Middle-East Journal of Scientific Research 20 (11): 1413-1416, 2014
ISSN 1990-9233
© IDOSI Publications, 2014
DOI: 10.5829/idosi.mejsr.2014.20.11.1049

Malicious Packet Loss During Routing Misbehavior-Identification

[1]K.P. Kaliyamurthie, [2]D. Parameswari and [3]R. Udayakumar

[1]Bharath University, Chennai-600073, India
[2]Department of MCA, Jerusalem College of Engineering, Chennai, India
[3]Department of Information Technology, Bharath University, Chennai-600073, India

Abstract: Defending the data from malicious attacks is an important yet demanding security issue. In this paper, we describe clarification for such network that protects both the routing and data forwarding functions. It guards the data by detecting and reacting to the malicious nodes. Although methods have been proposed to mitigate routing misbehavior in mobile ad hoc networks, they cannot be directly applied to DTNs because of the flashing connectivity between nodes. To overcome the problem, we propose a scheme to detect packet dropping in DTNs. In our proposal, a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since unruly nodes may misreport their contact records to avoid being detected, a small part of each contact record is scattered to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. We address a scheme to mitigate routing misbehavior by off-putting the number of packets forwarded to the misbehaving nodes. Trace-driven simulations show that our solutions are efficient and can effectively mitigate routing misbehavior.

Key words: Protection · Disruption tolerant networks · Mitigation · Routing misbehavior · Security

INTRODUCTION

Disruption Tolerant Networks (DTNs) consist of mobile nodes which contact each other opportunistically. Due to the low node density and unpredictable node mobility, only intermittent network connectivity exists in DTNs and the subsequent difficulty of maintaining end-to-end communication links advances "carry-and-forward" approaches for data delivery. More specifically, node mobility is exploited to let mobile nodes physically carry data as relays and forward data opportunistically upon contact with others.

In this paper, we focus on securing the packet delivery functionality because it is the premise for the multihop connectivity between two faraway nodes. Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets. For example, the malicious nodes can announce incorrect routing updates which are then propagated in the network, or drop all the packets passing through them. Several recent studies [1-4] have provided detailed description on such network-layer security threats and their consequences.

We address routing misbehavior in DTNs by answering two questions: how to detect packet dropping and how to limit the traffic flowing to the misbehaving nodes. We first propose a scheme which detects packet dropping in a distributed manner. In this scheme, a node is required to keep previous signed contact records such as the buffered packets and the packets sent or received and report them to the next contact node which can detect if the node has dropped packets based on the reported records. Misbehaving nodes may falsify some records to avoid being detected, but this will violate some consistency rules. To detect such inconsistency, a small part of each contact record is disseminated to some selected nodes which can collect appropriate contact records and detect the misbehaving nodes with certain probability. Then we propose a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes.

Corresponding Author: K.P. Kaliyamurthie, Bharath University, Chennai-600073, India.

This paper is structured as follows. Section II reviews related work. Section III introduces our Preliminaries. Section IV presents the packet dropping detection scheme. Section V concludes the paper.

Related Work: In mobile ad hoc networks, much work has been done to detect packet dropping and mitigate routing misbehavior. To detect packet dropping, Marti *et al.* proposed watchdog-based solutions in which the sending node operates in promiscuous mode and overhears the medium to check if the packet is really sent out by its neighbour. Some follow-up works [5], have used this neighbourhood monitoring approach to detect packet dropping. However, neighbourhood monitoring relies on a connected link between the sender and its neighbour, which most likely will not exist in DTNs. In DTNs, a node may move away right after forwarding the packet to its neighbour and thus cannot overhear if the neighbour forwards the packet.

