Ad Hoc Networks 21 (2014) 84–96

Contents lists available at ScienceDirect

Ad Hoc Networks

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

Lifetime elongation of ad hoc networks under flooding attack using power-saving technique

Fuu-Cheng Jiang [a], Chu-Hsing Lin [a,*], Hsiang-Wei Wu [b]

[a] Department of Computer Science, Tunghai University, No. 1727, Sect. 4, Taiwan Boulevard, Taichung 40704, Taiwan
[b] Department of Computer Science and Engineering, National Chung-Hsing University, No. 250 Kuo-Kuang Road, Taichung 40227, Taiwan

ARTICLE INFO

Article history:
Received 19 October 2013
Accepted 6 May 2014
Available online 15 May 2014

Keywords:
Petri Net
AODV
Flooding attack
Mobile ad hoc network

ABSTRACT

Without the management of centralized unit, mobile ad hoc networks (MANETs) are vulnerable to security threats from flooding attacks launched through compromised nodes or intruders. When a source node needs a data session with a destination node, it disseminates a route request (RREQ) message to its neighbors in a hop-by-hop manner. One crucial type of flooding attacks called RREQ flooding appears to be inevitably proliferated in wireless networks. In the RREQ flooding attack, attackers would launch massive RREQ packets with out-of-domain IP address as its destination node. The forwarding services conducted by all intermediate nodes exhaust their energy and processing resources. The proposed approach can suppress redundant RREQ packets using the co-operation of destination node and neighbor nodes within one-hop range of the attacking node. A Petri Net design was developed to model the proposed approach and configure all relevant system aspects in a concise fashion for qualitative analysis. From quantitative viewpoint, relevant network simulations were conducted to validate the proposed scheme using a NS2 network simulator. The experimental result reveals that the proposed power-saving technique can be applied to economically and effectively elongate the operational lifetime of MANETs under flooding attack.

1. Introduction

A mobile ad hoc network (MANET) is a wireless LAN (Local Area Network) model without the need of central base stations and operated as a self-organized, dynamically changing multi-hop network [1,2]. MANETs can be applied in medical emergencies, during natural catastrophes, for military applications and conducting geographic exploration [3,4]. Mobile and wireless devices belonging to a MANET are usually called mobile nodes. These nodes are characterized by high mobility, low power, limited storage, limited transmission range and finite energy budget without recharging gears. Mobile nodes communicate through bi-directional radio links and data transmission is a key challenge. MANET communication events are called sessions. The two communicating parties, namely the source node and the destination node comprise a session pair (or source–destination pair). A mobile node can communicate directly with other nodes if such a link exists within the radio transmission range. If the distance between a session pair is too large to establish direct contact, the data must then be sent via intermediate nodes connecting the two parties.

Based on a hop-by-hop routing scheme, the AODV (Ad hoc On-Demand Vector) routing protocol offers quick adaption to dynamic links, low processing and memory overhead. When a source node needs a route to a destination, it disseminates a route request (RREQ) message to its neighbors. Each node receiving the message creates a

* Corresponding author. Tel.: +886 423590043; fax: +886 423591567.
E-mail address: chlin@go.thu.edu.tw (C.-H. Lin).

http://dx.doi.org/10.1016/j.adhoc.2014.05.002
1570-8705/

reverse route to the source. This message is flooded until the information needed is completed by either reaching the destination or reaching an intermediate node that has a valid route (in its routing table) to the destination. A route reply (RREP) message is sent back to the source in a unicast manner along this newly found route or an existing valid route. Duplicate copies of RREQ packets received at any node are discarded. Each intermediate node receiving this RREP creates a forward route to the destination. Thus, each node remembers only the next hop required to reach any host, not the whole route. Once the source node receives RREP, it may start to forward data packets to the destination. If the source node later receives a RREP message containing a shorter route, it may update its routing table for that destination and adopt the shorter route instead of the old one.

