International Journal of Advanced Technology in Engineering and Science
Vol. No.3, Special Issue No. 01, August 2015
www.ijates.com
ijates
ISSN 2348 - 7550

PMDS: A PROBABILISTIC MISBEHAVIOR DETECTIONSCHEME IN DTN

Jyothi D B[1], Naveen G[2]

[1]M.Tech Student, [2]Assistant Professor Dept. of Computer Science and Engineering, STJIT, Ranebennur, Karnataka, (India)

ABSTRACT

Malicious and selfish behaviors represent a serious threat against routing in Delay or Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN represents a great challenge. In this paper, we propose PMDS, a probabilistic misbehavior detection scheme, for secure DTN routing. The basic idea of PMDS is introducing a periodically available Trusted Authority (TA), which judges the node's behavior based on the collected routing evidences. We model PMDS 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 a node's reputation. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.

Keywords: DTN, Security, Punishment and Compensation, Inspection Probability.

I. INTRODUCTION

Current networking protocols have been programmedwith the assumption that an end-to-end path between thepacket source and the destination is almost alwaysaccessible. If connectivity isdisturbed, 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). However, there is an entire class of wireless networks for which this assumption does not hold. For wireless networks with intermittent connectivity, also called Delay or Disruption Tolerant Networks (DTNs), absenceof endlessconnectivity, network partitioning and very long delays are actually the norm, not the exception. Such networks have recently received an increasing interest due to their greatpotential for supporting applications deployed in testedenvironments, such as vehicular networks [1], wireless social networks [2].

A Byzantine opponent (i.e., a physically captured and controlled legitimate node) can doserious damage to the network in terms of data availability,latency, and throughput. The typical examples of Byzantine attack include dropping, varying the legitimate packets and injecting falsepackets. Further, even for the non-malicious nodes, the sane(selfish) nodes may also try to maximize their own benefits by relishing the services provided by the DTN network and, at the same time, refusing to relay thebundles for others [4].

II. BACKGROUND

Most of prevailing works are based on forwarding history verification, (e.g. multi-layered credit [4], [5], three-hop feedback mechanism [3]), which are expensive in terms of transmission expenses and verification cost. The security overhead incurred by forwarding history checking is critical for a DTN since expensive security operations will be transformed into more energy consumptions, which denotes a fundamental challenge in resource-constrained DTN. Further, even from the Trusted Authority (TA) point of view, misbehavior detection in DTNs will unsurprisingly incur a high security overhead, which may include the cost of collecting the forwarding history evidence via deployed *judge nodes* [3] and transmission cost to TA.

III. RELATED WORK

We propose PMDS, 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. PMDS is motivated from the *Inspection Game*, which is a game theory model in which an inspector verifies if an another party, called inspectee, adheres to certain legal rules. In this model, the inspectee has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification resources. Therefore, the inspector could take advantage of partial verification and corresponding punishment to discourage the misbehaviors of inspectees.

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.

IV. SCOPE OF THE PROJECT

In this paper, we adopt the system model similar to normal DTN consisting of mobile devices owned by individual users. Each node *i* is assumed to have a unique ID *Ni* 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. Here 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 *Ni*, TA will request *Ni*'s forwarding history in the global network. Therefore, each node will submit its collected *Ni*'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 judgenodes in [4]) via DTN transmission.

4.1 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 amultihop manner. Our misbehaving detection scheme can be directly used but not limited in metric-based routing algorithms.

4.2 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 ownprofit. 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.

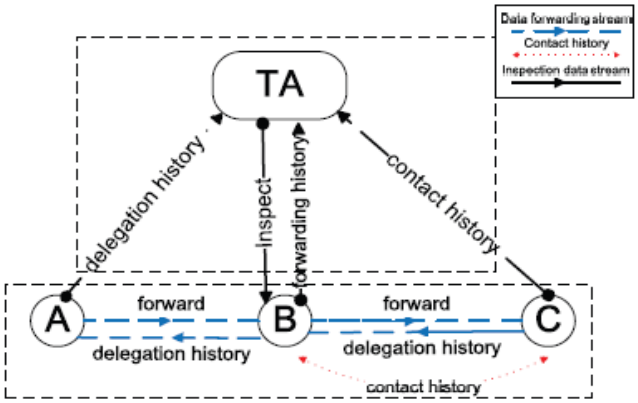


Fig. 1. In the Routing Evidence Generation Phase, A forwards packets to B ,then gets the delegation history back. B holds the packet and then encounters C. C gets the contact history about B. In the Auditing Phase, when TA decides to check B, TA will broadcast a message to ask other nodes to submit all 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.

4.3 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.

V. PROPOSED METHODOLOGY

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.

5.1 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 an 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 a misbehaviour or not:

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

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; SigCg, where SigC refers to the signature generated by node C to demonstrate the authenticity of this evidence. F is stored at node B.

Contact History Evidence E: Whenever B meets a new node E, new contact history evidence will be generated to demonstrate the contact of B and E as fB;E; TS; SigB; SigEg, where SigB 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.

Algorithm 1: Judge(node i)

1: demand all the nodes (including node i) to provide evidence $\mathcal{D}, \mathcal{E}, \mathcal{F}$ about node i
2: $\mathcal{W}$=**Find**(*Delegation Evidence* $\mathcal{D}$, *Contact History Evidence* $\mathcal{E}$, *Routing Protocol* $\mathcal{R}$)
3: **if** $\mathcal{F} == \mathcal{W}$ **then**
4: return 1
5: **else**
6: return 0
7: **end if**

Algorithm 1: Judge(node i)

5.2. The Basic Probabilistic Misbehavior Detection Scheme

Different from periodical detection, the proposed PMDS allows the TA to launch the misbehavior detection at a certain probability. Algorithm 2 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* (lose its deposit).

