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. 5, May 2014, pg.76 – 82

RESEARCH ARTICLE

A MISBEHAVIOR DETECTION SCHEME ESTABLISHMENT IN DELAY TOLERANT NETWORKS

B.Sivakumar[1], J.Sandhiya[2]

Assistant Professor[1], P.G.Scholar[2]

sivablack@gmail.com [1], sandy27born@gmail.com [2]

Veltech Multitech Dr.Rangarajan Dr.Sakunthala Engineering College, Chennai, TamilNadu, India

ABSTRACT

Delay Tolerant Network(DTNs) are a class of unique network characterized like lack of guaranteed connectivity ,typically low frequency between DTN nodes and long propagation delay within the networks. Existing routing algorithms for DTN assumes that nodes are willing to forward packets for others but in real word selfish and malicious behaviors occurs while forward packets for nodes. Due to unique characteristics the message propagation process DTNs follows a Store-Carry and Forward manners. In this paper, we propose iTrust, probabilistic misbehavior detection schemes for secure and to improve the efficiency of DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing Trusted Authority (TA) to judge the nodes behavior based on the collected routing evidences and probabilistically checking. To further improve the performance of the proposed probabilistic inspection schemes, we introduce a reputation system. The extensive analysis and simulations result shows that the proposed schemes substantiate the effectiveness and efficiency of the proposed schemes.

Keywords- DTN, Selfish nodes, iTrust, Trusted Authority, Store –Carry and Forward

INTRODUCTION

Delay Tolerant Networks (DTNs) have the unique feature of intermittent connectivity, which makes routing quite different from other wireless networks. Since an end-to-end connection is hard to setup, store-carry-and-forward is used to deliver the packets to the destination. In the real world, most people are selfish; we have two observations from the social perspective. First, a selfish user is usually willing to help others with whom he has social ties (e.g., friends, coworkers, roommates) will be referred to as *social selfishness.* Second, for those with social ties, a selfish user may give *different* preferences will be referred to as *individual selfishness.* While forwarding packets [4,6] if connectivity is interrupted, then routing protocols would provide an alternative path after at most a transient outage. This is also assumed for emerging wireless Mobile Ad-hoc NETworks (MANETs).

For wireless networks with intermittent connectivity, also called Delay or Disruption Tolerant Networks (DTNs), lack of continuous connectivity, network partitioning and very long delays are actually the norm, not the exception. For example, the in-transit messages in DTNs, also called bundles, as shown in fig.1,could only be forwarded when two DTN nodes (N1, N*2*) move within each other's transmission range and contact with each other during a period of time. If no other DTN node is within the transmission range of DTN node N*1*, N*1*will buffer the current bundles and carry them until other DTN node appears within its transmission range. Therefore, the bundle propagation process in DTNs follows a "store-carry-and-forward" manner and the bundles are *opportunistically* routed toward the destinations by intermittent connections.

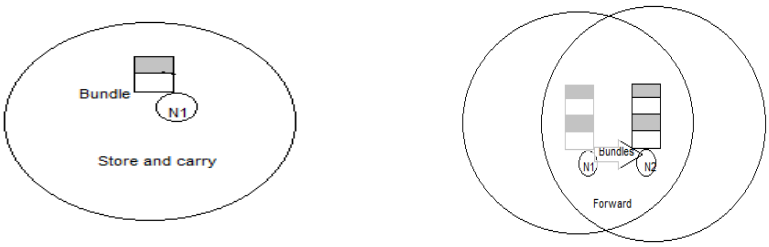

Fig. 1. Bundle store-carry-and-forward in DTNs.

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 in traditional mobile ad hoc networks use neighborhood monitoring or destination acknowledgement to detect packet dropping , and exploit credit-based and reputation-based incentive schemes. 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.

Recently, there are quite a few proposals for misbehaviors detection in DTNs , most of which are based on forwarding history verification (e.g., multi-layered credit , three-hop feedback mechanism , or encounter ticket), which are costly in terms of transmission overhead and verification cost. 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.

In this paper, we propose iTrust, a Probabilistic Misbehavior Detection Scheme for DTN, to adaptively detect misbehaviors in DTN and achieve the tradeoff between the detection cost and the detection performance. The proposed iTrust schemes are inspired from the *Inspection Game,* which is a game theory model in which an inspector verifies if another party, called inspectee, adheres to certain legal rules. Furthermore, the inspector could check the inspectee with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspectee must choose to comply the rules due to its rationality.

To further improve the performance of the proposed probabilistic inspection scheme, we introduce a reputation system, in which the inspection probability could vary along with the target node's reputation. Under the reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability.

The contributions of this paper can be summarized as follows.

- Firstly, we propose a general misbehavior detection framework based on a series of newly introduced data forwarding evidences. The proposed evidence framework could not only detect various misbehaviors but also be compatible to various routing protocols.
- Secondly, we introduce a probabilistic misbehavior detection scheme by adopting the Inspection Game. A detailed game theoretical analysis will demonstrate that the cost of misbehavior detection could be significantly reduced without compromising the detection performance. We also discuss how to correlate a user's reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability.
- Thirdly, we use extensive simulations as well as detailed analysis to demonstrate the effectiveness and the efficiency of the iTrust.

PERLIMINARY

In this section, we formulate the system model, routing model, threat model and design requirement.

