A Survey on the Misbehaving nodes and Counter Measures to avoid them

R.PandiyaRajan[1], D. Dennis Ebenezer[2]

[1]*PG Scholar, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*
Roseraja01@gmail.com

[2]*Associate Professor, Department of Computer Science and Engineering, Christian College of Engineering and Technology, Dindigul, Tamilnadu - 624619, India.*
dennisebe@gmail.com

Abstract— **The modern era communication is one of the main aspects in day-today life. Specifically, wireless communication has attracted lot of users with is dynamic infrastructure and ease of use. Disruption Tolerant Network (DTN) is on added to wireless technology as technology improves, the shortcomings also growing. One such drawback in DTN is breaking the communication without forwarding the messages to the neighbouring node. A node that does this is labelled as selfish node. In this proposed project a system connected to the network checks whether the system contains selfish node or not, and this checking is done by two method, one is partial selfish node and another is fully selfish node. If a node is selfish, some on alternative path for destination must be chosen. While choosing the alternative path the selfish node can be eliminated. By using the selfish node detection method, it is easy to reduce the impacts of selfishness. Selfish node is detected by the help of selfishness alarm, and this alarm is called as false alarm. After completing the selfish node detection is done the result can be produced with the help of two comparative charts, the charts are response chart and accuracy chart. By using this method, there will be an increase in the data accessibility with high accuracy, reduced time the query delay time, and also it reduces the impact of selfishness.**

Keywords- **DTN, selfish node, false alarm, Routing Evidence, game theory analysis, cluster based algorithms.**

I. Introduction

A network is a collection of computer, printer and other equipment that are connected together so that they can communicate with other. Network share data or information between computer nodes that are connected inside a room a campus, two separate buildings or any two different geographic locations. There are many types of network that are used but basically LAN, MAN, WAN is used [12]. Nowadays there are so many networks are used they are Wi-Fi, MANETs, DTN, VANET, wireless sensor networks are used for communication. The increased need and utility of networks has resulted in creating new network protocols and architecture. Most of them are adhoc in nature. Due to the success of MANETs, further improvements are done to form a network called Disruption Tolerant Network (DTN).

II.NETWORK PROBLEM

Cable Problem

Cables which interconnect different parts of a network can be shorted. A short may happen when the conductor wire gets contact with another conductive surface modifying the path of the signal. Cable testers are used to test the types of problems in the cable such as Cut cables problem, in corrected cable connections problem Cable is shorts, Interference level problem.

Connectivity Problems

The problems with connectivity on the one or more devices in a network may occur after an configuration change or by a malfunction in a connectivity components.

Networks Collision

This leads to the slower connectivity. The problems may occur as a result of bad network profile, a user transfer a lot of information's and jabbering network card Network problem. A jabber Network card is a suited on a transmit mode. This transmits light will remain constantly denoting that the Network card is always transmitted.

Software Problems

Networks problem may be occur and they are being tracked by software configuration such as DNS configurations, WINS configurations, the registered etc.

Duplicate IP Address

A common problems in many of network environments happens while two machines try to use the same IP address. This results in an intermittent communication.

IP Address and Network Card Issues

When two computers utilizes the same IP address and the IP address that is identifying computer's feature, which leads to the connectivity issues. In otherwise the network cards links the computers, and failures in the network cards disrupt connectivity.

Network Problems

Problems comparative to the connectivity plug-in us perceptually, and more over the solution occurs on checking their physical connectivity and connecting devices. Even through Wi-Fi networks, there may be some sort of unreachable areas such as where radio signals just refuse to venture and with multiple clients' WLAN, then choose a location to install the router.

Drop in Internet Connections

While troubleshooting, the internet connection falls must start with verifying the router and configuration problems occurs. Before that, confirm whether the signal strength is good or not, and if it is not fine then there is some problem in the internal connection.

Firewall Status

It provides the security, along with that the setting can be interferes with file sharing on connected computers. It is true that disabling security features can make the system vulnerable to attacks, although lowering security levels should not lead so much trouble.

Slow-moving Connectivity

Slow connectivity is the sign of a hazard plotted network, which leads to the extra collisions, and thus the network is incapable of handling. Heavily weighed file transfer brings down speed crucially. At times, the network card - actually in charge, could be overtaxed.

