Probabilistic Misbehaviour Detection and Optimization in Delay Tolerant Network

Suljiya S A

M-Tech Computer Science and Engineering

Lourdes Matha College of Science and Technology

Thiruvananthapuram, India

Abstract **:Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment.. In this paper, we propose ant colony optimization for DTN routing towards efficient trust establishment. Ant Colony Optimization (ACO) with Optimized Link State Routing (OLSR) protocol to identify stable paths in between source and destination nodes. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.**

1 .INTRODUCTION

Delay tolerant networking is a networking architecture that is designed to provide communications in the most unstable and stressed environs, where the network would generally be topic to regular and long lasting disruptions and high bit error rates that could severely degrade normal communications. Delay tolerant networks are frequently used in disaster relief assignments, peace-keeping assignments, and in vehicular networks. DTN is based on a new experimental protocol called the Bundle Protocol (RFC 5050). Delay tolerant networks utilize the mobility of nodes. The nodes can move anywhere at any time. In a delay tolerant networks all devices search for nearer visible devices. Due to the intermittent connectivity it is very difficult to maintain end-to-end connections. This consents the furthering of data, only if it is in dealings with other nodes. So many traditional protocols and conventional routing schemes are failed under this long propagation delay. The basic idea behind DTN network is that endpoints aren't always unceasingly linked. In order to aid data transfer, DTN usages a store-and-forward methodology athwart a router that is more disruption-tolerant than TCP/IP. A delay tolerant network (DTN) is a network designed so that temporary or intermittent communications evils, restrictions and incongruities have the smallest possible adverse impact. There are several aspects to the effective design of a DTN, containing:

- The usage of fault-tolerant techniques and technologies.
- The superiority of agile dilapidation under hostile situations or great traffic loads.
- The capacity to preclude or rapidly recuperate from electronic attacks.
- Capability to function with negligible dormancy even when routes are unclear or unpredictable.

Fault-tolerant systems are designed so that if a component fails or a network route turns out to be impracticable, a backup module, process or path can immediately take its place without forfeiture of service. At the software level, an interface consents the administrator to continuously monitor network traffic at multiple points and locate evils instantaneously. In hardware, fault tolerance is achieved by component and subsystem redundancy. Graceful degradation has always been important in large networks. In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities). 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.

Delay-tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Examples of such networks are those operating in mobile or extreme terrestrial environments, or planned networks in space.Recently, the term disruption-tolerant networking has gained currency in the United States due to support from DARPA, which has funded many DTN projects. Disruption may occur because of the limits of wireless radio range, sparsity of mobile nodes, energy resources, attack, and noise.

A DTN is a network of smaller networks. It is an overlay on top of special-purpose networks, including the Internet.DTNs support interoperability of other networks by accommodating long disruptions and delays between and within those networks, and by translating between the communication protocols of those networks. In providing these functions, DTNs accommodate the mobility and limited power of evolving wireless communication devices. DTNs were originally developed for interplanetary use, where the speed of light can seem slow and delay-tolerance is the greatest need. However, DTNs mayhave far more diverse applications on Earth, where disruption-tolerance is the greatest need. The potential Earth applications span a broad range of commercial, scientific, military, and public-service applications.DTNs can accommodate many kinds of wireless technologies, including radio frequency (RF), ultra-wide band (UWB), free-space optical, and acoustic (sonar or ultrasonic) technologies.

Delay tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information) , and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the “store-carry-and-forward” strategy, and the routing is decided in an “opportunistic” fashion.

2 .PROBLEM DEFINITION

Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge.iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node’s behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node’s reputation, which allows a dynamic detection probability determined by the trust of the users. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.

Disadvantages

- Transmission overhead and verification cost is high in the misbehaviors detection.
- Occur long feedback delay and high variation in network condition.
- Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs).
- Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge.
- 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, difficulty to predict mobility patterns, and long feedback delay, have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs
- Low efficiency of routing
- Low routing speed

To avoid these I propose antcolony optimiation in delay tolerant networks

3 .PROBLEM FORMULATION

To formulate probabilistic misbehavior detection scheme in delay tolerant network has major challenges are routing efficiency , speed ,time and transmission overhead.

3.1EXISTING SYSTEM

This section describes our system model and design goals.

3.1.1 Network phase

A DTN consisted of mobile device owned by individual users and each node has its unique ID and corresponding private/public key pair. By adopting the single- copy routing mechanism such as first contact routing protocol, and assuming the communication range of a mobile node is finite. Thus a data sender out of destination node's communi to submit collectedcation range can only transmit packetized data via a sequence of intermediate node in a multi-hop manner.

