An Efficient Trust Management Technique for Delay Tolerant Network

Ranjan Singh
Mtech Scholar
Department of CSE
MANIT, Bhopal, India

Meenu Chawla, Ph.D
Professor
Department of CSE
MANIT, Bhopal, India

ABSTRACT
Delay Tolerant Networks (DTNs) have high end-to-end latency, which is often faces disconnection, and unreliable wireless connections. It does not mean a delay service instead DTNs provides a service where network imposes disruption or delay. It operates in challenged networks with extremely limited resources such as memory size, CPU processing power etc. This paper presents an efficient trust managing mechanism for providing secure environment. The proposed dynamic trust management protocol uses a dynamic threshold updating which overcomes the problems with time changing dynamic characteristics by dynamically updating the criteria in response to changing network conditions. This reduces overheads and increases the efficient use of routing network even in conditions change. Also the dynamic threshold update reduces the false detection probability of the malicious nodes. To show the effectiveness of the proposed system, a detailed simulation in the presence of selfish and malicious nodes is performed with ONE simulator. Finally a comparative analysis of our proposed routing with previous routing protocols is also performed. The results demonstrate that presented algorithm deals effectively with selfish behavior with providing significant gain on effective delivery ratio in trade off with message overhead and delay.

Keywords
Delay Tolerant Networks (DTN), Selfish Attack, Network Security, Trust Management.

1. INTRODUCTION
Wireless Delay Tolerant Network (DTNs) [1] is a new Networks class which is characterized by a long message delay and lack of a fully connected path between the source and the target nodes. As a result, the use of mobile nodes acting as a buffer between the one to other end and behave as a store and forward approach. The message moves to a new node when it appears in the range, similarly the messages reach their destinations. The message sending is an opportunistic procedure because the messages are sent in an opportunistic way.

Because of its characteristics wide range of useful applications have been developed for DTNs and enable a new class of networking applications in the wireless network interface which increases popularity of mobile devices. DTNs can be used for developing low-cost internet services on remote area moreover it can be used for vehicle DTNs for local advertising, location-based information collection such as traffic reports and parking information. However, the practical DTNs implementation is questionable because its characteristics making them vulnerable to serious security threats.

In the system every node predicted that intermediate nodes (or vehicles) are relaying the message properly. However malicious node not carries the message properly in the network which causes multi-hop communications to fail and detection of their presence may be hard. DTNs relay carriers sharing which is the essential requirement, but this cannot be guarantee because selfish nodes can avoid participating for other messages. On other hand malicious node creates the black hole which carries out attacks by deliberately dropping messages. Overcome these attacks is a real challenge due to the connectivity and distributed nature of DTNs. DTN are resource constrained in nature to save its own resources and nodes may develop selfish behavior. In which its drop the packet of other nodes to maximize its own credit or benefits. Such nodes increase the message drop probability and reduce the message delivery rate. In this paper, we propose a dynamic trust based approach to protect network from black hole and selfish attacks. The rest of the paper is organized as follows: the second section provides a brief discussion of the most recent relative literatures of DTNs and the system model is defined in third section. The fourth section explains the proposed algorithm and the simulated results and the fifth section explain about conclusion and future work on the basis of the simulation results presented in fourth section.

2. LITERATURE REVIEW
Since the security in the DTN has already an open issue hence this section presents a brief review of some of the recent and relevant literatures. E. Bulut [2] presented a study on DTNs in presence of malicious nodes (also known as compromised DTNs). The literature analyzes the effects of malicious nodes presence on routing in compromised DTNs. They also proposed a two period routing to achieving the required delivery ratio with limited packet lifetime in presence of malicious nodes. The variants of social psychology based approach is one of the commonly found and widely applied [3] [4] [11] [12] because of their similarity with structure of the DTNs. These methods works by checking social characteristics like locality, community and relations to decide packet forwarding or consider other characteristics such as selfishness, unwillingness to avoid packet forwarding. Most of the literature shows that these techniques can effectively improve the routing performance of DTN. A combined social psychology and game theory is presented in [3] [8] which utilize the game theory to find the solution and cause of the social misbehaving. A probabilistic technique for nodes misbehavior detection and efficient trust establishment named iTrust is proposed by Haojin Zhu [8]. The iTrust utilizes the Trust Authority (TA) to periodically check the nodes behavior by cost. Trust Authority is small in numbers because it is fixed and little bit costly, so availability of TA probability cannot be guaranteed if network size is large. Another common approach [11] is trust management which works by estimating the trust level of the nodes either by locally or

