Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.548 – 554

SURVEY ARTICLE

A Survey on Trust Establishment in Delay Tolerant Networks

Vigneshkumar.P[1], Senthilnathan.K.R[2]

Department of Computer Science and Engineering, Sri Eshwar College of Engineering, Coimbatore

evervignesh@gmail.com [1], senthilnathanraj@gmail.com [2]

Abstract: This paper identifies various concepts involved in delay tolerant networks for finding the emerging topics. We focus on the various methods that can be applied for detecting the misbehaviour detection of nodes. The methods used are Probabilistic misbehaviour finding method, Complex network analysis, Social Selfishness Aware Routing (SSAR) algorithm, Secure Multilayer Credit-based Incentive (SMART) scheme, Practical incentive (Pi) protocol, Sprite. These methods provides various methods to find the misbehaviour nodes in DTNs, increase the delivery rate of a node, increase the routing performances in delay tolerant networks, reduce the computation overhead .

Index Terms: Misbehaviour node detection, Delay tolerant networks, Network failure

1. INTRODUCTION

A delay tolerant network is a network designed to operate effectively over long distance such as those in space communications. In such situations, long delay is inevitable.

In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data. Routing misbehaviour can be caused by selfish nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks. The recent researches show that routing misbehaviour will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance of DTN. Therefore, a misbehaviour detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the trust among DTN nodes in DTNs.

A. Misbehaviour Detection

In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data. Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or

malicious nodes that drop packets or modifying the packets to launch attacks. The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and, thus, pose a serious threat against the network performance of DTN. Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the trust among DTN nodes in DTNs. Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neighborhood monitoring or destination acknowledgement to detect packet dropping, and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes. Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficult to predict mobility patterns, and long feedback delay have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs. This can be illustrated by Fig. 1, in which a selfish node B receives the packets from node A but launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring-based misbehavior detection less practical in a sparse DTN.

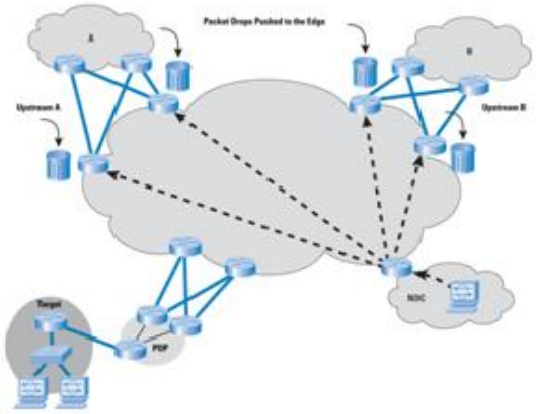

Fig. 1 Black Hole attack in DTN

Probabilistic misbehaviour detection scheme:

The routing evidence auditing costs high for verification and in order to reduce the cost, we introduce a probabilistic misbehaviour detection scheme. It allows the trust authority to launch the misbehaviour detection at a certain probability. This advanced technique is motivated by the inspection game, a game based theoretical technique, will have the positive probabilities of inspection and noncompliance based on the unique nash equilibrium.

The algorithm shows the details of the proposed probabilistic misbehavior detection scheme. For a particular node i, TA will launch an investigation at the probability of pb. If i could pass the investigation by providing the corresponding evidences, TA will pay node i a compensation w; otherwise, i will receive a punishment C

```
initialize the number of nodes n
for i 1 to n do
    generate a random number m_i from 0 to 10^n _ 1
    if m_i/10^n < pb then
    ask all the nodes (including node i) to provide
evidence about node i
     if BasicDetection(i,S_Stask , S_Sforward, [t1, t2],R,D)
then
    give a punishment C to node i
    else
         pay node i the compensation w
    end if
  else
     pay node i the compensation w
  end if
end for
```


Game Theory:

Before presenting the detailed inspection game, we assume that the forwarding transmission costs of each node *g* to make packet forwarding. It is also assumed that each node will receive a compensation *w* from TA, if successfully passing TA's investigation; otherwise, it will receive a punishment C from TA. The compensation could be the virtual currency or credits issued by TA; on the other hand, the punishment could be the deposit previously given by users to TA. TA will also benefit from each successful data forwarding by gaining *v*. In the auditing phase, TA checks the node Ni with the probability p_i^b. Since checking will incur a cost h, TA has two strategies, inspecting (I) or not inspecting (N). Each node also has two strategies, forwarding (F) and offending (O).

