is put.Age factored values are considered as edge values as time goes by.To each edge ij a value WRij is assigned,WRij=wij(t) * TRij denotes age factored TRij value. wij(t) represents time varying service quality,The input parameters given are Ri and WRij to obtain reputation parameters TRj and list of malicious raters.

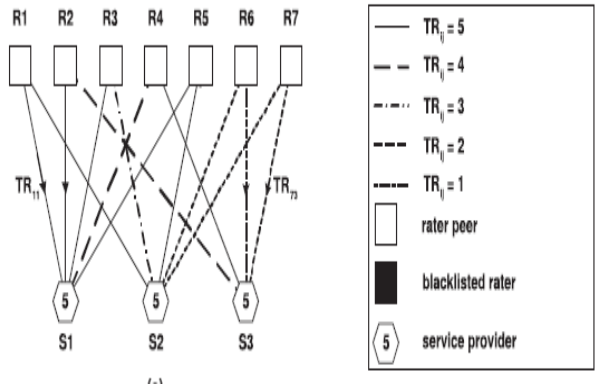
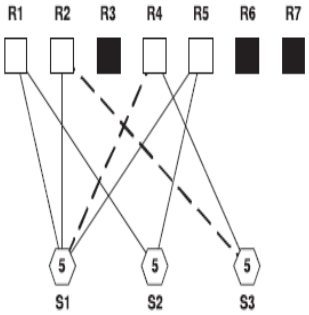



Fig 1: List Of Raters and Service Providers represented with their associated relationships.




| Iteration | $TR_1$ | $TR_2$ | $TR_3$ |
|---|---|---|---|
| 0 | 4.8 | 3 | 2.75 |
| 1 | 4.8 | 3.5 | 3.33 |
| 2 | 4.8 | 4.33 | 4.5 |
| 3 | 4.75 | 5 | 4.5 |

| Iteration | C1 | C2 | C3 | C4 | C5 | C6 | C7 |
|---|---|---|---|---|---|---|---|
| 0 | 1.1 | .72 | .10 | 1.52 | 1.1 | 1.87 | 1.87 |
| 1 | .85 | .43 | .35 | 1.23 | .85 | 2.42 | - |
| 2 | .43 | .35 | .77 | .65 | .43 | ▪ | ▪ |
| 3 | .12 | .38 | ▪ | .63 | .12 | ▪ | ▪ |

Fig 2: Malicious Raters Blacklisted

Global reputation TRj is computed as a weighted summation of Ri and WRij .

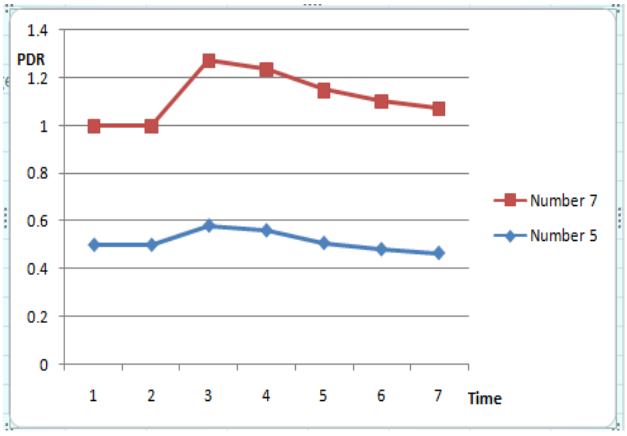
## 4. Application of Trust and Reputation Scheme for DTNs

An arbitrary node in network selected as judgenode. This node will create rating about another node by collecting feedbacks about another node and aggregating them and there is no direct monitoring. Each judgenode has a rating table and its entries are feedbacks about another node. Judge has to wait long to issue its ratings to all other nodes. Rating table of judgenode represented as bipartite graph with one check vertex and some bit vertices. The bit vertices represent subset of nodes for which the judge has received sufficient number of feedbacks to form rating with high confidence.

## 5. Simulation Setup and Results

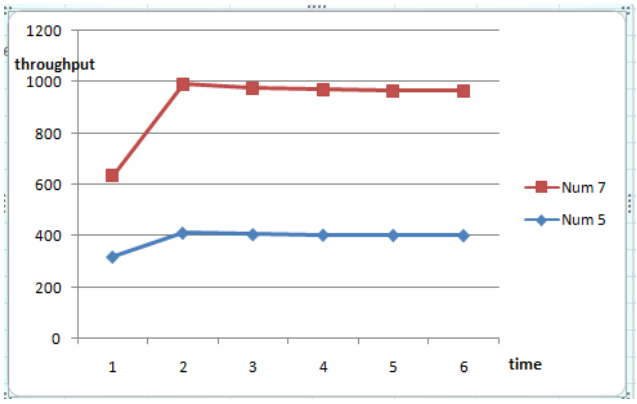
The scenario creation for nodes in DTN is done using NS-2 simulator. Since it is a special case of adhoc networks, the nodes are mobile. The ratings are assumed to be nonbinary (Normally assumed to be within 1 to 10 for simulation setup). The CBR traffic is generated and results of implemented trust and reputation scheme proves that there is a lot of requirement for collecting the ratings about another node by any arbiterary node in the DTN. This is due to the intermittent connectivity of the delay tolerant networks.