A. System Model

We consider a normal DTN consisted of mobile devices owned by individual users. Each node

i is assumed to have a unique ID N_i and a corresponding public/private key pair. We assume that each node must pay a deposit *C* before it joins the network, and the deposit will be paid back after the node leaves if there is no offend activity of the node. Similar to [10], we assume that a periodically available TA exists so that it could take the responsibility of misbehavior detection in DTN. For a specific detection target N_i, TA will request N_i's forwarding history in the global network. Therefore, each node will submit its collected N_i's forwarding history to TA via two possible approaches. In a pure peer-to-peer DTN, the forwarding history could be sent to some special network components (e.g., roadside unit (RSU) in vehicular DTNs or judge nodes in via DTN transmission. In some hybrid DTN network environment, the transmission between TA and each node could be also performed in a direct transmission manner (e.g., WIMAX or cellular networks). We argue that since the misbehavior detection is performed periodically, the message transmission could be performed in a batch model, which could further reduce the transmission overhead.

B. Routing Model

We adopt the 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 multihop manner. Our misbehaving detection scheme can be directly used but not limited in metric-based routing algorithms, such as MaxProp and ProPHET.

C. Threat Model

First of all, we assume that each node in the networks is rational and a rational node's goal is to maximize its own profit. In this work, we mainly consider two kinds of DTN nodes: selfish nodes and malicious nodes. Due to the selfish nature and energy consuming, selfish nodes are not willing to forward bundles for others without sufficient rewarding. As an adversary, the malicious nodes arbitrarily drop others bundles (blackhole or greyhole attack), which often take place beyond others observation, leading to serious performance degradation. Note that any of the selfish actions above can be further complicated by the collusion of two or more nodes.

D. Design Requirements

The design requirements include

Distributed: We require that a network authority responsible for the administration of the network is only periodically available and consequently incapable of monitoring the operational minutiae of the network.

Robust: We require a misbehavior detection scheme that could tolerate various forwarding failures caused by various network environments.

Scalability: We require a scheme that works irrespective of the size and density of the network.

In the Routing Evidence Generation Phase, A forwards packets to B ,then gets the delegation history back. B holds the packet and then encounters C. C gets the contact history about B. In the Auditing Phase, when TA decides to check B, TA will broadcast a message to ask other nodes to submit all the evidence about B, then A submits the delegation history from B, B submits the forwarding history (delegation history from C), C submits the contact history about B.

A PROPOSED BASIC PMDS FOR DTN

In this section, we initially analyze the PMDS as a basic scheme, then we will explore the PMDS with a global reputation system.

A. Generation and Auditing of the Routing Misbehavior Detection Metrics

In the proposed misbehavior detection scheme, we further separate the whole misbehavior detection process into the Routing Evidence Generation Phase and Auditing phase.

1) Routing Evidence Generation Phase*:* For the simplicity of presentation, we take a three step data forwarding process as an example. Suppose that node A has packets to be delivered to node C. Now, if node A meets another node B that could help to forward the packets to C, A will replicate and forward the packets to B. Thereafter, B will forward the packets to C when C arrives at the transmission range of B. In this process, we define three kinds of data forwarding evidences which could be used to judge if a node is misbehavior or not:

1.a)Delegation Evidence D**:** After node A delegates the packet transmission task to B, B will generate a delegation evidence back to A, the evidence includes *D = fM; A; B; Dst; TS; Exp; Sig_Bg* , where M is the message, *TS* and *Exp* refer to the time stamp and the packets expiration date of the packets, respectively, *Dst* is the packets destination, Sig_B refers to the signature generated by *B*. So D_B is the set of routing tasks of *B*, which will be stored at node A.

1.b)Forwarding History Evidence F: If node B successfully forward the packets to node C, C will generate a forwarding history evidence to demonstrate that B has successfully finished a forwarding task. F fM; B; C; Dst; TS; Exp; SigC g, where SigC refers the signature generated by node C to demonstrate the authenticity of this evidence. *F* is stored at node B.

1.c)Contact History Evidence E**:** Whenever B meets a new node E, a new contact history evidence will be generated to demonstrate the contact of B and E as *fB; E; TS; Sig_B; Sig_Eg*, where Sig_B refers to the signature generated by both of node B and E to demonstrate the authenticity of this evidence. Note that *E* will be stored at both of node B and E.

2) Auditing Phase*:* In the Auditing phase, TA will launch an investigation request towards node *B* in the global net-work. Then, each node will submit its collected Delegation Evidences and contact history evidences to TA. Node B will also submit its forwarding history evidences to TA. Note that Delegation Evidence represents the forwarding tasks, Contact History Evidence records the network environment constraints, and Forwarding History Evidence demonstrates the real data forwarding performed by node B. If B is an honest node, he will try his best to finish the forwarding tasks. So if we don't consider network constraints, *F* should fully match Delegation Task *D*. However, in reality, node *B* may fail to finish all of the tasks due to the network constraints (e.g., lack of enough contacts).

Algorithm 1: Judge (node *i*)

1: demand all the nodes (including node *i*) to provide evidence *D; E; F* about node *i*

2: *W*=Find(*Delegation Evidence D*, *Contact History Evidence E*, *Routing Protocol R*)
3: if *F* == *W* then

4: return 1
5: else

6: return 0
7: end if

THE ADVANCED ITRUST: A 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.

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 to [4]. In the auditing phase, TA checks the node N_i 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).

CONCLUSION

I propose a Probabilistic Misbehavior Detection Scheme (iTrust), which could reduce the detection overhead effectively. We model it as the Inspection Game and show that an appropriate probability setting could assure the security of the DTNs at a reduced detection overhead. My results confirm that iTrust will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively

REFERENCES

[1]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.

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

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

[5] 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.*

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

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

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

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

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