$$G=<N, \{s_i\}, \{\pi_i\}, \{p_i\}>.$$

- $N = \{N_0, N_1, \ldots\ldots N_n\}$ *is the set of players*
- $S= \{s_{i0}, si1, si2\ldots\ldots s_{in}\}$ *is the strategy set of the player* N_i.
- π_i *is the payoff of the* i^{th} *player.*
- P_i *is a mixed strategy for player.*

B. Complex Network Analysis

In DTN networks, forwarding decisions are generally made using locally collected knowledge about node behaviour to predict future contact opportunities.

In this work, demonstrate that Complex network analysis (CAN)-based DTN routing can offer significant performance benefits only if applied to social graphs exhibiting these properties. Furthermore, provide an efficient online algorithm to achieve this in a distributed fashion.

Evaluate SimBet and BubbleRap under a range of synthetic contact generation models (i.e., Small-World and Caveman) and real mobility traces. We show that good performance is consistently achieved only for a relatively narrow range of aggregation levels, where social graph structure closely reflects the underlying mobility structure.

Investigate different methods to identify this optimal operating point "on the fly". Specifically, we use clustering techniques to identify desirable patterns in observed node similarities, and then use concepts from spectral graph theory to maximize the modularity of such clusters, and compare the behavior of various contact models under different aggregation methods and levels.

A distributed online algorithm is presented that can adjust its contact graph mapping to achieve optimal performance, regardless of the mobility scenario or the specific routing protocol used.

In this paper, we have established the predominant importance of efficient mappings of mobility contacts to an aggregated social graph, which DTN algorithms using complex network analysis (CNA), can utilize to optimize forwarding decisions. Specifically, this aggregated social graph exhibits an optimal density where it best reflects the underlying social mobility and where performance benefits are maximized. Contrary to this, specific metrics and algorithms (e.g., for community detection, etc.) used by different CNA-based schemes seem to have a less prominent effect on performance. Finally, by mapping the problem to that of unsupervised clustering of observed node similarity values (online), we have shown that methods based on algebraic connectivity and cluster modularity can capture this optimal point in a robust manner both for synthetic models and real world traces. Using an algorithm based on these methods we can track this optimal point and achieve closed to offline performance, without prior knowledge. We believe that our preliminary findings and proposed solutions have a wider applicability for a large range of DTN data dissemination protocols based on social networks.

C. Social Selfishness Aware Routing

Existing routing algorithms for Delay Tolerant Networks (DTNs) assume that nodes are willing to forward packets for others. In the real world, however, most people are *socially selfish*; i.e., they are willing to forward packets for nodes with whom they have social ties but not others, and such willingness varies with the strength of the social tie. Following the philosophy of *design for user*, we propose a Social Selfishness Aware Routing

(SSAR) algorithm to allow user selfishness and provide better routing performance in an efficient way. To select a forwarding node, SSAR considers both users' willingness to forward and their contact opportunity, resulting in a better forwarding strategy than purely contact-based approaches. Moreover, SSAR formulates the data forwarding process as a Multiple Knapsack Problem with Assignment Restrictions (MKPAR) to satisfy user demands for selfishness and performance. Trace-driven simulations show that SSAR allows users to maintain selfishness and achieves better routing performance with low transmission cost.

