Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.388 – 392

RESEARCH ARTICLE

PREVENTION OF VAMPIRE ATTACKS TO CONTROL ROUTING BEHAVIOR IN WIRELESS AD HOC SENSOR NETWORKS

Kavya.H.B[1], Manjunath R Raikar[2]

[1]M.Tech (CSE), AIET, Moodbidri
[2]M.Tech, Assistant Professor, Dept of CSE, AIET, Moodbidri

[1] Kavyachinnu67@gmail.com
[2] raikar.manjunath@gmail.com

Abstract— An Ad hoc wireless sensor networks (WSNs) assuring many new exciting applications such as On-demand computing supremacy, incessant connectivity, and instantaneously deployable communication for armed and responders. As WSNs grow to be a greater extent essential to the everyday performance of people and organizations, many attacks are arisen in the Ad hoc wireless sensor networks. This project explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power. In the worst case, a single vampire can increase network-wide energy usage by a factor of O (N), where N is the number of network nodes. This project proposes methods to prevent the adversary influence on the network, including an implemented PLGPa method of AODV protocol that provably bounds the damage caused by vampires during the packet forwarding phase.

Keywords— Network, Protocol, Packet, Vampire attack

1. INTRODUCTION

Ad hoc Wireless Sensor Networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives, thus high availability of these networks is a critical property, and should hold even under malicious conditions.

Vampire Attack is defined as 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. These attacks do not disrupt immediate availability, but rather work over time to entirely disable a network.

1.1 Types of Vampire Attacks

1.1.1 Carousel Attack

The attack shown in Fig. 1, an adversary composes packets with purposely introduced routing loops; this attack is called as Carousel Attack, since it sends packets in circle.

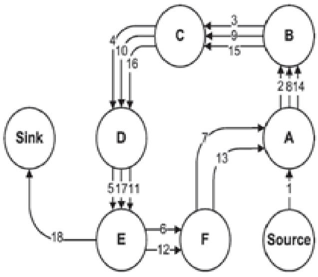


Fig.1: Carousel Attack

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.

1.1.2 Stretch Attack

In the second attack in Fig. 2, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network; this attack is called as Stretch Attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. Stretch Attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets.

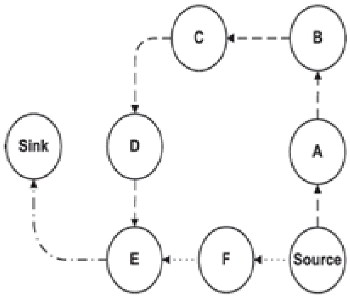


Fig.2: *Stretch Attack*

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.

2. RELATED WORK

As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to their ad hoc organization, wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks [1], and a great deal of research has been done to enhance survivability [2], [4], [6], [8]. While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability, the most permanent denial of service attack is to entirely deplete nodes batteries. This is an instance of a resource depletion attack with battery power as the resource of interest. There is also significant literature on attacks and defenses against Quality of Service (QoS) degradation, or Reduction of Quality (RoQ) attacks that produce long-term degradation in network performance [10]. The focus of this work is on the transport layer rather than routing protocols, so these defenses are not applicable. Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high.

Other work on denial of service in ad hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets [3],[7]. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire Attacks, since Vampires do not use or return illegal routes or prevent communication in the short-term.

Another attack that can be thought of as path based is the wormhole attack [9]. It allows two non-neighboring malicious nodes with either a physical or virtual private connection to emulate a neighbor relationship, even in secure routing systems. These links are not made visible to other network members, but can be used by the colluding nodes to privately exchange messages. Similar tricks can be played using directional antennas. These attacks deny service by disrupting route discovery, returning routes that traverse the wormhole, and may have artificially low associated cost metrics. While a defense was proposed against wormhole and directional antenna attacks called Packet Leashes [9], but solution comes at a high cost and is not always applicable.

Current work in minimal-energy routing, which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets (e.g., by minimizing wireless transmission distance) [11], [12] is likewise orthogonal: these protocols focus on co-operative nodes and not malicious scenarios. However, Vampires will increase energy usage even in minimal-energy routing scenarios and when power conserving MAC protocols are used; these attacks cannot be prevented at the MAC layer or through cross-layer feedback. Attackers will produce packets which traverse more hops than necessary, so even if nodes spend the minimum required energy to transmit packets, each packet is still more expensive to transmit in the presence of Vampires.

This paper will consider how routing protocols designed to be secure, lack protection from these attacks, which is called as Vampire Attacks, since they drain the life from networks nodes. These attacks are distinct from Denial of Service (DoS), Reduction of Quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network.

3. PROPOSED SYSTEM

3.1 Primary contributions of paper

- This paper thoroughly evaluates the vulnerabilities of existing protocols to routing layer battery depletion attacks. In this paper the security measures can be observed to prevent Vampire Attacks are orthogonal to those used to protect routing infrastructure and so existing secure routing protocols such as Ariadne [9], SAODV and SEAD [11] do not protect against Vampire Attacks.

- Simulation results can be shown for quantifying the performance of several representative protocols in the presence of a single Vampire.

- By modifying existing sensor network routing protocol can provably bound the damage from Vampire Attacks during packet forwarding.

3.2 Vulnerabilities

- Malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes that forward the packet based on the included source route.

- Routing schemes, where forwarding decisions are made independently by each node, Directional antenna and Wormhole Attacks can be used to deliver packets to multiple remote network positions, forcing packet processing at nodes that would not normally receive that packet at all, and thus increasing network energy expenditure.

