ISSN (Online): 2349-7084
GLOBAL IMPACT FACTOR 0.238
ISRA JIF 0.351

INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING IN RESEARCH TRENDS
VOLUME 1, ISSUE 6, DECEMBER 2014, PP 397-404

Exigent Life from Wireless ad-hoc Signal Networks

[1] J.JAYASANTHI, [2] K.SUMALATHA

[1] M.Tech Research Scholar, Priyadarshini Institute of Technology and Science for Women
[2] Assistant Professor, Priyadarshini Institute of Technology and Science for Women

Abstract: An ad hoc sensor wireless network has been drawing interest among the researches in the direction sensing and pervasive computing. The security work in this area is priority and primarily focusing on denial of communication at the routing or medium access control levels. In this paper the attacks which are mainly focusing on routing protocol layer that kind of attacker is known as resource depletion attacks. These “Vampire” attacks are not impacting any specific kind of protocols. Finding of vampire attacks in the network is not a easy one. It’s very difficult to detect, devastating .A simple vampire presenting in the network can increasing network wide energy usage. We discuss some methods and alternative routing protocols solution will be avoiding some sort of problems which causing by vampire attacks.

Keywords: Sensor Networks; Wireless Networks; Ad hoc Networks; Routing Protocols.

1. INTRODUCTION

An ad hoc wireless network is a collection of wireless mobile nodes that self-configure to form a network without the aid of any established infrastructure, as shown in without an inherent infrastructure, the mobiles handle the necessary control and networking tasks by themselves, generally through the use of distributed control algorithms. Multihop connections, whereby intermediate nodes send the packets toward their final destination, are supported to allow for efficient wireless communication between parties that are relatively far apart. Ad hoc wireless networks are highly appealing for many reasons. They can be rapidly deployed and reconfigured. They can be tailored to specific applications, as implied by Oxford’s definition. They are also highly robust due to their distributed nature, node redundancy, and the lack of single points of failure.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network device in link range. Ad hoc network often refers to a mode of operation of IEEE 802.11 wireless networks.

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.

A. Protocols and assumptions

In this paper we consider the effect of Vampire attacks on link-state, distance-vector, source routing and geographic and beacon routing protocols, as well as a logical ID-based sensor network routing protocol proposed by Parno et al. [53]. While this is by no means an exhaustive list of routing protocols which are vulnerable to Vampire attacks, we view the covered protocols as an important subset of the routing solution space, and stress that our attacks are likely to apply to other protocols.

All routing protocols employ at least one topology discovery period, since ad-hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically-organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, where topology discovery is done at transmission time, and static protocols, where topology is discovered during an initial setup phase, with periodic re-discovery to handle rare topology changes. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Furthermore, adversary location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was deployed, and cannot control their final positions. Note that this is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Intelligent adversary placement or dynamic node compromise would make attacks far more damaging.

B. Classification

The first challenge in addressing Vampire attacks is defining them — what actions in fact constitute an attack? DoS attacks in wired networks are frequently characterized by amplification [52,54]: an opposition can amplify the resources it spends on the attack, e.g. use one minute of its own CPU time to cause the victim to use ten minutes. However, consider the process of routing a packet in any multi-hop network: a source composes and transmits it to the next hop toward the destination, which transmits it further, until the destination is reached; consuming resources not only at the source node but also at every node the message moves through. If we consider 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. So, we must drop amplification as our definition of maliciousness and instead focus on the cumulative energy consumption increase that a malicious node can cause while sending the same number of messages as an honest node.

We define a Vampire attack as the composition and trans-mission 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. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e. the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant.

C. Overview

In the remainder of this paper, we present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience. In source routing protocols, we show how a 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. In routing schemes where forwarding decisions are made independently by each node (as opposed to specified by the source), we suggest how directional antenna and wormhole attacks [30] 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-wide energy expenditure.

In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles as shown in Figure 1(a). 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.

2 .RELATED WORKS

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, 15, 19, 63], is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios. Additional on power-conserving medium access control (MAC), upper-layer protocols, and cross-layer cooperation [24, 34, 43, 45, 66, 67, 69, 77]. 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. Our work can be thought of attack-resistant minimal-energy routing, where the adversary's goal includes decreasing energy savings.

Other work on denial of service in ad-hoc wireless net-works has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets [14, 28, 29, 36, 78]. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above. 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.