Another line of work uses the acknowledgement (ACK) packet [6-8] sent from the downstream node along the routing path to confirm if the packet has been forwarded by the next hop. Liu *et al.* [6] proposed a 2ACK scheme in which the sending node waits for an ACK from the next hop of its neighbour to confirm that the neighbour has forwarded the data packet. However, this technique is vulnerable to collusions, i.e., the neighbour can forward the packet to a colluder which drops the packet. Although end-to-end ACK schemes [8] are resistant to such colluding attacks, the ACK packets may be lost due to the opportunistic data delivery in DTNs. Moreover, in routing protocols where each packet has multiple replicas, it is difficult for the source to verify which replica is acknowledged since there is no persistent routing path between the source and destination in DTNs.

To mitigate routing misbehavior, existing works [9, 5, 6] in mobile ad hoc networks reduce the traffic flowing to the misbehaving nodes by avoiding them in path selection. However, they cannot be directly applied to DTNs due to the lack of persistent path.

In DTNs, serious routing misbehavior is the black hole attack, in which a black hole node advertises itself as a perfect relay for all destinations, but drops the packets received from others. Li *et al.* [8] proposed an approach that prevents the forgery of routing metrics. However, if the black hole node indeed has a good routing metric for many destinations, their approach will not work, but our approach still works by limiting the number of packets forwarded to the black hole node. Another related attack is the wormhole attack, which has been recently addressed by Ren *et al.* [10].

To address selfish behaviours, Shevade *et al.* proposed a gaming-based approach [11] and Chen *et al.* [12] proposed credit-based approach which provides incentives for selfish nodes to forward packets. Li *et al.* proposed a social selfishness aware routing algorithm to allow user selfishness and provide better routing performance in an efficient way. Our work is complementary since besides dealing with selfish routing we also consider the misbehavior of malicious nodes whose goal is not to maximize their own benefits but to launch attacks.

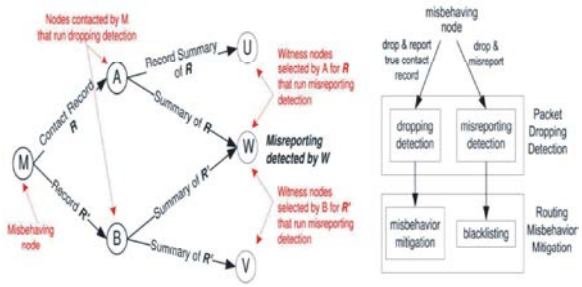
Our solution has some similarity with previous work (e.g., [12]) on detecting node clone attacks in sensor networks, since both detect the attacker by identifying some inconsistency. However, our work relies on a different kind of inconsistency in DTNs and DTNs do not have the reliable link connection used in existing solutions for node clone attacks.

Preliminaries

Network and Routing Model: Similar to many other works (e.g., [2]), we assume each node has two separate buffers. One has unlimited space and is used to store its own packets; the other one has limited space and is used to store packets received from other nodes. We assume the network is loosely synchronized; i.e., any two nodes should be in the same time slot at any time. Since the intercontact time is usually at the scale of minutes or hours, the time slot can be at the scale of one minute. Thus, such loose time synchronization is not hard to achieve.

Security Model: There are two types of nodes: *misbehaving nodes* and *normal nodes*. A misbehaving node drops the received packets even if it has available buffers, but it does not drop its own packets. It may also drop the control messages of our detection scheme. We assume a small number of misbehaving nodes may collude to avoid being detected and they may synchronize their actions via out-band communication channels. A normal node may drop packets when its buffer overflows, but it follows our protocol. In some DTN applications, each packet has a certain lifetime and then expired packets should be dropped whether or not there is buffer space. Such dropping can be identified if the expiration time of the packet is signed by the source. Such dropping is not misbehavior and will not be considered in the following presentations.

We assume a public-key authentication service is available. For example, hierarchical identity-based cryptography [13] has been shown to be practical in



DTNs [14]. In identity-based authentication, only the offline trusted private key generator can generate a public/private key pair, so a misbehaving node itself cannot forge node identifiers (e.g., to launch Sybil attacks) [15-20]. Generally speaking, a node's private key is only known by itself; however, colluding nodes may know each other's private key.

Overview of Our Approach: Our approach consists of a packet dropping detection scheme and a routing misbehavior mitigation scheme. Fig. 2(a) illustrates our basic approach for misbehavior detection.