globally. Generally the trust is estimated by observing the packets in surrounding environment. Since the trust estimated by any node is shows its own criteria or vision and the major problem with such systems are false negative trust estimation because of nodes visibility, hence effective approaches are required to reduce the false detection. Geographic routing protocol is one of the recent approaches but they required special costly hardware such as GPS, directional antennas etc. Ing-Ray Chen [9] proposed and analyzes the trust management protocols for encounter based routing. They incorporated in quality-of-service (QoS) trust properties (connectivity) and social trust based properties (honesty and unselfishness) for trust evaluation in the routing protocol. In their literature review two different protocols, an equal-weight QoS, social trust based management protocol and a QoS only trust management protocol are considered. A Credit Based Incentive System is proposed in [5], which allows the routing protocol to search the most efficient routes, with incentive considerations, hence protect against behavior of purposely waste transfer opportunity and unfairly increased rewards of selfish nodes. The algorithm also provides different incentive mechanisms to effectively handle different properties. A secure data forwarding scheme is presented by Mohamed Elsalih Mahmoud [6], they named it SATS. The SATS uses credits to measure the node's cooperation in forwarding other node's messages and to maintain fairness. It also utilizes a trust system to assign a specific trust value to each node. A node's trust value indicates that how actively it forwards other's messages. The nodes with high trust values are preferable in data forwarding to avoid the attackers that are not participating in routing process. The SATS forces nodes for cooperation to only earn trust but also maintain it at higher values. Haojin Zhu [7] proposed a multilayer credit based incentive technique, to encourage forwarding cooperation among DTN nodes. The scheme has feature to operate in a fully distributed manner to defend various attacks without depending upon any specialized hardware. The performance of proposed method is further increased by different optimization techniques by exploiting the unique characteristics of DTNs.

3. SYSTEM MODEL

In the present work we consider the DTN environment without any centralized trusted authority (TA). Nodes are able to use multi hops communication. Node exchanges the information on encounters with another node.

3.1 Selfish Behavior and Model

The selfish behavior of the node is defined as the unwillingness of node in participation of its resources on others requirement, this is generally done to maintain its limited resources such as power. Since DTNs required participation of all nodes in packet relaying this could cause severe degradation of the performance. They considered selfish nodes acts for its own interests, so to save energy it just drop the packet but it may decide to forward a message with a certain probability. Two kind of selfishness:

1. Individual Selfishness: Here node forwards only those packets which are generated by it and drop packets from other node.
2. Social Selfishness: Here nodes are willing to forward packets for other nodes with whom they have social connect but not others and such willingness varies with the strength.

Strategies [13] for prevention of selfishness are as follows:
1. Barter Based
2. Credit Based
3. Reputation Based

Barter Based is pair wise Tit-For-Tat strategy. The procedure is that two encounter nodes exchange the equal value of messages. A message in which the nodes are interested is called primary message and other are secondary messages, hence it degrades the performance of nodes drastically.

Credit Based strategy are cooperative to forward the messages, the idea is to gets certain amount of credit as a reward that it can later explore for its own profit. Credit Based are generally of two types: Message Purse Model and Message Trade Model. In Message Purse Model source node pay credits to the intermediate nodes which are involve in forward the messages to the destination. In Message Trade Model the sender of the message pay credits to receivers in each hop-by-hop transmission until the message reach the destination, which finally pays credits for the message forwarding.