General DTN formed by a set of mobile devices owned by individual users. Each node i is assumed to have a unique nonzero identifier Ni, Which is bound to a specific public key certificate. We interchangeably use node I and Ni here after. We also assume that each node has limited transmission and reception capabilities so that two nodes in a multihop manner. End-to-end connections are not always guaranteed, and routing, therefore is made in an opportunistic" way. Similar to other credit-based schemes, we assume that there exists some special network components, such as the round side unit in verticular DTNs and the information publisher in social network. The DTN nodes can exploit opportunistic link to these network components to submit collected coin to the VB. Before joining the DTN network, every DTN node should be registered with the OSM and obtain its public key certificate.

3.1.2 Routing phase

A normal user will honestly follow the first routing protocol by forwarding the message as long as there are enough contacts. The requested messagehas been forwarded to the next hop,the chosen next hop nodes are desirable nodes according to a specific DTN routing protocol,and the number of forwarding copies satisfy the requirement defined by a multy-copy forwarding routing protocol.

Single-copy routing mechanism such as first contact routing protocol and we assume the communication range of a mobile node is finite. Thus a data sender out of destination node's communication range can only transmit packetized data via a sequence of intermediate nodes in a multi-hop manner. Our misbehaving detection scheme can be applied to delegation based routing protocols or multi-copy based routingones,such as MaxProp and ProPHET.

3.1.3 Auditing phase

Auditing Phase In the Auditing phase, TA will launch an investigation request towards node Nj in the global network during a certain period [t1,t2]. Then, given N as the set of total nodes in the network, each node in the network will submit its collected {Ei→j task,Ej→k forward,Ej↔k contact|∀i,k ∈ N}to TA. Bycollecting all of the evidences related to Nj, TA obtains theset of messages forwarding requests Stask, the set of messages forwarded Sforward and the set of contacted users Scontact, all of which could be verified by checking the corresponding evidences.

To check if a suspected node Nj is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by Nj. We assume that m ∈ Stask is a message sent to Nj for future forwarding and Tts(m) is its expiration time. We further define Nk(m) as the set of next-hop nodes chosen for message forwarding, R as the set of contacted nodes satisfying the requirements of DTN routing protocols during [Tts(m),t2] and D as the number of copies required by DTN routing. The misbehavior detection procedure has the following three cases.

- Class I (An Honest Data Forwarding with Sufficient Contacts):

A normal user will honestly follow the routing protocol by forwarding the messages as long as there are enough contacts. Therefore, given the message m ∈Stask, an honest data forwarding in the presence of sufficient contacts could be determined if

$$m \in Sforward \text{ and } Nk(m) \subseteq R\text{and } |Nk(m)| == D$$

which shows that the requested message has been forwarded to the next hop, the chosen next hop nodes are desirable nodes according to a specific DTN routing protocol, and the number of forwarding copies satisfy the requirement defined by a multi-copy forwarding routing protocol.

- ClassII(AnHonestDataForwardingwithInsufficient Contacts):

In this class, users will also honestly perform the routing protocol but fail to achieve the desirable results due to lack of sufficient contacts. Therefore, given the message m ∈Stask, an honest data forwarding in the presence of sufficient contacts could be determined if

$$m/ \in Sforward \text{ and } |R| == 0$$

or

$$m \in Sforward \text{ and } Nk(m) ==R \text{ and } |Nk(m)| == |R| < D$$

- Class III (A Misbehaving Data Forwarding with/without Sufficient Contacts):

A Misbehaving node will drop the packets or refuse to forward the data even when there are sufficient contacts, which could be determined by examining the following rules

$\exists m \in S_{task}, m / \in S_{forward}$ and $R != 0$ (7)

Or

$\exists m \in S_{task}, m \in S_{forward}$ and $N_k(m)$ R

Or

$\exists m \in S_{task}, m \in S_{forward}$ and $N_k(m) \subset R$ and $|N_k(m)| < D$

Note that Equation refers to the case that the forwarder refuses to forward the data even when the forwarding opportunity is available. The second case is that the forwarder has forwarded the data but failed to follow the routing protocol, which is referred to Equation . The last case is that the forwarder agrees to forward the data but fails to propagate the enough number of copies predefined by a multi-copy routing protocol, which is shown in Equation .

Next, we give the details of the proposed scheme as follows. In particular, TA judges if node Nj is a misbehavior or not by triggering the Algorithm 1. In this algorithm, we introduce BasicDetection, which takes j,Stask,Sforward, [t1,t2],R,D as well as the routing requirements of a specific routing protocol R,D as the input, and output the detection result "1" to indicate that the target node is a misbehavior or "0" to indicate that it is an honest node.