III.TRUSTED MANAGEMENT SCHEMES IN DTNS

The aim of trust management is to develop a security mechanism for DTNs, which evaluates the node based interaction and detects the misbehaving node. The DTN cannot monitor other intermediate nodes, then forwarding packets and finally send the acknowledgment for source to destination in repeated operation for DTN networks. In DTN networks, the trust authority is periodically checked for the misbehaviour node or selfish node to work as estimated - the trust of node in search of selfish node in DTN network locally or globally[1]-[5]. The main problem of these system false-negative nodes not visible to the user, it is only visible for system. It is mainly occur in packet loss and data modify in the network problem.

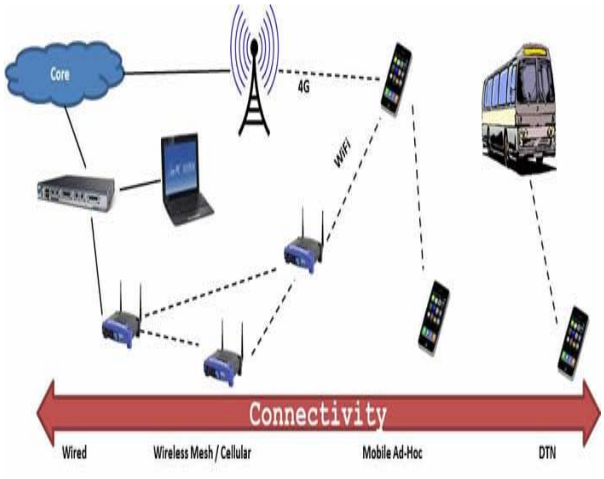

Fig.1 Generation Of Connectivity In Network

The figure shows the evolution of connectivity from wired to DTN. In case of wired connectivity there exists a wired connection between the sender and receiver. With the advent of wireless mesh/cellular the wired components were completely replaced by satellite signals. In case of abrupt changes in climatic conditions leads to signal distortion or loss which leads to a shortcoming of wireless mesh connectivity. In order to rectify the problem caused by wireless mesh overcomes the mobile ad-hoc connectivity this trusted on real time mobile connectivity. The recent invention in connectivity is the DTN (Disruption Tolerant Networks) which finds use in vehicle communication overcoming the disruptions caused during vehicle movement.

IV.DISRUPTION TOLERANT NETWORKS COMMUNICATION ARCHITECTURE

In the DTNs, many real time applications are there with some advantages in business, education, governments-military purpose. Using DTNs the secure transfer of data is happened with users such as organization's (companies), cities, Universities.

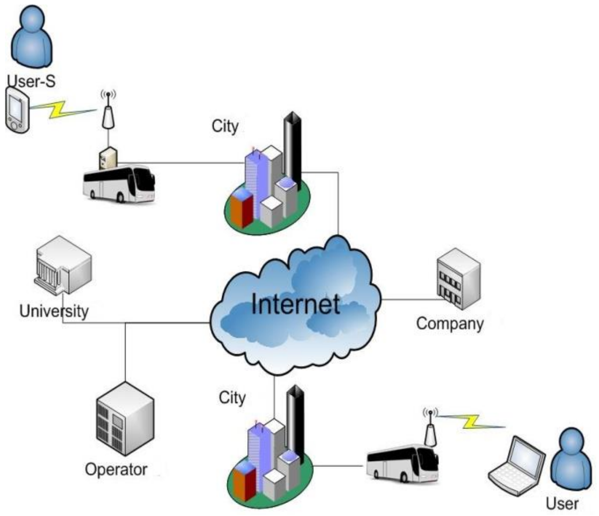

Fig.2 Example Of DTNs

V.PROBLEMS IN DTN

In normally network, there are lots of problems in the existing system which occurs because of collision, Traffic, data breakup by nature fault and due to these reasons the data loss happens and attackers attack the data. To overcome the above problem I develop iTrust formation. I reduce the data hackers and product the data. We can access the data very fast and add multiple nodes simultaneously by forming of iTrust. We can access the data insecure manner using inspection game theory.

VI.OVERCOMING THE PROBLEMS IN DTN

The group members are that’s based on the structure, which is used to efficiently track the group membership and member's position. In that three sub modules. They are Local Group Membership Management, Membership Management at the Network Level. In local group membership management contains a member joins or removes send the message through unicast to the zone leader. Membership management at the level contains Zone membership reporting by zone leaders, Empty-zone handling and Message aggregation.