Reputation Based strategy based upon cooperative experiences and observation of its past activities. If the reputation value of a node is less, it reflects that the node is selfish according to other nodes, otherwise Cooperative nature to the nodes. Each intermediate node receives a reputation value after pass a message to other nodes. The reputation value is a proof about the cooperative nature of the intermediate node. Reputation Based are generally of two types: Detection Based Model and Without Detection Based Model. In Detection Based every node detects the behaviour of the receiver which receives the message from him, in order to monitor the selfishness and encourage them to be cooperative in nature. In reputation the node is punished if it is not cooperate in nature. Reputation is also used in Social Selfishness Aware Routing (SSAR), the performance of the node is not affected by the not well-behaved nodes. First check the willingness of receiving node if it is ready then the message with higher delivery probability in the network is transferred.

When a node behave as a selfish then forward the messages only to its community while a malicious node aims to break all the protocols of basic DTN routing functionality. A malicious node drops the packets and also performs the trust related attacks:

1. Self-promoting attacks: To attract other packets in the network its increase own importance by providing good credits or recommendations for itself.
2. Bad-monitoring attacks: It decreases the probability of packet routing through good nodes by providing bad recommendations and its ruin the reputation of well-behaved nodes.
3. Ballot stuffing: It increase the probability of packet transfer through malicious node by proving good recommendations to the bad nodes, it increase the reputation of not well-behaved nodes.

A malicious node attacker performs random attacks to evade detection. We introduce a new random attack probability to reflect random attack behavior. When random attack probability is equal to 1, the malicious attacker is a reckless attacker, when random attack probability is less than 1 it is a random attacker. The node trust value is directly accessed by the trust evaluation and indirect trust value by recommendations. Upon the encounter process the

one node trust is depend upon other. Trust protocol is independently run by each node. Most of the detection scheme [14] focuses on the detection of node. However after detection how their behavior can change and how they can be motivated to avoid such malicious behavior haven't been explained anywhere. We have also focused on the scenario when an honestly behaved node changes it's behavior then how it's should be motivated to do honest behavior.

3.2 Trust Model

The node's trust level is defined as a number in the open interval between 0 and 1, (since the presented model neither distrust completely nor trusts completely), the trust increases with higher values. The proposed algorithm flow chart as represented in **Fig. 1.**

The proposed trust estimation uses the equation 1 to estimate the trust for the other nodes.

$$T_{ij} = \frac{w_j * N_j}{\sum_{j=1}^{n} w_j * N_j} K_i$$

.....eqn. 1

Where,

T_{ij} represents the truth of j^{th} node calculated by i^{th} node

W_j is the weight factor of j^{th} node calculated by eqn. 2

N_j is the number of packet send by j^{th} node and observed by i^{th} node

k_i is the network condition estimated by i^{th} node

$$w_j = \frac{F_r * P^t_{routing} + F_d * P^t_{data} + F_c * P^t_{control}}{P^t_{routing} + P^t_{data} + P^t_{control}}$$

.....eqn. 2

Where,

$P^t_{routing}$, P^t_{data} , $P^t_{control}$ are the total number of routing, data and control packets received till time t

F_f , F_d and F_c are weight factor for each type of packet in the range of (0, 1)

$$K_i = \frac{sum(P^t_{routing} + P^t_{data} + P^t_{control})}{K_{t-1}}, K_{t=1,}\ at \quad t = 0$$

.....eqn. 3

R_n = random number generated by using number probability distribution and follows eqn. 4