Algorithm 1 The Basic Misbehavior Detection algorithm

```
procedure BASICDETECTION((j,Stask,Sforward,[t1,t2],R,D))
  for Each m ∈Stask do
    if m/ ∈Sforward and R!=0 then
      return 1
    else if m ∈Sforward and Nk(m) R then
      return 1
    else if m ∈ Sforward and Nk(m) ⊂ R and |Nk(m)| < D then
      return 1
    end if
  end for
  return 0
end procedure
```

3.1.4 Misbehavior detection phase

iTrust introduce a periodically available Trust Authority(TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then TA could punish or compensate the node based on its behaviour. iTrust as the inspection game and use game theoretical analysis to demonstrate that TA could ensure theMisbehavior detection phase security of DTN routing at a reduced cost via choosing an appropriate investigation probability.

Probabilistic misbehavior detection scheme in DTNs

To reduce the high verification cost incurred by routing evidence auditing, in this section, we introduce a probabilistic misbehavior detection scheme, which allows the TA to launch the misbehavior detection at a certain probability. The advanced iTrust is motivated by the Inspection Game, a game theoretical model, in which an authority chooses to inspect or not, and an individual chooses to comply or not, and the unique Nash equilibrium is a mixed strategy, with positive probabilities of inspection and non-compliance.

We start from Algorithm 2, which 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. Ifi could pass the investigation by providing the corresponding evidences, TA will pay node i a compensation w; otherwise, i will receive a punishment C (lose its deposit).

In the next subsection, we will model the above described algorithm as an Inspection Game. And we will demonstrate that, by setting an appropriate detection probability threshold, we could achieve a lower detection overhead and still stimulate the nodes to forward the packets for other nodes.

Algorithm 2 The Proposed Probabilistic Misbehavior Detection algorithm

```
initialize the number of nodes n
for i ← 1 to n do
  generate a random number mi from 0 to 10n −1
  if mi/10n <p b then
    ask all the nodes (including node i) to provide evidence about node i
```

```
        if BasicDetection(i,Stask,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
```

The proposed algorithm itself incurs a low checking overhead. However, to prevent malicious users from providing fake delegation/forwarding/contact evidences, TA should check the authenticity of each evidence by verifying the corresponding signatures, which introduce a high transmission and signature verification overhead. We will give a detailed cost analysis in Section. In the following section, inspired by the inspection game, we will propose a probabilistic misbehavior detection scheme to reduce the detection overhead without compromising the detection performance.

Game Theory Analysis

Before presenting the detailed Inspection Game, we assume that the forwarding transmission costs of each node g to make a 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, which could be charged from source node similar . In the auditing phase, TA checks the node Ni with the probability pi 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).

3.2 PROPOSED SYSTEM

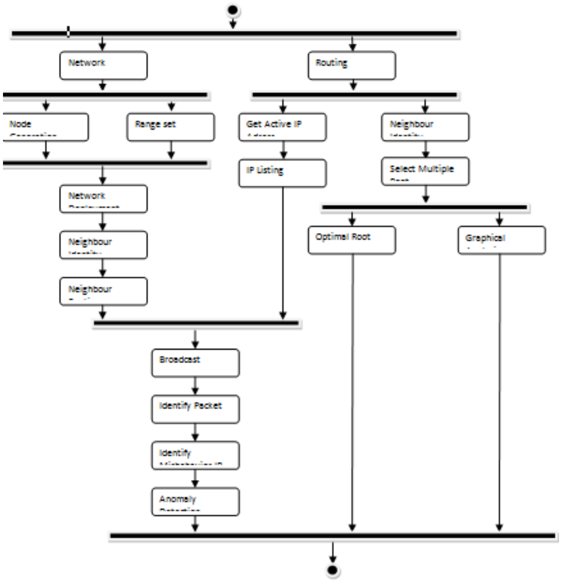
3.2.1 Optimization

Ant colony optimization algorithm is a probabilistic technique for solving computational problem which can be reduced to finding good path through graphs. Ant colony optimization algorithm was called ant system and its was aimed to solve find the shortest round-trips along the node. In this algorithm state they have fixed path. Choose the node exactly shortest distance and more traveled root. Ant colony optimization (ACO) is a population-based meta heuristic that can be used to find approximate solutions to difficult optimization problems. In ACO, a set of software agents called artificial ants search for good solutions to a given optimization problem.