We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion can be found in [68], as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus depletes their batteries faster. Newer research on "denial-of-sleep" only considers attacks at the medium access control (MAC) layer [59]. Additional work mentions resource exhaustion at the MAC and transport layers [60, 75], but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned [10, 53], but no effective defenses are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing.

Even in non-power-constrained systems, depletion of resources such as memory, CPU time, and bandwidth may easily cause problems. A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the adversary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity (e.g. SYN cookies [7], which offload the initial connection state onto the client, or cryptographic puzzles [4, 48, and 73]). These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting and not always desirable as it punishes nodes that produce bursty traffic but may not send much total data over the lifetime of the network. Since Vampire attacks rely on amplification, such solutions may not be sufficiently effective to justify the excess load on legitimate nodes.

While this strategy may protect against traditional DoS, where the malefactor overwhelms honest nodes with large amounts of data, it does not protect against "intelligent" adversaries who use a small number of packets or do not originate packets at all. As an example of the latter, Aad et al. show how protocol-compliant malicious intermediaries using intelligent packet-dropping strategies can significantly degrade performance of TCP streams traversing those nodes [2]. Our adversaries are also protocol-compliant in the sense that they use well-formed routing protocol messages. However, they either produce messages when honest nodes would not, or send packets with protocol headers different from what an honest node would produce in the same situation.

Another attack that can be thought of as path-based is the wormhole attack, first introduced in [30]. 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 [3]. 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 The network is composed of 30 nodes and a single randomly-positioned Vampire. Results shown are based on a single packet sent by the attacker by disrupting route discovery, returning routes that traverse the wormhole and may have artificially low associated cost metrics (such as number of hops or discovery time, as in rushing attacks [31]).

3. 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. In fact, any time adversaries cannot specify the full path, the potential for Vampire attack is reduced. However, malicious nodes can still misforward packets, forcing packet forwarding by nodes that would not normally be along packet paths. For instance, an adversary can forward packets either back toward the source if the adversary is an intermediary or to a non-optimal next hop if the adversary is either an intermediary or the source.

We now move on to stateful routing protocols, where network nodes are aware of the network topology and its state, and make local forwarding decisions based on that stored state. Two important classes of stateful protocols are link-state and distance-vector. In link-state protocols, such as OLSR [12], nodes keep a record of the up-or-down state of links in the network, and flood routing updates every time a link goes down or a new link is enabled. Distance-vector protocols like DSDV [55] keep track of the next hop to every destination, indexed by a route cost metric, e.g. the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated.

While this may seem benign in a dense obstacle-free topology, worst-case bounds are no better than in the case of the stretch attack on DSR. For instance, consider the special case of a ring topology: forwarding a packet in the reverse direction causes it to traverse every node in the network (or at least a significant number, assuming the malicious node is not the packet source but rather a forwarder), increasing our network-wide energy consumption by a factor of O (N). While ring topologies are extremely unlikely to occur in practice, they do help us reason about worst-case outcomes. This scenario can also be generalized to routing around any network obstacle along a suboptimal path.

Some recent routing research has moved in the direction of coordinate- and beacon-based routing, such as GPSR and BVR [21, 37], which use physical coordinates or beacon distances for routing, respectively. In GPSR, a packet may encounter a dead end, which is a localized space of minimal physical distance to the target, but without the target actually being reachable (e.g. the target is separated by a wall or obstruction). The packet must then be diverted (in GPSR, it follows the contour of the barrier that prevents it from reaching the target) until a path to the target is available. In BVR, packets are routed toward the beacon closest to the target node, and then move away from the beacon to reach the target. Each node makes independent forwarding decisions, and thus a Vampire is limited in the distance it can divert the packet. These protocols also fall victim to directional antenna attacks in the same way as link-state and distance-vector protocols above, leading to energy usage increase factor of O(d) per message, where d is the network diameter.

4. ATTACKS ON STATELESS PROTOCOLS

As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected, with some losing almost 10% of their total energy reserve per message. Figure 3(a) diagrams the energy usage when node 0 sends a single packet to node 19 in an example network topology with only honest nodes. Black arrows denote the path of the packet.

Carousel attack: In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. 2 An example of this type of route is in Figure 1(a). In Figure 3(b), malicious node 0 carries out a carousel attack, sending a single message to node 19 (which does not have to be malicious). Note the drastic increase in energy usage along the original path. 3 Assuming the adversary limits the transmission rate to avoid saturating the network, the theoretical limit of this attack is an energy usage increase factor of O (λ), where λ is the maximum route length.