$$0 \le R_n < \frac{F_r + F_d + F_c}{3}$$

.....eqn. 4

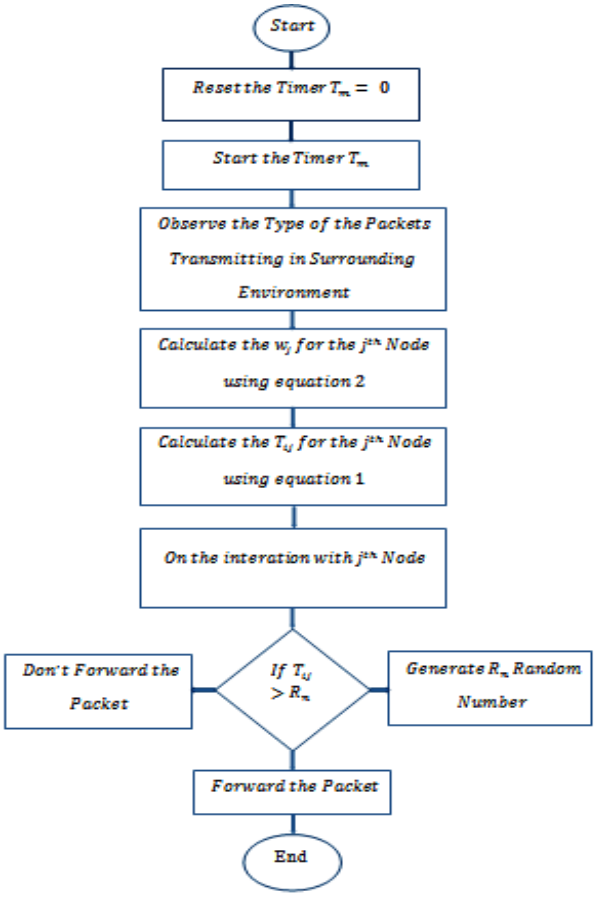

Fig. 1: Flow Chart of the Proposed Algorithm

4. Simulation Setup and Results

To evaluate the performance of proposed model, the simulation of the proposed technique is performed using ONE simulator, using the following configurations as in **Table 1**.

Table 1: Simulation Environment Configuration

Configuration Parameter	Value
Bluetooth Transmission Rate	250 Kbps
Bluetooth Transmission Range	150m
High Speed Interface Transmission Rate	10Mbps
High Speed Interface Transmission Range	1000m
Number of Groups	6
Message TTL	300 minutes
Area	4500mX3400m
Number of Nodes	240
Simulation Time	5000 Seconds

The simulation is performed for different ratios of malicious nodes and the different selfishness. The simulation results are presented in **Table 2** and **3** respectively. The different percentage of attacker nodes as compare to delivery ratio,

average latency, average buffer time and average hop count are represented in **Fig. 2, 3, 4** and **5** respectively.

Table 2: Effect of different numbers of attackers

Percentage of Attackers	Measures											
	Delivery Ratio			Average Latency			Average Buffer Time			Average Hop Count		
	Att.	Pre.	Prop.	Att.	Pre.	Prop.	Att.	Pre.	Prop.	Att.	Pre.	Prop.
5	0.5680	0.6036	0.7041	53.2344	557.0206	437.616	37.413	1025.125	977.3333	2.7188	1	1
10	0.5207	0.5621	0.6568	69.9273	557.9263	456.6486	35.7754	889.2909	586.4	2.9886	1	1
15	0.5266	0.5621	0.6627	62.6528	573.4937	421.5384	33.8188	771.1462	586.4	2.8202	1	1
20	0.4793	0.4911	0.574	69.9741	80.5193	452.533	32.3663	426.1921	260.5857	2.8272	1	1
25	0.503	0.5148	0.574	538.3482	81.3862	438.1041	258.3409	30.4581	178.6326	1	2.8621	1

Table 3: Effect of selfishness of attackers

selfishness of Attackers	Measures											
	Delivery Ratio			Average Latency			Average Buffer Time			Average Hop Count		
	Att.	Pre.	Prop.	Att.	Pre.	Prop.	Att.	Pre.	Prop.	Att.	Pre.	Prop.
50	0.5444	0.574	0.5976	498.175	69.7041	420.8525	259.0818	30.4943	178.8721	1	2	1
60	0.5266	0.5621	0.5858	514.2506	80.5631	429.3061	258.6023	30.6454	178.7535	1	2	1
70	0.5266	0.5621	0.5917	514.873	80.5747	425.052	258.8886	30.2907	178.8442	1	2	1
80	0.5207	0.5325	0.574	520.0625	60.5012	438.1041	258.5909	30.4832	178.6372	1	2	1
90	0.5148	0.5148	0.574	526.046	78.2659	438.1041	258.4864	30.6495	178.6326	1	2	1
100	0.503	0.5148	0.574	538.3482	81.3862	438.1041	258.3409	30.4581	178.6326	1	2	1