Algorithm 3 Ant Colony Optimization

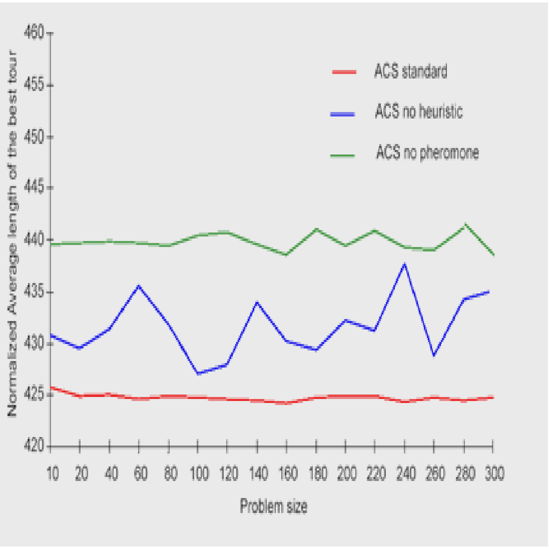
```
Procedure ACO1(source, destination) {
    assign initial positions to a set of ants(packets) at the given source;
    while(source != destination) {
        Procedure findnextnode(source) {
            check the routing table entries corresponding to the source
            if a link exists with the source {
                if (the node is already visited) {
                    cancel the node;
                else if (the node not already visited)
                    mark the node as eligible of being selection
                end if
            using the pheromone information,
            select a node from the list of eligible nodes;
            return the selected node;
            end if
        set newsource = selected node;
        source = newsource;
    end while
    update the pheromone table using the paths selected by the successful packets;
send a next set of packets(ants) guided by the information
left by all the previous visitor ants(packets);
```

ACTIVITY DIAGRAM



4 .PERFORMANCE EVALUATION

Pheromone trail and heuristic function:
are they useful?



Comparison between ACS standard, ACS with no heuristic (i.e., we set B=0), and ACS in which ants neither sense nor deposit pheromone. Problem: Oliver30. Averaged over 30 trials, 10,000/*m* iterations per trial.

5. CONCLUSION

Security has gained a lot of importance as network technology is widely used. Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). A misbehavior detection scheme in DTN is regarded as a great challenge. iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost.

The propose ant colony optimization for DTN routing towards efficient trust establishment. Ant Colony Optimization (ACO) with Optimized Link State Routing (OLSR) protocol to identify stable paths in between source and destination nodes. The work is divided in to five modules are network, routing, auditing, misbehavior detection and optimization. The proposed system has high performance, accuracy and speed.

REFERENCES

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots", in Proc. of IEEE INFOCOM'09, Rio de Janeiro, Brazil, April 19-25, 2009.

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

[3] Q. Li, S. Zhu, G. Cao, "Routing in Socially Selfish Delay Tolerant Networks" in Proc. of 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," in IEEE Transactions on Vehicular Technology,vol.58,no.8,pp.828-836,2009.

[5] E. Ayday, H. Lee and F. Fekri,"Trust Management and Adversary Detection for Delay Tolerant Networks," in Milcom'10, 2010.

[6] R. Lu, X. Lin, H. Zhu and X. Shen,"Pi: a practical incentive protocol for delay tolerant networks," in IEEE Transactions on Wireless Communications,vol.9,no.4,pp.1483-1493,2010.

[7] F. Li, A. Srinivasan and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets," in Proc. of IEEE INFOCOM'09, 2009.

[8] Fudenburg,"Game Theory",p17-18,example1.7:inspection game.

[9] M. Rayay, M. H. Manshaeiy, M. Flegyhziz, J. Hubauxy"Revocation Games in Ephemeral Networks" in CCS'08,2008

[10] S. Reidt, M. Srivatsa, S. Balfe,"The Fable of the Bees:Incentivizing Robust Revocation Decision Making in Ad Hoc Networks" in CCS'09, 2009

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

[12] S. Zhong, J. Chen, Y. R. Yang"Sprite: A Simple, Cheat-Proof, CreditBased System for Mobile Ad-Hoc Networks",in INFOCOM'03,2003.

[13] M. Dorigo, V. Maniezzo & A. Colorni, 1996. "Ant System: Optimization by a Colony of Cooperating Agents", IEEE Transactions on Systems, Man, and Cybernetics–Part B, 26 (1): 29–41.

[14] Beckers R., Deneubourg J.L. and S. Goss (1992). Trails and U-turns in the selection of the shortest path by the ant Lasius niger. Journal of theoretical biology, 159, 397-415.

[15] AntNet:ACO routing algorithm in practice: Vincent Verstraete, Matthias Strobbe, Erik Van

[16] M.Dorigo & T.Stiitzle, Ant Colony Optimization, MIT Press, 2004.

[17]Mcgraw-Hill's Advanced Topics in Computer Science Series, New Ideas in Optimization.