The misbehaving node [in Fig. (a)] is required to generate a *contact record* during each contact and report its previous contact records to the contacted node [and in Fig. (a)]. Based on the reported contact records, the contacted node detects if the misbehaving node has dropped packets. The misbehaving node may misreport (i.e., report forged contact records) to hide its misbehavior, but forged records cause inconsistencies which make misreporting detectable. To detect misreporting, the contacted node also randomly selects a certain number of *witness nodes* for the reported records and sends a summary of each reported record to them when it contacts them. The witness node

[in Fig. (a)] that collects two inconsistent contact records can detect the misreporting node.

Fig. (b) illustrates our approach for routing misbehavior mitigation. It reduces the data traffic that flows into misbehaving nodes in two ways: 1) If a misbehaving node misreports, it will be blacklisted (after the misreporting is detected) and will not receive any packet from other nodes; 2) if it reports its contact records honestly, its dropping behavior can be monitored by its contacted nodes and it will receive much less packets from them.

Packet Dropping Detection

Basic Idea: When two nodes contact, they generate a *contact record* which shows when this contact happens, which packets are in their buffers before data exchange and what packets they send or receive during the data exchange. The record also includes the unique sequence number that each of them assigns for this contact. The record is signed by both nodes for integrity protection [21-25]. A misbehaving node may report a false record to hide the dropping from being detected. However, misreporting will result in inconsistent contact records generated by the misbehaving node. To detect misreporting, for each contact record that a normal node generates with (or receives from) other nodes, the normal node selects witness nodes and it transmits the record summary to them. The summary only includes a part of the record necessary for detecting the inconsistency caused by misreporting. With some probability, the summaries of two inconsistent contact records will reach a common witness node which will detect the misreporting node.

Packet Dropping Detection: In a contact, each of the two contacting nodes reports its previous contact record [see (1)] to the other node. In this contact, the two nodes also exchange their current vector of buffered packets (as a step of contact record generation). In this way, one node knows the two sets of packets the other node buffers at the beginning of the previous contact and the beginning of the current contact, which are denoted by and, respectively.

Misreporting Detection: Suppose a misbehaving node has dropped some packets. To hide the dropping from being detected by the next contacted node, will not report the true record of the previous contact. However, when there is no collusion, cannot modify the true record since it is signed by the previous contacted node. Also, cannot forge a contact record because it does not know the private key of any other node. Thus, the only misreporting it can perform is to replay an old record generated before the previous contact

CONCLUSION

In this paper, we presented a scheme to detect packet dropping in DTNs. The detection scheme works in a distributed way; i.e., each node detects packet dropping locally based on the collected information. Moreover, the detection scheme can effectively detect misreporting even when some nodes collude. Analytical results on detection probability and detection delay were also presented. Based on our packet dropping detection scheme, we then proposed a scheme to mitigate routing misbehavior in DTNs. The proposed scheme is very generic and it does not rely on any specific routing

algorithm. Trace-driven simulations show that our solutions are efficient and can effectively mitigate routing misbehavior.