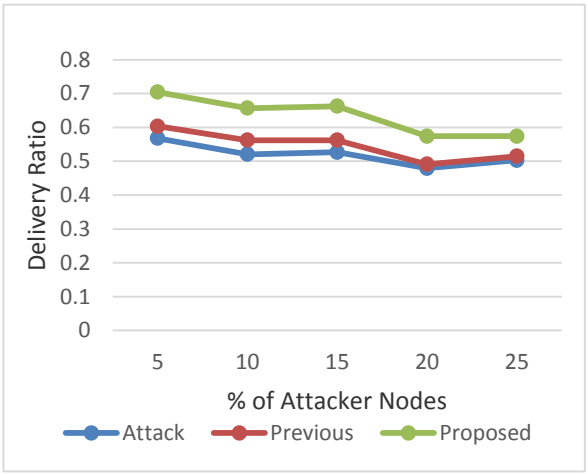

Fig. 2: Percentage of Attacker Nodes vs. Delivery Ratio

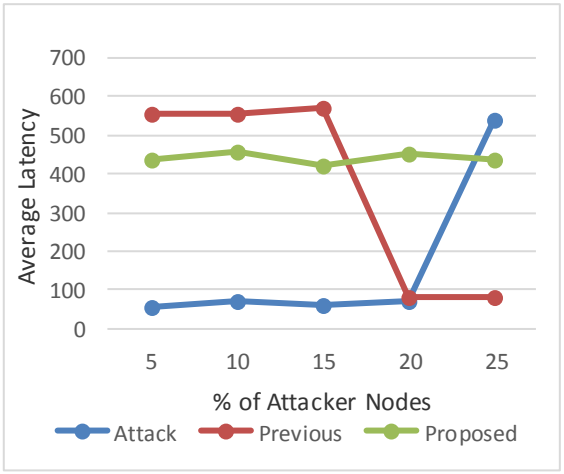

Fig. 3: Percentage of Attacker Nodes vs. Average Latency

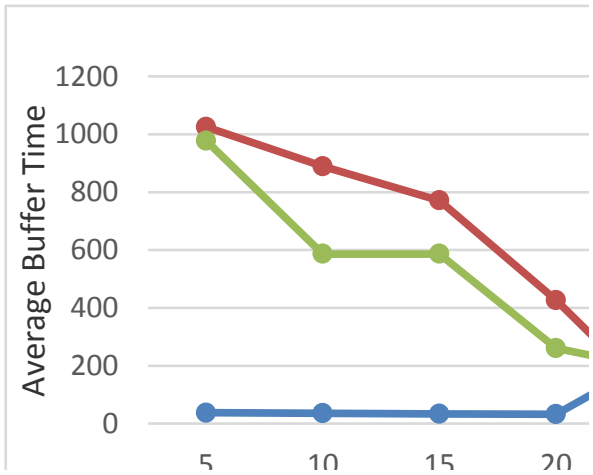

Fig. 4: Percentage of Attacker Nodes vs. Average Buffer Time

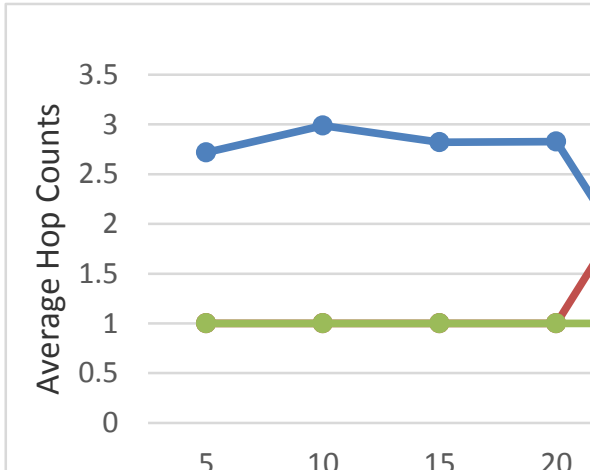

Fig. 5: Percentage of Attacker Nodes vs. Average Hop Counts

5. CONCLUSION

In this paper, we first classified the selfish behavior in DTNs and then existing strategies for preventing selfish behavior. We subsequently analyzed the mechanisms and explored techniques of the proposed strategies. Further, we pointed out the problems in previous technique. The previous strategy cannot work in an environment in which the node saves a high probability of being selfish to other nodes. But, we conducted an experiment to investigate the performance of the representative strategies in each category. The results of our experiment illustrate that the performance of proposed strategies outperforms the previous technique.

6. REFERENCES

[1] Forrest Warthman, Delay Tolerant Networks (DTNs), a tutorial, March 2008

[2] E. Bulut, B. Szymanski "Secure Multi-copy Routing in Compromised Delay Tolerant Networks", Wireless Personal Communication, vol. 73(1), November 2013, pp.149-168.

[3] WANG Cheng-jun, GONG Zheng-hu, TAO Yong, ZHANG Zi-wen, ZHAO Bao-kang "CRSG: A congestion control routing algorithm for security defense based on social psychology and game theory in DTN", J. Cent. South Univ. (2013) 20: 440–450

[4] Ying Zhu, Bin Xu, Xinghua Shi, and Yu Wang "A Survey of Social-Based Routing in Delay Tolerant Networks: Positive and Negative Social Effects", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 1, FIRST QUARTER 2013.