In order to get added and leave a multicast group, nodes in the network should have the source information. As a source moves in a DTN, it quickly finds the source when need and efficiently tracks the location of the source node. RSGM incorporates mechanisms for session creation and efficient source discovery [2]. It contains two sub modules like session initiation and source tracking. A source needs to send the multicast packets reliably to the group members and destination node. With the membership management the member zones are recorded by source S, while the local group members and their positions are recorded by the zone leaders. Multicast packets will be sent along a virtual distribution tree from the source to the member zones, and then along a virtual distributions tree from the zone leader to the group members. A virtual distribution tree is formulated to during transmission time and guided by the destination positions.

A. Misbehaviour Node

Identification of misbehaving nodes in ad hoc networks is critically important to detect security attack in the network [5][8]. Two types of misbehaving nodes such as selfish and malicious nodes are taken into consideration in Selfish nodes do not intend to directly damage other nodes, but however it does not co-operate, saving battery life for their own communications. But malicious nodes do not give priority to saving battery life, and aim at damaging Identification of misbehaving nodes in ad hoc networks is critically important to detect security attack in the network. Two types of misbehaving nodes such as selfish and malicious nodes are taken into consideration in Selfish nodes don't intend to directly damage other nodes, but however, do not cooperate, saving battery life for their own communications. But malicious nodes do not give priority to saving battery life, and aim at damaging other nodes. In the current research paper, with reference to we introduce two different types of selfish nodes. As the nodes in DTN are battery powered, energy becomes a precious resource, and thus, role of selfish Nodes draw more attention.

Thus, we introduce altogether three routing behaviours of Nodes in a DTN. a) Type 0: well-behaved node: a well cooperates in the communication well, performs as required routing protocol, and equally participates in the communication activities like route discovery, maintenance, packet forwarding and receiving [4][5] etc. b) Type 1 : active selfish node : Such a node does not participate in and drops every received packet, and thus, It packet forwarding mechanism for the packets which have a destination address, other than this selfish node. In fact, it helps the selfish node to save its own energy, thereby still contributing to network maintenance. c) Type 2: passive selfish such a node practically does nothing stays idle in the network. It does not contribute to any of the activities like packet forwarding, receiving route discovery, network maintenance With respect to above mentioned misbehaving nodes, we evaluate the performance of DSDV, DSR and AODV routing protocols through extensive simulations where a certain percentage of nodes behave as active and/or passive selfish nodes with the remaining nodes being well-behaved[8]-12].

B. Mechanism for Detecting Misbehaviour Nodes

The IDS we propose belongs to specification-based detection with distributed cooperative nodes that are suitable for DTN. The misbehaviour node detection process that we propose validates the communication path then detects and isolates Misbehaviour nodes in the invalid paths. The proposed IDS use the collaboration of a group of nodes to make accurate decisions. The successfully detected misbehaviour node is added to a black-list which is broadcast to all 1-Neighbors and so on to all Network nodes. Then all neighbour nodes receive this list and it makes another confirmation by sending a PVM message to the attacker to be certain this node is actually an attacker. After confirmation it resends the black-list to its neighbours with a higher Rating. When the neighbour receives this black-list it excludes the attacker from the routing table to ignore attacking attempts.

C. Methods for Handling Selfishness in DTN

The nodes which act selfishly to conserve their resources are called selfish nodes in DTN some node data forwarding packets to other nodes [3] . The selfish nodes are engaged to Many selfish node detection methods are found to detect the nodes detect the selfish nodes which do not allocate replica for the purpose terms of allocating replica to other nodes. This also discusses the key features of selfish nodes and numerous allocation techniques will considerably reduce the delay in query processing infrastructure and base station This mobility causes frequent partitioning in network, hence the data accessibility in DTNs, the main requirement is that all the nodes have to fully in terms of their resources. The selfish node that does not allocate data items for the purpose of the selfish nodes allocate data items that are highly accessed by Selfish nodes reduce the data accessibility, wherever closest in appearance to Times. Avoid using bit-mapped fonts. True Type 1 or Open Type fonts are required. Please embed all fonts, in particular symbol fonts as well, for math, etc.

VII.FALSE ALARM DETECTION IN HANDLING OF SELFISH NODES IN DTN

In a mobile ad hoc network, the mobile nodes may move randomly to a big problem such as performance degradation and the poor techniques on data replication. Most of the users assigns that mobile nodes in reality [3][5], some nodes may decide not operate with others nodes. The behaviour of those selfish data accessibility in the network, Selfish node detection algorithm that considers the partial selfish replica allocation has developed. The replica will be allocated using specific node. An alarm will be raised based on the selfish behaviour be initiated because of disconnections in the network, it affects the false alarm detection as different from all other selfishness and to inform that the other nodes are at route as exactly as the disconnections happens to select the another best alternative path and by including those Detection of attacker node in the network and that must be informed to all others stations[10][12].