REFERENCES

1. Fall, K., 2003. The delay-tolerant network architecture for challenged internets, in Proc. SIGCOMM, pp: 27-34.
2. Burgess, J., B. Gallagher, D. Jensen and B. Levine, 2006. Maxprop: Routing for vehicle-based disruption-tolerant networks, in Proc. IEEE INFOCOM, pp: 1-11.
3. Gao, W. and G. Cao, 2011, User-centric data dissemination in disruption tolerant networks, in Proc. IEEE INFOCOM, pp: 3119-3127.
4. Daly, E. and M. Haahr, 2007. Social network analysis for routing in disconnected delay-tolerant manets, in Proc. ACM MobiHoc, pp: 32-40.
5. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. Mitigating routing misbehavior in mobile ad hoc networks, in Proc. ACM MobiCom, pp: 255-265.
6. Xue, Y. and K. Nahrstedt, 2004. Providing fault-tolerant ad-hoc routing service in adversarial environments, Wireless Pers. Commun., 29(3-4): 367-388.
7. Hui, P., J. Crowcroft and E. Yoneki, 2008. Bubble rap: Social-based forwarding in delay tolerant networks, in Proc. ACM MobiHoc, pp: 241-250.
8. Li, F., A. Srinivasan and J. Wu, 2009. Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets, in Proc. IEEE INFOCOM, pp: 2428-2436.
9. Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs, IEEE Trans. Mobile Comput., 6(5): 536-550.
10. Shevade, U., H. Song, L. Qiu and Y. Zhang, 2008. Incentive-aware routing in dtns, in Proc. IEEE ICNP, pp: 238-247.
11. Chen, B. and C. Choon, 2010. Mobicent: A credit-based incentive system for disruption tolerant network, in Proc. IEEE INFOCOM, pp: 1-9.
12. Parno, B., A. Perrig and V. Gligor, 2005. Distributed detection of node replication attacks in sensor networks, in IEEE Symp. Security and Privacy, pp: 49-63.
13. Gentry, C. and A. Silverberg, 2002. Hierarchical id-based cryptography, in Proc. Int. Conf. Theory and Application of Cryptography and Information Security, pp: 548-566.
14. Seth, A., D. Kroeker, M. Zaharia, S. Guo and S. Keshav, 2006. Lowcost communication for rural internet kiosks using mechanical backhaul, in ACM Proc. Mobicom, pp: 334-345.
15. Erramilli, V., A. Chaintreau, M. Crovella and C. Diot, 2008. Delegation forwarding, in Proc. ACM MobiHoc, pp: 251-260.
16. Eagle, N. and A. Pentland, 2006. Reality mining: Sensing complex social systems, Pers. Ubiquitous Comput., 10(4): 255-268.
17. Burgess, J., G.D. Bissias, M. Corner and B.N. Levine, 2007. Surviving attacks on disruption-tolerant networks without authentication, in Proc. ACM MobiHoc, pp: 61-70.
18. Awerbuch, B., D. Holmer, C.N. Rotaru and H. Rubens, 2002. An on-demand secure routing protocol resilient to byzantine failures, in Proc. ACM WiSe, pp: 21-30.
19. Ren, Y., M.C. Chuah, J. Yang and Y. Chen, 2010. Detecting wormhole attacks in delay tolerant networks, IEEEWireless Commun.Mag., 17(5): 36-42.
20. Gao, W. and G. Cao, 2010. On exploiting transient contact patterns for data forwarding in delay tolerant networks, in Proc. IEEE ICNP, pp: 193-202.
21. Irurhe, N.K., S.B. Raji, O.A. Olowoyeye, A.O. Adeyomoye, R.A. Arogundade, K.O. Soyebi, A.Z. Ibitoye, L.C. Abonyi and F.J. Eniyandunni, 2012. Knowledge and Awareness of Breast Cancer among Female Secondary School Students in Nigeria, Academic Journal of Cancer Research, 5(1): 01-05.
22. Kabita Lahkar and Rita Mahanta, 2012. Status of Thyroid Hormone During 3-Methylcholanthrene Induced Carcinogenesis with Thyroid Stress, Academic Journal of Cancer Research, 5(1): 06-10.
23. Achenef, M.B. and A.K. Arifah, 2012. Cytotoxic Effects of Conjugated Linoleic Acids on Human Breast Cancer Cells (MCF7) Academic Journal of Cancer Research, 5(1): 11-16.
24. Jagadeeswaran, M., N. Gopal, B. Jayakar and T. Sivakumar, 2012. Simultaneous Determination of Lafutadine and Domperidone in Capsule by High Performance Liquid Chromatography, Global Journal of Pharmacology, 6(2): 60-64.
25. Yogeswari, S., S. Ramalakshmi, R. Neelavathy and J. Muthumary, 2012. Identification and Comparative Studies of Different Volatile Fractions from Monochaetia kansensis by GCMS, Global Journal of Pharmacology, 6(2): 65-71.