[5] Bin Bin Chen &MunChoon Chan, "MobiCent: a Credit-Based Incentive System for Disruption Tolerant Network",National University of Singapore,2008

[6] Mohamed Elsalih Mahmoud, MrinmoyBarua, and Xuemin (Sherman) Shen, "SATS: Secure Data-Forwarding Scheme for Delay-Tolerant Wireless Networks",IEEEGlobecom –Communication and system security,2011

[7] Haojin Zhu, XiaodongLin,Rongxing Lu, Yanfei Fan, and Xuemin (Sherman) Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks",IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 58,OCTOBER 2009

[8] Haojin Zhu, Member, Suguo Du, ZhaoyuGao, Mianxiong Dong, Member, IEEE, and Zhenfu Cao "A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks",IEEE,2013

[9] Ing-Ray Chen, FenyeBao, Moonjeong Chang, Jin-Hee Cho, "Trust Management for Encounter-Based Routing in Delay Tolerant Networks",Standard Form 298 (Rev. 8-98) Prescribed by ANSI-Std Z39-18,2010

[10] Ing-Ray Chen, FenyeBao, MoonJeong Chang, and Jin-Hee Cho, "Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing",IEEE TRANSACTION,2013

[11] Ting Ning, Zhipeng Yang, Hongyi Wu, and Zhu Han, "Self-Interest-Driven Incentives for Ad Dissemination in Autonomous Mobile Social Networks",2013 Proceedings IEEE INFOCON

[12] LIFEI WEI,HAOJIN ZHU,ZHENFU CAO,XUEMIN SHEN, "SUCCESS: A Secure User-centric andSocial-aware Reputation based Incentive Scheme for DTNs", 15 October 2011, Grant No. 61033014, National Natural Science Foundation of China

[13] Jingwei Miao, Omar Hasan, Sonia Ben Mokhtar, Lionel Brunie, Kangbin Yim, "An analysis of strategies for preventing selfish behaviour in mobile DTN",University of lyon france,2011

[14] Jingwei Miao, Omar Hasan, Sonia Ben Mokhtar, Lionel Brunie, KangbinYim, "An investigation on the unwillingness of nodes to participate in mobile delay tolerant network routing",International Journal of Information Management,2012