International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 2, August 2014)

An iTrust Based Misbehaviour Detection Technique on Clustered Nodes in Delay Tolerant Network

A. Mary Judith[1], V. Anusha[2], S. Vinod[3]

[1,2]*M.E Student,* [3]*Assistant Professor, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, Tamil Nadu, India.*

***Abstract*-- The delay tolerant network suffers from various problems such as frequent network disconnectivity and many routing problems .The transmission attains a failure due to these problems. The existing system created an iTrust scheme to detect the malicious nodes that puts down the transmission. This detection mechanism works at a certain probability and reputation in order to reduce the cost and to ensure the security. The proposed system makes the DTN into clusters and implements the same detection scheme. This will make the network more efficient than the existing system by reducing the traffic, energy consumption, time consumption and prolong the DTN lifetime.**

***Key Terms*-- Clustering, Malicious node detection, DTN, inspection game model.**

I. INTRODUCTION

The ultimate aim of the paper is to make the DTN more reliable and efficient in terms of energy, cost, traffic and malicious node detection.

This paper detects the malicious nodes in the network more efficiently than the existing work by reduction in energy consumption and traffic reduction. It is designed to use storage within the network to support store-and-forward operation over multiple paths and potentially long timescales, and not to require but to support end-to-end reliability.

The DTN architecture envisages security mechanisms that protect the infrastructure from unauthorized use by allowing for policy-based discarding of traffic as quickly as possible.

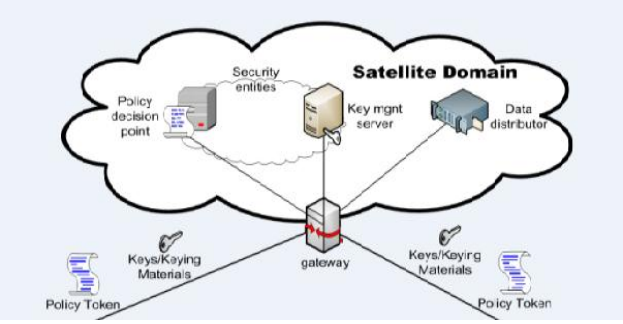

Fig 1

Some of the issues in delay tolarent networks are

- Key Management
- Handling Replays
- Traffic Analysis
- Routing Protocol Security
- Multicast Security

DTN such as wireless sensor network suffer mostly from a problem of disconnectivity during the transmission of location dependent information, traffic reports and various other information. In DTN nodes involve in activities such as droping the packets and modify the data in order to launch attacks. This activity can be referred as routing misbehaviour [2]. This misbehaviour induces reduction in packet delivery rate and imposes threat to network performance and network lifetime. Thus detecting the misbehaviour is desirable in order to ensure secure and energy efficient routing and security on the nodes.

There are various methods to detect the packet dropping where the destination acknowledgement can be used and by using the revocation schemes the malicious nodes can be revoked. But the detection schemes are found to be inefficient in DTNs changing network conditions, delay in acknowledgement and hop monitoring etc[3]. Forwarding the history information to detect the misbehaviours in the network is also found to be inefficient as it will require more security due to the exposure of previous information, this may lead to more energy consumption by the nodes in the network.

The existing system as used technique called iTrust, a probabilistic misbehaviour detection scheme where it establishes both the detection and trust mechanisms in the DTN [6]. Here the security is ensured where the iTrust scheme involves in verifying whether the participating node adheres to the rules. The iTrust method adopted this mechanism from the game theory model called inspection game. To detect the misbehaviour the existing system introduced a Target Authority (TA) which detects by capturing a target node and judges it by using the previous history information and either compensates the node with another new node or removes it.

Further it introduced a reputation system where the inspection probability varies with the target node reputation. It checks the nodes reputation with higher and lower probability. Thus the existing system used the TA to ensure security of routing in DTN with an appropriate probability[1].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 2, August 2014)

The DTN security will consume high bandwidth. The amount consumed depends on the way parameters are encoded.

The proposed system uses the same security and detection mechanisms in the cluster. This system will group the nodes into clusters for various advantages and to overcome certain issues [11].By forming the nodes into clusters the consumption of energy by the nodes will be reduced which will save the power as it is not possible to recharge or replace the battery often in the DTN. Implementing the security and detection schemes in the clusters in the proposed work will reduce the traffic, collision among the nodes and the reduction in energy consumption of the nodes. If more than one security services is used in the same cluster more of the bandwidth amount will be used [14].