Devices in the specified range can be with a point-to-point manner. Mobility is a vital feature of DTN. This device has some features considering Bluetooth, WI-Fi network interfaces and communication in a decentralized manner. Mobile-ad hoc networks can be able to instantaneously interconnect without any defined pre-existing infrastructure. [13]More networks suffer due to the high cost and lack simulation and in general, that has two different approaches for enabling.

1) *Infrastructure -Based network* Wireless mobile networks usually been based on which mobile devices communicate with access points.

2) *Less Infrastructure network* In this approach, there is no central wireless network - less infrastructure in manner commonly known as tolerant network (DTN).

A DTN is a collection of network that can dynamically form a network to transfer informations.DTN have a lot of attraction because in each node in a DTN must act as a router, and the nodes will move freely in a DTN .Although it leads to some data accessibility is often a significant performance metric in a DTN [1][2]. It has some great features such as mobility and flexibility in the real world application areas whereas topology changes very quickly. DTN is dangers from compromised nodes inside the network, limited security, dynamic topology, scalability and Because of these vulnerabilities criteria, DTN Devices in DTN should be able to detect the presence of other facilitate communication and sharing of data and service. Nodes that directly is responsible for dynamically discovering each theirs. In order to within each other's communication range, intermediate nodes acts as routers that relay packets generated respective destination.

The nodes in DTN are often energy constrained such as battery, memory space in our point of memory space as the constraint to find out the behaviour of the node. In DTN, breaking of communication link is very frequent, to move anywhere. The density of nodes and number of nodes depend on the topology of DTN results in route changes and Data's are replicated at nodes, than the unique owners, to increase data partitions [15][16. A large amount of research has been recently proposed simultaneously improve data accessibility and reduce query response time if the original data. However, there is often a trade- off between data accessibility DTN have only limited memory.

1) *Preventions methods*

Detect the misbehaviours node in using routing evidence and auditing phase will be used some routing mechanisms are delegation, forwarding history contact history. The attack is prevent for using reactive routing protocol and novel tech, voting, random key selection tech and monitoring in malicious node and using some other technical's.

2) *Game theory analysis*

In this method, all the nodes in a particular range is formed as a group and they are provided with the public key and private key to identify itself When a particular node leaves the group and when it returns back it needs to identify the group with the public key and itself by using the private key. This is done to all the leaving nodes when they come back as a game.

3) *Routing Evidence Generation Phase*

In this method when packets are forwarded from the router the router sends an empty acknowledgement and also a confirmation of from where the data packet is forwarded. The empty acknowledgement is used to receive an acknowledgement from the destination that the data has reached a valid destination.

4) *False Alarm*

The false alarm will be different from the overall selfishness alarms. If any alarm generates must be verify the reason of the alarm. False alarm will calculate the degree of selfishness and confirm the behaviour of selfish nodes at the network. If the number of selfish nodes exceeding the threshold value means it will give confirmation of overall selfishness alarm else the alarm has been raised for the reason that of the network disconnections. We are about to diagnose the network disconnections by use of false node detection algorithm. If it will became true we should neglect the alarm with of less disquiets. The detection of this false alarm leads to better performance in the overall network.

There may be any network disconnections can happen over the route. When Route Maintenance specifies and informs that the source route is broken or destroyed, the Source node which needs to send data can attempt to use any alternate route it chances to know the Destination node, or can invoke Route Discovery again to find a new route. Route Discovery and Route Maintenance operate entirely on request. In particular, DSR does not require periodic packets of any kind at any level within the network.

5) *Adaptive Query Processing*

The adaptive algorithm adapts to the dynamic changes to achieve the least transmission cost. The adaptive algorithm basically, the base station collects cost statistics in each processing round but it only decides whether to switch algorithms for every round, where is an adjustable system parameter, based on the lowest average transmission cost estimated. The cost statistics is cleared after a switch. Since the switch is triggered by the base station, which is also responsible for tracking the cost statistics the incurred overhead is limited to the cost of some extra information in the NSB and BB methods.

Sufficient Set-based

The sufficient set collecting data from its cluster, a cluster head computes the sufficient set from the local collected tupels and sends it to the base station.

Necessary Set based

Cluster head first computes its own necessary set and sends the set to the base station. Station merges all the received tuples into a finds the necessary boundary .That is called the global boundary (GB).

