THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

A Secured iTrust Key towards Periodic Trust Establishment in Delay Tolerant Networks

H. Bharani
Assistant Professor, Department of Information Technology
Karpaga Vinayaga College of Engineering Technology
Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram, Tamil Nadu, India
M. Kanchana
Professor, Department of Information Technology
Karpaga Vinayaga College of Engineering Technology
Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram, Tamil Nadu, India
V. Kavitha
Assistant Professor, Department of Information Technology
Karpaga Vinayaga College of Engineering Technology
Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram, Tamil Nadu, India
S. B. Dhivya
Assistant Professor, Department of Information Technology
Karpaga Vinayaga College of Engineering Technology
Chinna Kolambakkam, Madurantakam Taluk, Kanchipuram, Tamil Nadu, India
I. Vinnarasi Tharania
Assistant Professor, Department of Information Technology
Karpaga Vinayaga College of Engineering Technology

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 Delay/Disruption Tolerant Networks (DTNs) is regarded as a great challenge. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure Delay/Disruption Tolerant Networks (DTNs) 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, Trusted Authority (TA) could ensure the security of Delay/Disruption Tolerant Networks (DTNs) 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. Related Works

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) [1], 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] [3]. 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) [4].This research is supported by National Natural Science Foundation of China (Grant No.61003218, 70971086, 61272444, 61161140320, 61033014), Doc- toral Fund of Ministry of Education of China (Grant No.20100073120065). H. Zhu, Z. Gao, and Z. Cao are with Computer Science Department of Shanghai Jiao Tong University (e-mail:{zhu-hj, zhaoyu, zfcao}@sjtu.edu.cn). S. Du is with Antai College of Economics & Management of Shanghai Jiao Tong University (e-mail: sgdu@sjtu.edu.cn). M. Dong is with The University of Aizu. (e-mail: mx.dong@ieee.org).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 [4], [17]. 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 neigh- borhood monitoring or destination acknowledgement to detect packet dropping [20], and exploit credit-based and reputation- based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes [4], [6]. 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 [4]. 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 [7]. 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. Recently, there are quite a few proposals for misbehaviors detection in DTNs [4]–[7], most of which are based on forwarding history verification (e.g., multi-layered credit [4], [6], three-hop feedback mechanism [5], or encounter ticket [7], [18]), which are costly in terms of transmission overhead and verification cost. The security overhead incurred by forwarding history checking is critical for a DTN since expensive security operations will be translated into more energy consumption- s, which represents a fundamental challenge in resource- constrained DTN.

2. Proposed Method

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 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. For data Security, we used the RSA algorithm and Hash function for User Authentication.

Advantages

- Data forwarding scheme
- Inspection game
- RSA and Hash function for more security

2.1 Modules Description

2.1.1. DTN Network Formation

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 multi-hop manner. For the simplicity of presentation, we take a three-step data forwarding process as an example. Suppose that node A has packets, which will 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. They are Delegation Task Evidence, Forwarding History Evidence and Contact History Evidence.

2.1.2. Route Discovery and Data Forwarding

A normal user will honestly follow the first routing protocol by forwarding the messages as long as there are enough contacts. 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.

2.1.3. Trust Authority I-Scheme

The tradeoff between the security and detection cost, iTrust introduces 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 behaviors. 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. We model iTrust as the Inspection Game and use game theoretical analysis to demonstrate that TA could ensure the security of DTN routing at a reduced cost via choosing an appropriate investigation probability.

3. Output Analysis

3.1 Node Creation

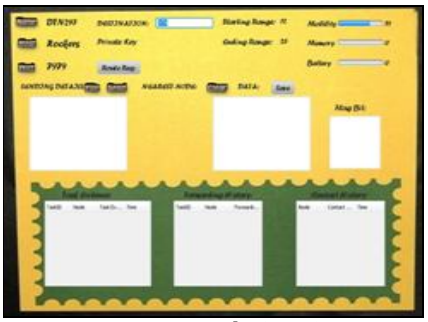

Figure 3.1 Node Creation

3.2. Trusted Authority

Figure 3.2 Trusted Authority

3.3. Key Sharing

Figure 3.3 Key Sharing

3.4. Path Selection

Figure 3.4 Path Selection

3.5. Data Forwarding

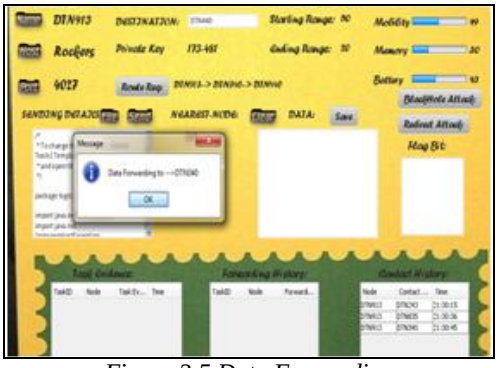

Figure 3.5 Data Forwarding

3.6. Set the Private Key value

Figure 3.6 Set the Private Key value

3.7. Data Receiver

Figure 3.7 Data Receiver

3.8. Black Nodes Notification bar

Figure 3.8 Black Nodes Notification bar

3.9. Data Redirect to Source

Figure 3.9 Data Redirect to Source

3.10. Inspection Game

Figure 3.10 Inspection Game

4 Conclusion

We proposed 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. Our simulation results confirm that iTrust will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively. Our future work will focus on the extension of iTrust to other kinds of networks.

5 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 pro- tocol 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, Credit- Based System for Mobile Ad-Hoc Networks",in INFOCOM'03,2003.
13. J. Douceur,"The sybil attack" in IPTPS,2002.

14. R. Pradiptyo"Does Punishment Matter? A Refinement of the Inspection Game",in German Working Papers in Law and Economics,Volume 2006,Paper 9.
15. J. Burgess, B. Gallagher, D. Jensen and B. Levine. "Maxprop: Routing for vehicle-based disruption-tolerant networks." In Proc. of IEEE INFO- COM'06, 2006.
16. A. Lindgren and A. Doria." Probabilistic Routing Protocol for Intermit- tently Connected Networks." draft-lindgren-dtnrg-prophet-03, 2007.
17. W. Gao and G. Cao "User-centric data dissemination in disruption tolerant networks", in Proc. of IEEE INFOCOM, 2011.
18. A. Keranen, J. Ott, T. Karkkainen."The ONE Simulator for DTN Protocol Evaluation," in SIMUTools 2009, Rome, Italy