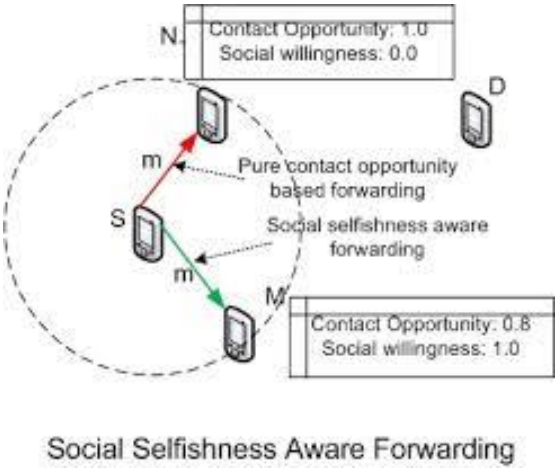

Fig. 2 SSAR Overview

Compute the selfish gain g for any packet in C
Sort C in the decreasing order of g/l (Let i denote the i^{th} packet in C)
for Packet i from 1 to $|C|$ do
if N is not in contact with M anymore then
break
end if
if $Li \geq l_i$ then
Forward i to N
for Packet j from $i + 1$ to $|C|$ do
$Lj -= li$
end for
else
continue
end if
end for

Algorithm for MKPAR through SSAR

D. SMART

In DTNs, the intermediate nodes on a communication path are expected to store, carry, and forward the in-transit messages (or bundles) in an opportunistic way, which is called opportunistic data forwarding. Such a forwarding method depends on the hypothesis that each individual node is ready to forward packets for others. This assumption, however, might easily be violated due to the existence of selfish or even malicious nodes, which may be unwilling to waste their precious wireless resources to serve as bundle relays. To address this problem, we propose a secure multilayer credit-based incentive scheme to stimulate bundle forwarding cooperation among DTN nodes. The proposed scheme can be implemented in a fully distributed manner to thwart various attacks without relying on any tamperproof hardware. In addition, we introduce several efficiency optimization techniques to improve the overall efficiency by exploiting the unique characteristics of DTNs. Extensive simulations demonstrate the efficacy and efficiency of the proposed scheme.

Pairing Technique:

SMART is based on bilinear pairing, which will be briefly introduced in the succeeding discussion. Let G be a cyclic additive group and G*T* be a cyclic multiplicative group of the same order *q*, i.e., |G| = |G*T* | = *q*. Let *P* be a generator of G. We further assume that ˆ*e*: G × G → G_T is an efficient admissible bilinear map with three properties.

1) ***Bilinear.*** For *a, b E* Zq^*, ˆ*e*(*aP, bP*) = ˆ*e*(*P,P*)*ab*.
2) ***Non degenerate.*** ˆ*e*(*P,P*) _= 1_{GT} .
3**) *Computable.*** There is an efficient algorithm to compute ˆ*e*(*P*1,*Q*1) for any *P*1, *Q*1 ∈ G.

Overview of SMART

Before presenting our SMART scheme, we first introduce a naive multilayer coin scheme. In such a naive scheme, the data-forwarding process can also be regarded as a layered coin generation process. When a node sends its own messages, the node will lose credit (or virtual money) to the network because other nodes incur a cost to forward the messages. The bundle sender first generates the base layer of a layered coin and then sends it together with the original bundles to a certain number of downlink nodes. At each subsequent hop, each intermediate node generates a new endorsed layer based on the previous layered coin. It is obvious that, with layered coins, each hop of a successful data-forwarding process can easily be tracked. After that, each intermediate node periodically submits its collected layered coins to the VB, which can calculate credits for each intermediate node and make a charge on the bundle senders. Note that, since only the nodes on the successful delivery path are rewarded, each intermediate node can launch different kinds of attacks on this naive system. We progressively determine what SMART needs to prevent the various attacks.

SMART scheme is proposed to stimulate cooperation in packet forwarding for DTNs. Two efficiency-optimization methods are evaluated to reduce the transmission and computation overhead. The SMART scheme is compatible to diverse existing routing schemes and is expected to improve the system performance of DTNs, which suffer from selfishness.

E. Practical Incentive (Pi) Protocol

Delay Tolerant Networks (DTNs) are a class of networks characterized by lack of guaranteed connectivity, typically low frequency of encounters between DTN nodes and long propagation delays within the network. As a result, the message propagation process in DTNs follows a store-carry and- forward manner, and the in-transit bundle messages can be opportunistically routed towards the destinations through intermittent connections under the hypothesis that each individual DTN node is willing to help with forwarding. Unfortunately, there may exist some selfish nodes, especially in a cooperative network like DTN, and the presence of selfish DTN nodes could cause catastrophic damage to any well designed opportunistic routing scheme and jeopardize the whole network. In this paper, to address the selfishness problem in DTNs, we propose a practical incentive protocol, called Pi, such that when a source node sends a bundle message, it also attaches some incentive on the bundle, which is not only attractive but also fair to all participating DTN nodes. With the fair incentive, the selfish DTN nodes could be stimulated to help with forwarding bundles to achieve better packet delivery performance. In addition, the proposed Pi protocol can also thwart various attacks, which could be launched by selfish DTN nodes, such as free ride attack, layer removing and adding attacks. Extensive simulation results demonstrate the effectiveness of the proposed Pi protocol in terms of high delivery ratio and lower average delay.