In a conventional wired-networking environment, flooding attacks were once notorious for firing pervasive Denial-of-Service (DoS) attacks or/and Distributed DoS (DDoS) attacks on the crucial servers of worldwide enterprises and institutions [5,6]. In a wireless local area network, flooding attacks would be proliferated in some similar fashions. As more consumers use their portable electronic devices such as laptop computers, cellular phones and Tablet PCs, MANETs are expected to emerge ubiquitously in the coming years. In a MANET, wireless packets are transmitted via neighbor nodes instead of a base station. Without the control and management of centralized control nodes, MANETs are vulnerable to security threats because all signals go through bandwidth-constrained wireless links and mobile neighbor nodes with a limited energy budget.

During route discovery process of AODV protocol, attackers may maliciously deteriorate the broadcast problem to deplete communication energy and processing resources on legal MANET nodes. Upon receiving RREQ packets for the first time, any legal node in an AODV-based MANET has the obligation to re-disseminate the message. Even in a scenario without malicious attackers, there are considerable negative impacts incurred from the rebroadcasting regulation. Some obvious and unavoidable impacts include redundant rebroadcast, contention, and collision [5]. Aimed at such storm attack scenarios, Yi et al. [7] coined a new phrase in MANETs: RREQ flooding attack. Using the RREQ flooding attack, attackers would issue a massive number of RREQ packets with an out-of-domain IP address as its destination node.

To explore possible solutions for prior flooding attacking issues, a dual defense wall system (DDWS) was elaborated to mitigate the impact from flooding attacks. To balance the defensive loads among legal nodes, the defensive tasks are executed cooperatively by two bodies composed of the first-hop intermediate node around the attacker and the destination node. The first-hop intermediate nodes around the attacker constitute the first defensive wall. Basically on mission-oriented MANETs, the legal nodes should be informed of applicable and legal IP domains at the preparation stage for their mission period. So the alien attackers would use arbitrary out-of-domain IP address as the destination node to launch massive RREQ flooding attacks. This sort of bogus RREQs can be suppressed by the first defensive wall. For a malicious insider, the massive quantity of RREQs in short intervals can be a clue for the second defensive wall. By monitoring the frequency of sending RREQs by a suspicious node, the first-hop intermediate nodes are able to reject RREQ flooding attacks.

The contribution of this article is threefold: (i) To conserve valuable and limited bandwidth for legal MANET nodes, we propose an efficient approach capable of not only mitigating massive useless RREQ packets caused by intruders but also excluding misjudgment on instantly unstable legal nodes. (ii) Our general modeling approach is based on Petri Nets for qualitative analysis. Through elaborating Petri Net design, it is possible to incorporate all relevant details in a concise model. (iii) The NS2 network simulation is conducted to verify and validate the proposed scheme. The simulation results demonstrate not only on the considerable reduction of fraudulent RREQ traffic loads but also the significant reduction of the impact on power deletion from RREQ flooding attacks.

The rest of this paper is organized as follows: Section 2 describes the background profile and related work regarding flooding attacks in MANET. In Section 3, we present and describe relevant constituent elements of the proposed DDWS implemented by spreading defensive loads among legal nodes in a co-operative manner. In Section 4, based on the architecture of dual defensive walls, a Petri Net design is developed to model the DDWS for in-depth understanding from the qualitative point of view. The network experiments with NS2 simulator are also conducted in Section 5. Section 6 presents some concluding remarks.

2. Background and related work

2.1. Route discovery in AODV-based protocol

When a source needs to initiate a data session to a destination but does not have any route information, it searches for a route by flooding a ROUTE REQUEST (RREQ) packet. Each RREQ packet has a unique identifier so that nodes can detect and drop duplicate packets. An intermediate node, upon receiving a non-duplicate RREQ, records the previous hop and the source node information in its route table (i.e., backward learning). It then broadcasts the packet or sends back a ROUTE REPLY (RREP) packet to the source if it has a route to the destination. The destination node sends a RREP via the selected route when it receives the first RREQ or subsequent RREQs that traversed a better route (in AODV for instance, fresher or shorter route) than the previously replied route.

An illustrative scenario describing topology and route discovery process are shown in Figs. 1 and 2 respectively. Fig. 1 depicts the network topology with nine nodes when an edge between two nodes indicates that the nodes are within direct transmission range of each other. For instance, node S (Source) is within transmission range of nodes 1 and 2, and node D (Destination) is within transmission range of nodes 3 and 7. The operational message sequence on this exemplified AODV wireless network is illustrated in Fig. 2. It is assumed that a new route is