Algorithm 2: Basic PMDS

```
1: initialize the number of nodes n
2: for i ← 1 to n do
3:    generate a random number m_i from 1 to 10^n − 1
4:    if m_i/10^n < p_b then
5:       ask all the nodes (including node i) to provide
         evidence about node i
6:       if Judge(node i)==1 then
7:          pay node i the compensation w
8:       else
9:          give a punishment C to node i
10:      end if
11:   else
12:      pay node i the compensation w
13:   end if
14: end for
```

Algorithm 2: Basic PMDS

5.3 Game Theory Analysis

Here we assume that the forwarding transmission costs each node *g* to forward a packet and, thus, 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 [5]. In the auditing phase, TA checks each node with the same probability *pb*. Since checking willincur a transmission cost *h*, TA has two strategies, inspecting (I) or not inspecting (N). Each node also has two strategies, forwarding (F) and offending (O).

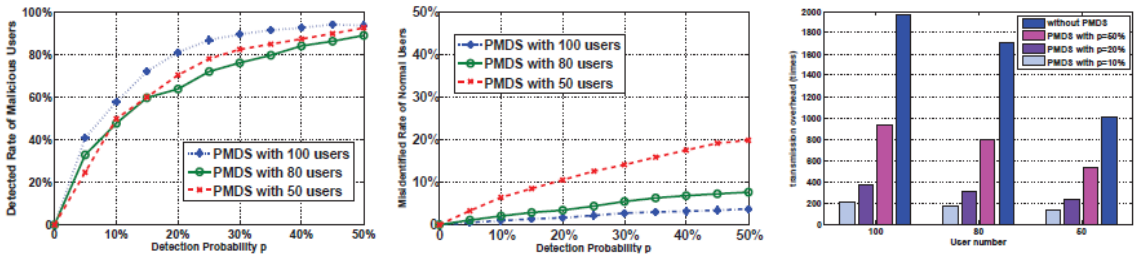
5.4 Inspection Based on Reputation

The previous analysis has shown that the basic PMDS is enough to assure the security. However, the basic scheme assumes the same detection probability for each node, which may not be desirable in practice. It is observed that a good node could be detected less frequently while a bad node should be inspected at a higher probability. Therefore, we could combine PMDS with a reputation system which correlates the detection probability with nodes' reputation.

VI. SIMULATION OF PMDS

We set up the experiment environment with the Opportunistic Networking Environment (The ONE) simulator, which is designed for evaluating DTN routing and application protocols. In our experiment, we adopt the First Contact routing protocol, which is a single-copy routing mechanism, and we use our campus map as the experiment environment.

Fig. 2. Experiment results with user number of 100, 80, 50



(a) Detected rate of malicious nodes (b) false rate of misidentified nodes (c) Transmission overhead incurred by PMDS

We use the Packet Loss Rate (PLR) to describe the misbehavior level of a malicious node. In DTN, when a node'sbuffer is depleted, a new received bundle will be dropped by the node, and PLR denotes the rate between dropped bundles and received bundles. But a malicious node will pretend no more buffer for others and drop all the bundles it received. Thus PLR actually denotes a node's misbehavior level, e.g. if a node's PLR is 1, it is totally a malicious node; if a node's PLR is 0, we take it as a normal node.

In our experiment, we set PLR=1. On the other hand, since a normal node may also be identified as malicious due to the depletion of its buffer, so we need to measure the false rate of such misidentified nodes to prove that PMDS has little impact on the normal users who adhere to the security and routing protocols.

Finally, as we claimed, PMDS will incur a much lower transmission overhead than the system without PMDS, so we will evaluate and compare the transmission times of the system with and without PMDS.

VII. CONCLUSION

In this paper, we propose a Probabilistic Misbehavior Detection Scheme (PMDS), 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. Our simulation results confirm that PMDS will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively. Our future work will focus on the extension of PMDS to other kinds of networks.

VIII. ACKNOWLEDGEMENT

I consider it is a privilege to express my gratitude and respect to all those who guiding me in the progress of my paper.

I wish my grateful thanks to **Mr. Naveen G, M.Tech,** project guide, for his invaluable support and guidance.

JYOTHI D B

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 IEEEINFOCOM'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] E. Ayday, H. Lee and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," in Milcom'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] R. Lu, X. Lin, H. Zhu and X. Shen, "Pi: a practical incentive protocol for delay tolerant networks," in IEEE Transactions on WirelessCommunications,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 IEEEINFOCOM'09, 2009.

[7] D. Fudenburg and J. Tirole, "Game Theory," p17-18, The MIT Press, Cambridge, Massachusetts, London, England.

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

BIOGRAPHY

Jyothi D B is a student pursuing her Master degree in Computer Science and Engineering department at STJ Institute of Technology, Ranebennur, Karnataka, India. Her research interests are Computer Science related aspects such as Networking technology, Java programming language and web 2.0.

Naveen G is an Assistant Professor in the department of Computer Science and Engineering at STJ Institute of Technology, Ranebennur, Karnataka, India. He received his Master degree in Computer Networks. His research interests are related to computer networks.

ijates
ISSN 2348 - 7550