Hence by the time a fifth or sixth feedback reaches a judge node, the first feedback packet may be dropped and hence packet delivery ratio reduces and eventually throughput is also found to be low. The graphical results are shown below.




Graph 1: Simulation Time versus PDR (Varying Number of Nodes)

The packet delivery ratio for 5 and 7 nodes are shown in graph 1 above. The Overall capacity utilization is summarized in the graph 2.




Graph 2: Simulation Time Versus Throughput(Varying Number of Nodes)

## 6. Conclusion

The security mechanism implemented here effectively isolates malicious nodes in a network .The simulation results highlights the need for a much more effective method to improve the packet delivery ratio due to the short range contact or intermittent connectivity in DTNs. The throughput also doesn't show much improvement with varying number of nodes. A method to improve PDR and throughput could be considered in the future for effective secure communication in DTNs.

## References

[1] Ing-Ray Chen,Fenye Bao,MoonJeong Chang and Jin-Hee Cho "Dynamic Trust management for Delay tolerant networks and its application to secure routing" IEEE Transactions on parallel and distributed system ,2013

[2] P Srilega and Nagajyothi M E , "Minimised Delay and Adversary detection in DTNs" International Journal of Engineering Science Invention ,April 2013

[3] Sangeetha R and Krishnammal N, "Detection of routing attacks in Disruption tolerant networks" The international journal of engineering and science,2013

[4] Zhaovu Gao,Haojin Zhu,Suguo Du,Chengxin Xiao and Rongxing Lu, "PMDS:A probabilistic misbehaviour detection scheme in DTN" IEEE Signal Proc. Mag,2012

[5 ]Erman Ayday and Faramarz Fekri, "An iterative algorithm for trust management and adversary detection for delay-tolerant networks" IEEE Transactions on mobile computing,September 2012.

[6] Ing-Ray Chen,Fenye Bao,MoonJeong Chang and Jin-Hee Cho, "Integrated Social and Qos Trust based routing in Delay Tolerant Networks" Springer,2012

[7] Gianluca Dini and Angelica Lo Duca, "A reputation based approach to tolerating misbehaving carriers in Delay tolerant networks" IEEE International conference,2010

[8] Rabin patra,Sonesh Surana,Sergu Nedevschi "Hierarchical Identity based cryptography for End-to-End security in DTNs" IEEE International Conference,2008

[9] Sonja buchegger and Jean-Y ves Le Boudec "Robust Reputation System for P2P and Mobile adhoc networks" National Competence center in research on mobile information and communication systems,2004

[10] Sepandar D Kamvar ,Mario T Schlosser and Hector Garcia-molina "The EigenTrust Algorithm for reputation management in P2P Networks" ACM international confer-
ence,May 2003

[11] K liu,J.Deng,P.K Varshney and K Balakrishnan, "An Acknowledgement-based approach for the detection of routing misbehaviour detection in MANETs" IEEE transactions on mobile computing,2007

[12] K .Fall, "A delay-tolerant network architecture for challenged internets" Proceedings of ACM SIGCOMM,2003

**Vrinda A** She obtained her BTech in Information Technology from university of Calicut in the year 2007. She was a member of faculty in the department of information technology at Amrita School Of Engineering,ettimadai, Coimbatore from 2007 to 2009.Later she took up employment as lecturer in department of information technology in MESCE,kuttippuram, kerala. Presently she is pursuing her MTech programme in computer science and engineering at MESCE kuttippuram. She has 5 years of teaching experience. Her research interests covers areas of network security, cryptography and mobile ad-hoc networks.

**Arun Anoop M** He obtained his BTech in Computer Science and Engineering from cochin university in the year 2008.He completed his PG diploma in information security and system administration from DOEACC center, NIT , Calicut and obtained his MTech in Information Technology from kalasalingam university in the year 2011.Presently he is working as Assistant Professor in Computer Science and Engineering, MESCE, kuttippuram, kerala.Before joining MESCE he has worked as teaching assistant in information technology in kalasalingam university, krishnankoil, Tamilnadu. He is having 3.6 years of teaching experience. He has attended many workshops, FDPs and conferences. His areas of interest are network security, wireless sensor networks, protocol design, formal languages and theoretical computer science. He has presented 3 papers in National and International Conferences. He has published 8 journals and guided 6 Mtech students.