Early Detection and Prevention of Vampire Attacks in Wireless Sensor Networks

Priyanka Chandragiri

Assistant Professor in CSE, Christu Jyothi Institute of Technology & Science, Jangaon, India.

Abstract - Vampire attacks are not specific to any protocol, but rather rely on the properties of classes of routing protocols. A single Vampire can increase network-wide energy usage by a factor of O (N), where N is the number of network nodes. This paper uses two attacks on stateless protocol in which the Carousel attack is an adversary and sends a packet with a route composed as a series of loops, such that the same node appears in the route many a times, and the Stretch attack where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. The vampire attacks are very difficult to detect and prevent.

Keywords – Ad-hoc Networks, Carousel attack, Stretch attack and malicious discovery attack.

1. Introduction

Wireless ad-hoc network is needed to explore in sensing and pervasive computing. The security work focuses on denial of communication at the routing or medium access control levels. The “Vampire” attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. Vampire attack is the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmits a message of identical size to the same destination, although using different packet headers. All the protocols are devastating, difficult to detect and easy to carry out using as few as one malicious insider sending only protocol compliant messages. The proposed system discuss the methods to detect and mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

This paper makes three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing infrastructure, and so existing secure routing protocols such as SAODV, and SEAD do not protect against Vampire attacks.

DOS attacks represents in wired networks are frequently characterized by amplification an adversary can amplify the resources it spends on the attack the cumulative energy of an entire network, amplification attacks are always possible, given that an adversary can compose and send messages which are processed by each node along the message path. Vampire attack has the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers.

1.2 Protocols and Assumptions

All routing protocols employ at least one topology discovery period, since ad-hoc deployment implies no prior position knowledge. a single Vampire may attack every network node simultaneously, meaning that continuous recharging does not help unless Vampires are more resource-constrained than honest nodes Vampire attacks may be weakened by using groups of nodes with staggered cycles: only active-duty nodes are vulnerable while the Vampire is active; nodes are safe while the Vampire sleeps this defence is only effective when duty cycle groups outnumber Vampires, since it only takes one Vampire per group to carry out the attack.

1.3 Overview

In the first attack that is Carousal attack an adversary composes packets with purposely introduced routing loops it targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. In the second attack that is stretch attack an adversary constructs artificially long routes, potentially traversing every node in the network. The assumption has been made that only messages originated by adversaries may have maliciously-composed routes.

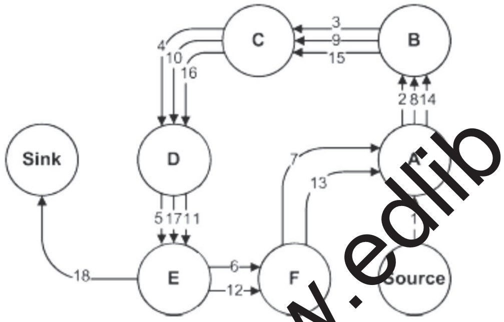


Fig (a) An honest route would exit the loop Fig (b) Honest route is dotted while immediately from Node E to sink. Malicious code is dashed. Above figure shows Malicious route construction attacks on source routing: carousel attack Fig (a) and stretch attack Fig (b).

2. Related Work

Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action. [1,2,3] the most permanent denial of service attack is to entirely deplete nodes batteries.Disadvantages of existing system are power outages, due to environmental disasters, loss in the information, lost productivity various dos attacks, secure level is low, they do not address attacks that affect long-term availability.

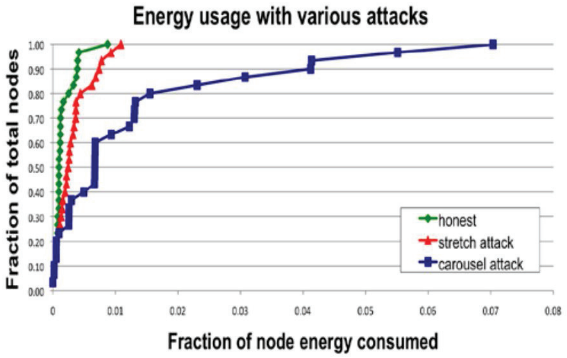
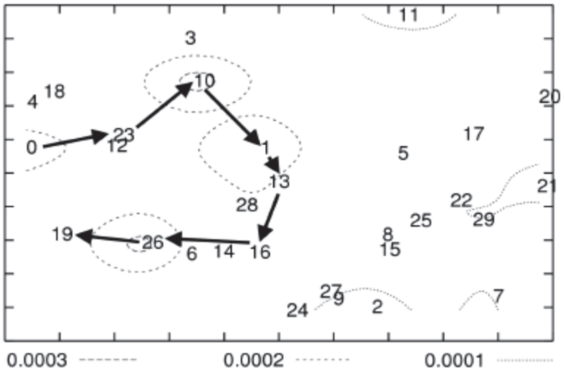


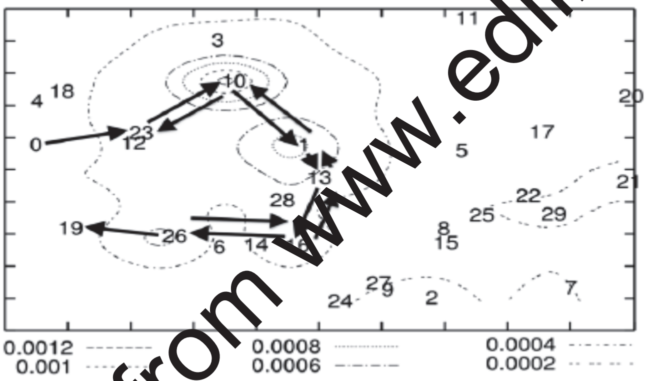
Fig (c) Node energy distribution under various attack scenarios.