II. System Analysis

System Analysis is a combined process dissecting the system responsibilities that are based on the problem domain characteristics and user requirement.

2.1 Existing System

The ability to transport, or route, data from a source to a destination is a fundamental ability all communication networks must have. Delay and disruption-tolerant networks (DTNs) are characterized by their lack of connectivity.

A common technique used to maximize the probability of a message being successfully transferred is to replicate many copies of the message in the hope that one will succeed in reaching its destination [13]. This is feasible only on networks with large amounts of local storage and internode bandwidth relative to the expected traffic.

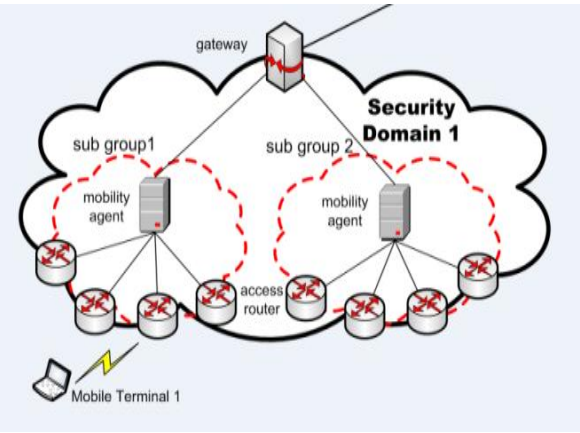

Fig 2

Security concerns for delay-tolerant networks vary depending on the environment and application, though authentication and privacy are often critical.

These security guarantees are difficult to establish in a network without persistent connectivity.

Routing in networks faces many threats which may lead to the damage and destruction of the network. Designing a threat detection technique is great challenge.

The existing system used a mechanism called iTrust, probabilistic misbehaviour detection scheme was established [1]. This scheme is used to detect the routing threat in the DTN network. This mechanism also ensures secure routing in the DTN network.

The iTrust creates a trusted authority to find the nodes behaviour in the network by using the various information's such as routing information's, transmission rate, traffic information's etc[2][4]. It further verifies the security of the routing in the DTN network by using the iTrust scheme[1][2].

The iTrust mechanism follows game theory model called inspection game to detect the threat and ensure secure routing in the DTN [6]. This scheme involves in verifying whether the another party adheres to the rules (protocols) [5]. Here the inspector does only partial verification due to limited resources. To detect the misbehaviour the existing system introduced a Target authority which detects by capturing a target node and judges it by using the previous history information and either compensates the node with another new node or removes it.

Further it introduced a reputation system where the inspection probability varies with the target node reputation [1]. It checks the nodes reputation with the inspection probability which varies according to the nodes reputation. A node with good reputation will be verified with lower probability where as node with bad reputation will be checked will higher probability [7].

2.2 Proposed System

The proposed system forms clusters among the nodes in the DTN. Clustering of nodes has various advantages. The components of a cluster are usually connected to each other through fast area_networks ("LAN"), with each node (computer used as a server) running its own instance of an operating_system. In the proposed system the nodes in the network are clustered aiming at traffic reduction, reduction on the energy consumption by the nodes in the network and to reduce the time taken to detect the malicious node in the network [12]. Clusters are usually deployed to improve performance and availability over that of a single computer, while typically being much more cost-effective than single computers of comparable speed or availability. Clustering relies on a centralized management approach which makes the nodes available as orchestrated shared servers. It is distinct from other approaches such as peer to_peer or grid_computing which also use many nodes, but with a far more distributed_nature.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347-6435(Online) Volume 3, Issue 2, August 2014)

Clusters involve in performing load balancing and high availability. High-availability clusters" (also known as failover clusters, or HA clusters) improve the availability of the cluster approach. They operate by having redundant nodes, which are then used to provide service when system components fail.

The existing misbehaviour detection mechanism is used in the in the clusters in the DTN in the proposed system. Instead of verifying the nodes the network that is not involved in transmitting the packet which leads to unnecessary use of the energy, it is better to use the detection scheme in the clusters individually. This mechanism will save the energy consumption, reduce the traffic in the network and consume the detection time [7].

III. System Implementation

Implementation is the stage of the project when the theoretical design is turned out into a working system. The most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and its constraints on implementation, designing of methods to achieve change over and evaluation of change over methods.

3.1 Module Description

- Information Generation Phase
- Information Investigation Phase
- Probabilistic Verification And Reputation System
- Node Clusteration

3.1.1 Information Generation Phase

This phase generates information's such as the number of routing task and packet forwarding informations. These information's will be forwarded to the next phase called audit phase to detect the malicious nodes that causes threat in the network.

