Computer Communications 71 (2015) 111–118

Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Catabolism attack and Anabolism defense: A novel attack and traceback mechanism in Opportunistic Networks

Majeed Alajeely*, Robin Doss, Asma'a Ahmad, Vicky Mak-Hau

School of Information Technology, Deakin University, Geelong, Australia

ARTICLE INFO

Article history:
Received 19 June 2014
Revised 9 October 2015
Accepted 10 October 2015
Available online 22 October 2015

Keywords:
Opportunistic Networks
Security
Packet dropping attacks
Denial-of-service
Malicious node detection

ABSTRACT

Security is a major challenge in Opportunistic Networks (OppNets) because of its characteristics, such as open medium, dynamic topology, no centralized management and absent clear lines of defense. A packet dropping attack is one of the major security threats in OppNets since neither source nodes nor destination nodes have the knowledge of where or when the packet will be dropped. In this paper, we present a novel attack and traceback mechanism against a special type of packet dropping where the malicious node drops one or more packets and then injects new fake packets instead. We call this novel attack a Catabolism attack and we call our novel traceback mechanism against this attack Anabolism defense. Our novel detection and traceback mechanism is very powerful and has very high accuracy. Each node can detect and then traceback the malicious nodes based on a solid and powerful idea that is, hash chain techniques. In our defense techniques we have two stages. The first stage is to detect the attack, and the second stage is to find the malicious nodes. Simulation results show this robust mechanism achieves a very high accuracy and detection rate.

1. Introduction

Opportunistic Networks (OppNets) refer to a number of wireless nodes that opportunistically communicate with each other in the form of "Store-Carry-Forward" when they come into contact with each other without proper network infrastructure. Due to these characteristics, OppNets have gained significant research attention due to the security and privacy challenges that have emerged. A packet dropping attack is one of the major security threats in OppNets. It can be classified as a denial of service attacks (DoS) where the malicious node drops all or some of the packets. This attack is one of the most difficult DoS attacks since neither source node nor the destination node has the knowledge of where or when the packet will be dropped. Packet dropping can degrade the performance of the network and may obstruct the propagation of sensitive data. It is a significant challenge to deal with such an attack since the unreliable wireless communication and resource limitations can result in communication failure and result in the wrong prediction about the presence of a packet dropping attack. Moreover, a node's resources, such as energy and bandwidth can be the real reasons behind packet dropping. A power shortage or communication failure such as physical damage can make a node unavailable. It may be difficult to recognize whether packets were dropped due to a security attack or for non security reasons. Dropping packets can lead to an increase in the number of packet retransmissions, transfer time, response time and network overhead. However, there is no doubt about the malicious behavior if the node drops some legitimate packets and then injects fake packets to replace them. In this case the malicious node obviously has enough resources to do this.

In this paper, we present a novel packet dropping attack and novel traceback mechanism. A malicious node can selectively drop some packets and inject fake packets so it can maintain the original total number of packets originated from the sender node. The existing packet dropping defense mechanism, such as the multipath routing based mechanisms [1–5], reputation based mechanism [6], data provenance based mechanisms [7], acknowledgment based mechanisms [8–10], are inefficient as in OppNets we have no end to end connections and usually have no alternative paths from the sender to the destination or vice versa. Network coding based mechanisms [11], are inefficient as the destination nodes should have a copy of all neighbors packets/messages so it can decode its message, which is difficult to achieve in OppNets. Watchdog and pathrater mechanism [12–17] are inefficient for detecting this type of attack as the detection idea is based on the calculation of the total number of transmitted/received packets. Encryption techniques [18] are inefficient as well, as we required the use of a secret key which is difficult to manage in OppNets since we have no centralized management.

Our new detection and traceback mechanism is very accurate for addressing this type of attack as we relied on the use of hash chain techniques [19] to maintain packet integrity.

* Corresponding author. Tel.: +61 478092905.
E-mail address: malajeel@deakin.edu.au, alajeely@gmail.com (M. Alajeely).

http://dx.doi.org/10.1016/j.comcom.2015.10.004
0140-3664/© 2015 Elsevier B.V. All rights reserved.

Contribution. To the best of our knowledge, this is the first attempt to identify this type of attack and the traceback mechanism. The main contributions of this work are:

1. To identify a Catabolism attack where malicious nodes drop some packets and then inject fake packets instead.
2. To identify an Anabolism defense where the legitimate nodes can check the received packets to detect the attack, and then traceback and identify the malicious nodes that triggered this attack.

The remainder of this paper is organized as follows. In Section 2, we present related work. In Section 3, we present the Catabolism attack and Anabolism defense. In Section 4, we present our mathematical model. In Section 5, we present our simulation results and in Section 6, we present our conclusion and future work.

2. Related work

Defense mechanisms for packet dropping attacks use multipath routing based mechanisms where packets divide into a number of groups and then send to a destination in more than one path [1–5].