Boundary-based method

Instead of directly deliver the data tuples to the base station; the boundary-based method first delivers the local knowledge in clusters, in the form of sufficient boundary and necessary boundary to the base station in order to facilitate a refined global data pruning among clusters later.

VIII.CONCLUSION

Thus I have reduced the impacts of selfishness replication in DTN with improved accuracy and reduced communication cost. We have addressed the problem of selfish nodes from the replica-allocation perspective. Selfish replica allocation guides to improve the overall poor accessibility in DTN. It is proposed as a selfish node detection method and a novel replica allocation technique to handle the selfish allocation correctly. It is also applied the concept of credit risk from economics to detect the selfish nodes. Every node calculates the degree of selfishness from credit risk value. Traditional replica allocation techniques cannot judge the selfish nodes, so it proposed novel replica allocation techniques additionally we have upgraded the DTN network and adaptive query processing algorithm. Extensive results show that the proposed strategies do better than existing represents techniques such as data accessibility communication cost, query delay and false alarm.

IX .REFERENCES

[1] Haojin Zhu et al, "A probabilistic misbehaviour detection scheme towards efficient trust establishment in delay tolerant networks" IEEE transaction on parallel and distributed systems Feb-2014.

[2] Haojin Zhu et al," PMDS: A Probabilistic Misbehaviour Detection Scheme in DTN" international journal.

[3] Qinghua Li, Sencun Zhu Guohong Cao, "Routing in Socially Selfish Delay Tolerant Networks Department of Computer Science & Engineering the Pennsylvania State University park.

[4] Ying Zhu, Bin Xu "A Survey of Social-Based Routing in Delay Tolerant Networks: Positive and Negative Social Effects" Senior Member, IEEE.

[5] J.Ameen Basha1 , D.S Arul Mozhi2 "Detection of Misbehaviour Activities in Delay Tolerant Network Using Trust Authority" 1M.E.Student Assistant professor, Department of Computer Science and Engineering, Dhanalakshmi College of Engineering Chennai.

[6] Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto1 "Detecting Black hole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method" Received Dec. 19, 2005; revised and accepted Jan 27 mar 2006.

[7] ”The Sybil Attack in Sensor Networks: Analysis & Defences" James Newsome, Elaine Shi, Dawn Carnegie Mellon University adrian@cmuedu.

[8] Ms.Aarthy D.K.1, Mr.C.Balakrishnan2 "Detecting selfish routing and misbehaviour of malicious node in disruption tolerant networks" Computer Science Department, S.A Engineering College, Chennai ,Tamil Nadu.

[9] N.Bhutta, G.Ansa, E. Johnson "Security analysis for Delay Disruption Tolerant satellite and sensor Networks" Centre for Communication Systems Research University of Surrey Guildford, United Kingdom.

[10] Qinghua Li." Mitigating Routing Misbehaviour in Disruption Tolerant Networks" Student Member, IEEE, and Guohong Cao, Fellow, IEEE.

[11] Jingzhe Du ,“Distributed Key Establishment in Disruption Tolerant Location Based Social Wireless Sensor and Actor Network" Evangelos Kranakis School of Computer Science Carleton University Ottawa, Canada.

[12] Damon McCoy, Doug Sicker, Dirk Grunewald," A Mechanism for Detecting and Responding to Misbehaving Nodes in Wireless Networks" Department of Computer Science University of Colorado Boulder, Colorado.

[13] Chi Zhang*, Xiaoyan Zhu+, Yang Song* and Yuguang Fang*+" A Formal Study of Trust-Based Routing in Wireless Ad Hoc Networks", Department of Electrical and Computer Engineering, University of Florida, Gainesville FL 32611, USA National Key Laboratory of Integrated Services Networks, University, Xi'an 710071, China.

[14] Behrouz Jedari1 , Rouhollah Goudarzi2, Mehdi Dehghan3 "Efficient Routing using Partitive Clustering Algorithms in Ferry-based Delay Tolerant Networks" 3Computer

Engineering Department Amirkabir University of Technology, Tehran.

[15] Ha Dang, Hongyi Wu, "Clustering and Cluster-Based Routing Protocol for Delay-Tolerant Mobile Networks Member, IEEE.

[16] Shabbir Ahmed and Salil s., "Cluster-based Forwarding in Delay Tolerant Public Transport Networks" Computer Science and Engineering, The University of New South Wales Sydney, Australia.