4. METHODOLOGY

4.1 Clean-Slate Sensor Network Routing

In this paper, a clean-slate secure sensor network routing protocol by Parno et al. ("PLGP" from here on) [7] can be modified to provably resist Vampire Attacks during the packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to Vampire Attacks. PLGP consists of a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current.

Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. When discovery begins, each node has a limited view of the network, the node knows only itself. Nodes discover their neighbors using local broadcast, and form ever expanding neighbor hoods, stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbor relationship and group membership that will later be used for addressing and routing.

4.2 Provable Security against Vampire Attacks

4.2.1 No-Backtracking property

No-Backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network. This property implies Vampire resistance.

4.2.2 PLGP with attestations (PLGPa)

Add a verifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. These signatures form a chain attached to every packet, allowing any node receiving it to validate its path.

4.2.3 PLGPa satisfies No-Backtracking

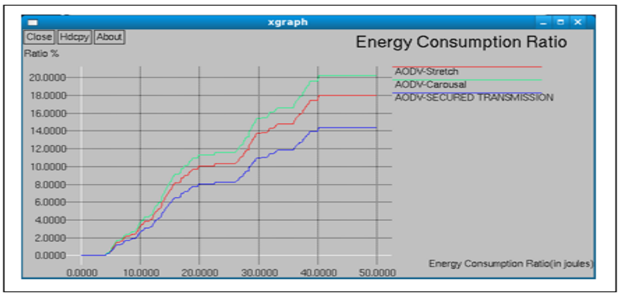
Since all messages are signed by their originator, messages from honest nodes cannot be arbitrarily modified by malicious nodes wishing to remain undetected. Rather, the adversary can only alter packet fields that are changed in route, so only *the* route attestation field can be altered, shortened, or removed entirely. To prevent truncation, which would allow Vampires to hide the fact that they are moving a packet away from its destination, use one-way signature chain construction which allow nodes to add links to an existing signature chain, but not remove links, making attestations append only.

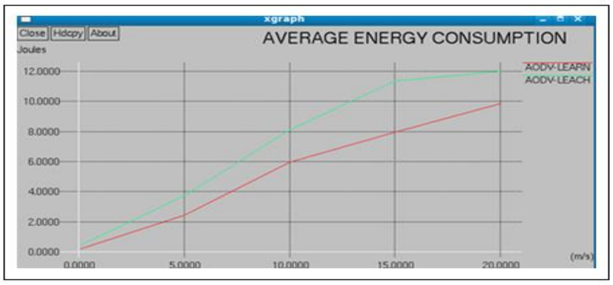
5. IMPLEMENTATION

The forwarding phase of PLGP is modified to provably avoid the above mentioned attacks. First by introducing the No-Backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. To preserve No-Backtracking, verifiable path history is added to every PLGP packet, similar to route authentications in Ariadne [9].

The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure, so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, this by attaching a non replayable attestation (signature), these signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space as shown in the above function for the modified protocol.

6. EXPERIMENTAL RESULT





According to result of this paper, the energy usages in carousel attack is 20.197 and energy usages of stretch attack is 17.984. Using resulting PLGPa protocol, secured transmission is established that nodes forwarding the packet from source to destination consuming comparatively less energy that is 14.387 joules. Resulting graph shows the comparison between Vampire Attacks and secured transmission.

7. CONCLUSION

Vampire Attacks are dangerous kind of attacks as in worst case a single Vampire can cause a network wide energy by a factor of O (N) where N is the number of nodes in the network. In an Ad hoc wireless network during the attacks in packet forwarding the energy usage is increased in network. In this paper the main highlight of the implementation is to prevent adversary influence on the nodes battery power and to establish the secured transmission with less energy consumption. According to our result, using implemented routing protocol adversary influence can be prevented as honest nodes can forward the packets in secured transmission consuming less energy.

REFERENCES

[1] I. Aad, J.-P. Hubaux, and E.W. Knightly, “Denial of Service Resilience in Ad Hoc Networks,” Proc. ACM MobiCom, 2004.
[2] J. Bellardo and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” Proc. 12th Conf. USENIX Security, 2003.
[3] J. Deng, R. Han, and S. Mishra, “Defending against Path-Based DoS Attacks in Wireless Sensor Networks,” Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.
[4] J. Deng, R. Han, and S. Mishra, “INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks,” Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.
[5] A. Nasipuri and S.R. Das, “On-Demand Multipath Routing for Mobile Ad Hoc Networks,” Proc. Int’l Conf. Computer Comm. And Networks, 1999.
[6] A.D. Wood and J.A. Stankovic, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.
[7] B. Parno, M. Luk, E. Gaustad, and A. Perrig, “Secure Sensor Network Routing: A Clean-Slate Approach,” CoNEXT: Proc. ACM CoNEXT Conf., 2006.
[8] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff, “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols,” IEEE Trans. Vehicular Technology, vol. 58, no. 1,pp. 367-380, Jan. 2009.
[9] Y.C. Hu, D.B. Johnson, and A. Perrig, “Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks,” Proc. MobiCom, 2002.
[10] J. Deng, R. Han, and S. Mishra, “Defending against Path-Based DoS Attacks in Wireless Sensor Networks,” Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.
[11] Y.C. Hu, D.B. Johnson, and A. Perrig, “SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks, ”Proc. IEEE Workshop Mobile Computing Systems and Applications, 2002.
[12] Y.C. Hu, D.B. Johnson, and A. Perrig, “Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks,” Proc .IEEE INFOCOM, 2003.