First, provide a fair incentive model in which selfish DTN nodes are stimulated to help forward bundles with credit-based incentive as well as reputation-based incentive. In the reward model, to achieve fairness, if and only if the bundles arrive at the destination node, the intermediate forwarding nodes can get credits from the source node. Furthermore, for the failure of bundle forwarding, those intermediate forwarding nodes still can get good reputation values from a trusted authority (TA).

Second, in order to guarantee the feasibility of the fair incentive model, use the layered coin model and verifiably encrypted signature techniques to provide authentication and integrity protection in the proposed Pi protocol.

Third, to confirm the effectiveness of the proposed Pi protocol, also develop a custom simulator built in Java to substantially show that the proposed Pi protocol can achieve the high delivery ratio and low average delay of DTNs when the high incentive is provided.

F. Sprite

Mobile ad hoc networking has been an active research area for several years. How to stimulate cooperation among selfish mobile nodes, however, is not well addressed yet. In this paper, we propose Sprite, a simple, cheat-proof, credit based system for stimulating cooperation among selfish nodes in
mobile ad hoc networks. Our system provides incentive for mobile nodes to cooperate and report actions honestly. Compared with previous approaches, our system does not require any tamper proof hardware at any node. Furthermore, we present a formal model of our system and prove its properties. Evaluations of a prototype implementation show that the overhead of our system is small. Simulations and analysis show that mobile nodes can cooperate and forward each other's messages, unless the resource of each node is extremely low.

A system to provide incentive to mobile nodes to cooperate is proposed. Our system determines payments and charges from a game-theoretic perspective, and we showed that our system motivates each node to report its behavior honestly, even when a collection of the selfish nodes collude. We also modeled the essential component of our system as the receipt-submission game, and proved the correctness of our system under this model. As far as we know, this is the first pure-software solution that has formal proofs of security. Our main result works for packet forwarding in unicast, and we extended it for route discovery and multicast as well. We also implemented a prototype of our system and showed the overhead of our system is insignificant. Simulations and analysis of the power-and-credit-conservative nodes showed that the nodes can cooperate and forward each other's messages, unless the resource of the nodes is extremely low.

S.No	Methods	Usage
1	Misbehaviour Detection	Detecting Misbehaviour Node
2	Complex Network Analysis	Graph Mapping
3	Social Selfishness Aware Routing	Packet Forwarding
4	SMART	Layer Concatenation
5	Practical Incentive Protocol	Authentication and Integration
6	Sprite	Message Forecast

2. CONCLUSION

The paper describes the comparison and analysis between various methods involved in the detection of emerging topics. It also illustrates that there are many techniques that can be followed for detecting the misbehaviour, forwarding node and node weights. This kind of comparison reflects that the efficiency differs from each method. This paper shows the usage of misbehaviour detection scheme based on network failure.

REFERENCES

[1] Haojin Zhu, 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 DISTRIBUTED SYSTEMS, Vol. 25, No. 1, January 2014.

[2] 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.

[3] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10, 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] 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] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM '03, 2003.

[7] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM '09, Apr. 2009.

[8] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858- 3868, Oct. 2008.

[9] 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.

[10] S. Reidt, M. Srivatsa, and S. Balfe, "The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks," Proc. 16th ACM Conf. Computer and Comm. Security (CCS '09), 2009.

[11] B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM '10, 2010.

[12] J. Douceur, "The Sybil Attack," Proc. Revised Papers from the First Int'l Workshop Peer-to-Peer Systems (IPTPS '01), 2001.

[13] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM '06, 2006.

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