E-HSAM [1] propose a security improvement mechanism where packets that go through a path with a malicious node redirect to an alternative path. However, in OppNets this variety is not always available since there is no end to end connection and no alternative path available all the time. This technique results in network overhead and difficulty in identifying malicious nodes. Moreover, this technique might be vulnerable to route discovery attacks.

In [2], the authors use multipath data forwarding only when a Neighbor Watch System detects a malicious node, while single path data forwarding is used in normal operation in order to reduce power consumption. The authors in [3], propose a packet dropping detection mechanism based on cooperative participation at the network-bootstrapping phase. Alternative routing is used to avoid malicious nodes or non-trust paths. However, this solution leads to network overhead.

Lee and Gerla , [4] propose an on-demand routing protocol by establishing and using multiple routes. This protocol uses a per-packet allocation scheme to spread data packets into multiple paths. This will utilize available network resources and prevent nodes from being traffic congested.

Lu and Wong, [5] propose a distributed, scalable and localized multipath search protocol for discovering multiple node-disjoint paths between the sink and source nodes. The authors also propose a load balancing mechanism to spread the traffic over the discovered paths.

Acknowledgement based mechanisms can also be used for detecting a packet dropping attack [8–10]. This is based on authenticated acknowledgment from the intermediate nodes and the destination within a specific time. The source or destination can detect a malicious node.

Baadache and Belmehdi, [10] propose a mechanism for detecting a packet dropping attack where the intermediate node acknowledges the reception of packets. A source node then uses this acknowledgment to construct a Merkle tree, and then compares the value of the tree root with a precalculated value. If these values are equal then no packets were dropped in that path, otherwise there is a packet dropping attack. However, this technique can detect a path with a malicious node but is unable to detect the malicious node, therefore it looks for an alternative path for retransmission, thus resulting in network overhead.

Network coding based mechanisms can be used for detection and defense as in [11], where a mitigation scheme to evaluate the impact of the packet selective dropping attack in DTN is proposed by using network coding. In this scheme the destination node measures the delivery ratio and sends it back to the sender. The sender then begins adjusting the redundancy factor dynamically to mitigate against the degradation in the delivery ratio caused by the attack. Theoretical analysis and experimental simulations also disclose some characteristics of the impact of packet dropping on the routing performance, such as delivery ratio, delivery cost and delivery latency. These are degraded if the major nodes behave as packets dropping or behave selfishly. In addition, the impact of the non-cooperative action like selfishness or non-forwarding and dropping of messages in the routing performance where behavior of non-forwarding of messages reduces the delivery cost, while the behavior of dropping messages increases the delivery cost.

Data provenance based mechanisms [7] can be used to identify malicious nodes where the characteristics of the watermarking based secure provenance transmission mechanism and the inter-packet timing characteristics are exploited to achieve this goal. There are three stages to this technique. The first detects lost packets using the distribution of the inter-packet delay. The second identifies the present of the attack by comparing the empirical average packet loss rate with the natural packet loss rate of the data flow path, and finally the technique identifies a malicious node or link then isolates it by transmitting more provenance information along with the sensor data . However, this technique is not very accurate because it does not detect the exact malicious node in the entire path or link. The impact of TCP packet dropping attacks and detection methods are explored in [20]. Three dropping mechanisms are investigated. These are periodic packet dropping (PerPD), Retransmission packet dropping (RetPD) and Random packet dropping (RanPD). Statistical based analysis (TDSAM) used for detection of these kinds of attacks are based on the NIDESETAT algorithm running on the ftp client side. However, only one detection technique is proposed in this work without any defense mechanism.

Watchdog and Pathrater mechanism is also used for detecting malicious attacks [12,13,15–17]. Watchdog is a technique for monitoring the behavior of neighbor nodes in order to classify nodes as either legitimate or malicious. Pathrater uses the output of watchdog to select the best path to the destination.

In [12], watchdog and pathrater are used to improve throughput in a mobile ad hoc network. In the watchdog stage, the sender node detects the misbehaving node by overhearing the neighbor node and comparing the message transmission with the saved copy on its buffer and checks if it's matching. If matching, this means the node is not malicious and the message copy on the buffer will be deleted. If the sender node does not hear for a certain time the watchdog will increment the failure tally of that neighbor node. If that tally exceeds the threshold value, the node will then be recorded as a misbehaving node. Each node runs the pathrater phase to determine the best path with the highest metric by combining the information from the watchdog with the link reliability data to calculate the best path. According to the information from the watchdog and pathrater, each node will build a rating table for other known nodes on the network to use for future transmissions. However, the watchdog technique is not that efficient in case of the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, or collusion.

To solve the weakness of watchdog, authors in [13] propose ExWatchdog to enhance the intrusion detecting system for discovering malicious nodes. ExWatchdog has the ability to detect malicious nodes that can partition the network by untruthfully reporting other nodes as malicious. Each node builds a table with the number of received packets and the number of forwarded packets. When a node receives a report about the misbehavior of some node, the source of the communication starts sending a message to the destination to check if the number of received and forwarded packets are equal. If equal, the node that reported the other node as malicious is actually malicious itself.