Firstly, when a source node is about to transmit a packet to the destination node where the destination node is not in the transmission range of the source node, the source node will select an intermediate node through which it will transmit the packet the packet to the destination. The task of transmitting the packet from the source to the intermediate node and the required number of intermediate node transmission and then finally to the destination indicates the number of routing task has taken place [4]. This is referred as the delegation task.

Secondly, when a node chooses the next intermediate node and checks whether it is the desirable node to transmit the packet [10]. If it is, then it will forward the packet. This packet forwarding information will be provided in this phase.

3.1.2 Information Investigation Phase

In the audit phase the TA will verify the nodes using the information's provided from the generation phase. The generation phase will provide the routing task and the forwarding information to the authority for investigation. In order to verify the TA will initially collect the set of message forwarding requests, the set of forwarded messages and the set of contacted users.

It verifies whether the forwarding requests is satisfied and checks whether the next hop node chosen is the desirable node according to the DTN routing protocol [5][8]. Further it investigates whether the multi hop forwarding is done according to the multihop routing protocol [8]. This is how the target authority detects the malicious nodes in the network.

3.1.3 Probabilistic Verification and Reputation System

In order to reduce the cost of malicious detection a probabilistic method of verification is done as explained below. This method allows the target authority to detect the malicious nodes at a certain probability. This method allows the authority to make choice to either inspect the node or not.

The target authority will verify the node at a certain probability [8]. Further it introduced a reputation system where the probability varies with the reputation of the target node. It checks the nodes reputation with the inspection probability [1]. A node with good reputation will be verified with lower probability where as node with bad reputation will be checked will higher probability.

3.1.4 Node Clusteration

In order to increase the life time of the Delay tolerant network and to reduce the energy consumption by the nodes in the network the proposed system groups the nodes in the network into clusters [12]. The existing work of the probabilistic method of malicious node detection will be performed in each of the clusters in the network that performs the transmission of data [8]. This proposed work will reduce the cost which is proved in the existing system long with the traffic reduction and time reduction in the malicious node detection in the DTN.

IV. Conclusion

The proposed system follows the same malicious node detection scheme and security mechanisms performed in the existing network. In order to make the DTN more reliable and efficient, the proposed system forms clusters among the nodes in the network. This work will reduce the energy consumption by the nodes and it will reduce the traffic and save the detection time in the network as it performs the detection scheme and security mechanisms on the clusters in the network.

REFERENCES

[1] Haojin Zhu, Suguo Du, Zhaoyu Gao, Mianxiong Dong, and Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks", IEEE transactions on parallel and distributedsystems,vol.25,no.1,january2014.

[2] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10, 2010.

[3] 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.

[4] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security,vol. 7, no. 2, pp. 664-675, Apr. 2012.

[5] 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.

[6] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary DetectionforDelayTolerantNetworks,"Proc.MilitaryComm.Conf.(Milcom'10), 2010.

[7] B.B. Chen and M.C. Chan, "Mobicent: A Credit-BasedIncentive System for Disruption-Tolerant Network," Proc. IEEEINFOCOM'10,2010.

[8] A. Lindgren and A. Doria, "Probabilistic Routing Protocol for Intermittently Connected Networks," draft-lindgren-dtnrg-prophet-03, 2007.

[9] W. Gao and G. Cao, "User-Centric Data DisseminationinDisruptionTolerant Networks," Proc. IEEE INFOCOM '11, 2011.

[10] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM '10, 2010.

[11] O. Younis, M. Krunz, and S. Ramasubramanian, "Node Clusteringin WirelessSensorNetworks:RecentDevelopmentsandDeploymentChallenges,"IEEENetwork, vol.20,no.3,pp.20-25,May/June2006.

[12] S. Bandyopadhyay and E. Coyle, "An Energy Efficient Hierarchical Clustering Algorithm for Wireless Sensor Networks," Proc.IEEE INFOCOM, vol. 3, pp. 1713-1723, Mar.2003.

[13] Vahdat, Amin; Becker, David (2000), "Epidemic routing for partially connected ad hoc networks", *Technical Report CS-2000-06*, Duke University.

[14] Harminder Singh Bindra, Amrit Lal Sangal," Considerations and Open Issues in Delay Tolerant Network'S (DTNs) Security", Department of Computer Science and Engineering, NIT Jalandhar, Punjab, India, June 2, 2010.