3. Attacks on Stateless Protocol

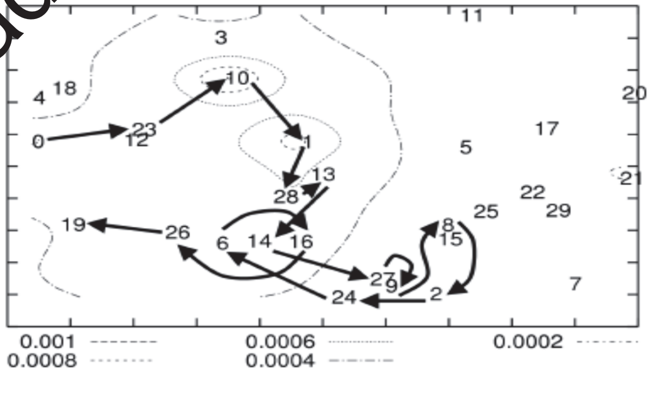
The carousel and stretch attacks (Fig (a) & Fig (b)) in a randomly-generated 30-node topology and a single randomly-selected malicious DSR agent, using the ns-2 network simulator. Malicious nodes are not driving down the cumulative energy of the network purely by their own use of energy.



(a) Honest scenario: node 0 sends a single message to node 19



(b) Carousel attack (malicious node 0): the nodes traversed by the packet are the same as in (a), but the loop over all forwarding nodes roughly triples the route length (the packet traverses the loop more than once). Note the drastically increased energy consumption among the forwarding nodes.



(c) Stretch attack (malicious node 0): the route diverts from the optimal path between source and destination, roughly doubling in length. Note that while the per-node energy consumption increase is not as drastic as in (b), the region of increased energy consumption is larger. Overall energy consumption is greater than in the carousel attack but spread more evenly over more network nodes.

3.1 Mitigation methods

The carousel attack can be prevented when a loop is detected, the source route could be corrected and the packet sent on, but one of the attractive features of source routing is that the route can itself be signed by the source. The stretch attack is more challenging to prevent. Its success rests on the forwarding node not checking for optimality of the route.

4. Attacks on Stateful Protocols

Routes in link-state and distance-vector networks are built dynamically from many independent forwarding decisions, so adversaries have limited power to affect packet forwarding, making these protocols immune to carousel and stretch attacks. Vampires have little control over packet progress when forwarding decisions are made independently by each node, but they can still waste energy by restarting a packet in various parts of the network. In Malicious discovery attack the attack on all previously-mentioned routing protocols (including stateful and stateless) is spurious route discovery.

5. Provable Security Against Vampire Attacks

The non backtracking property is satisfied for a given packet if and only there exists routes for its transmission. This means that the adversary cannot perform carousel or stretch attacks, no node may unilaterally specify a suboptimal path through the network.

Results

S.No.	A	B	c	d	E	f	Result
1	No link	No link	No link	No link	No link	received	F
2	No link	No link	received	No link	No link	sent	C
3	Received	No link	sent	No link	No link	No link	A
4	Sent	No link	No link	received	No link	No link	D

Table 1: Validation with the given link source f-c-a-d

6. Conclusion & Future Work

Distance Vector is the wireless sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The detection and avoidance of formation of loops help this protocol detect and avoid vampire attacks. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

7. References

1. Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, "Denial of service resilience in ad hoc networks", MobiCom, 2004.
2. John Bellardo and Stefan Savage, "802.11 denial-of-service attacks: real vulnerabilities and practical solutions", USENIX security, 2003.
3. Jing Deng, Richard Han, and Shivakant Mishra, "Defending against pathbased DoS attacks in wireless sensor networks", ACM workshop on security of ad hoc and sensor networks, 2005.

4. Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, “Secure sensor network routing: A clean-slate approach”, CoNEXT, 2006.
5. David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, “Effects of denial-of-sleep attacks on wireless sensor network MAC protocols”, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.
6. Frank Stajano and Ross Anderson, “The resurrecting duckling: security issues for ad-hoc wireless networks”, International workshop on security protocols, 1999.
7. Amitabh Saxena and Ben Soh, “One-way signature chaining: a new paradigm for group cryptosystems”, International Journal of Information and Computer Security 2 (2008), no. 3.
8. Michael Scott, Neil Costigan, and Wesam Abdul wahab, “Implementing cryptographic pairings on smartcards”, CHES, 2006.
9. Rahul C. Shah and Jan M. Rabaey, “Energy aware routing for low energy ad hoc sensor networks”, WCNC, 2002.