Stretch attack: Another attack in the same vein is the stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. An honest source would select the route Source →F →E →Sink, affecting four nodes including itself, but the malicious node selects a longer route, affecting all nodes in the network. These routes cause nodes that do not lie along the honest route to consume energy by forwarding packets they would not receive in honest scenarios. An example of this type of route is in Figure 1(b). The outcome becomes clearer when we examine Figure 3(c) and compare to the carousel attack. While the latter uses energy at the nodes who were already in the honest path, the former extends the consumed energy "equivalence lines" to a wider Effects of a single-node stretch attacker on a network of 30 nodes after removal of source route length limits. Maliciousness is measured in terms of the induced stretch of the optimal route, in number of hops section of the network. Energy usage is less localized around the original path, but more total energy is consumed.

The true significance of the attack becomes evident in Figure 4(a), which shows network-wide energy consumption in the presence of a single randomly-selected Vampire in terms of the "maliciousness" of the adversary, or the induced stretch of the optimal route in number of hops. (Increasing maliciousness beyond 9 has no effect due to the diameter of our test topology.) Network links become saturated at 10,000 messages per second (even without the stretch attack), but the adversary can achieve the same effects by sending an order of magnitude fewer messages at a stretch attack maliciousness level of 8 or greater. This reduces cumulative network energy by 3%, or almost the entire lifetime of a single node.

Mitigation methods

The carousel attack can be prevented entirely by having forwarding nodes check source routes for loops. While this adds extra forwarding logic and thus more overhead, we can expect the gain to be worthwhile in malicious environments. The ns-2 DSR protocol does implement loop detection, but confusingly does not use it to check routes in forwarded packets. 5 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 [29]. Therefore, it is better to simply drop the packet, especially considering that the sending node is likely malicious (honest nodes should not introduce loops). An alternate solution is to alter how intermediate nodes process the source route. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be automatically truncated (the last instance of the local node will be found in the source route rather than the first). No extra processing is required for this defense, since a node must perform this check anyway — we only alter the way the check is done.

5 .PROVABLE SECURITIES AGAINST VAMPIRE ATTACKS

First we introduce 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. More formally:

Definition 1: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network. (Maliciously-induced route stretch is bounded to a factor of 1.)

No-backtracking implies Vampire resistance. It is not immediately obvious why no-backtracking prevents Vampire attacks in the forwarding phase. Recall the reason for the success of the stretch attack: intermediate nodes in a source route cannot check whether the source-defined route is optimal, or even that it makes progress toward the destination. When nodes make independent routing decisions such as in link-state, distance-vector, coordinate-based, or beacon-based protocols, packets cannot contain maliciously composed routes. This already means the adversary cannot perform carousel or stretch attacks — no node may unilaterally specify a suboptimal path through the network. However, a sufficiently clever adversary may still influence packet progress.

To preserve no-backtracking, we add a verifiable path history to every PLGP packet, similar to route authentications in Ariadne [29] and path-vector signatures in [70]. 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, it this by attaching a non-repayable 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. See Function secure_forward_packet for the modified protocol.

Definition 2: The hop count of packet p, received or forwarded by an honest node, is no greater than the number of entries in p's route attestation field, plus 1.When any node receives a message, it checks that every node in the path attestation 1) has a corresponding entry in the signature chain, and 2) is logically closer to the destination than the previous hop in the chain (see Function secure_forward_packet). This way, forwarding nodes can enforce the forward progress of a message, preserving no-backtracking. If no attestation is present, the node checks to see if the originator of the message is a physical neighbor. Since messages are signed with the originator's key, malicious nodes cannot falsely claim to be the origin of a message, and therefore do not benefit by removing attestations.

6 .CONCLUSIONS

In this paper we defined Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather ex-pose vulnerabilities in a number of popular protocol classes. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly-generated topology of 30 nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000 percent. Theoretical worst-case energy usage can increase by as much as a factor of O(N) per adversary per packet, where N is the network size. We proposed defenses against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

REFERENCES

[1] The network simulator — ns-2. http://www.isi.edu/nsnam/ns/.

[2] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on-demand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.

[4] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[5] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.

[6] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[7] Daniel J. Bernstein, Syn cookies, 1996. http://cr.yp.to/syncookies.html.

[8] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.

[9] Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.

[10] Haowen Chan and Adrian Perrig, Security and privacy in sensor net-works, Computer 36 (2003), no. 10.

[11] Jae-Hwan Chang and Leandros Tassiulas, Maximum lifetime routing in wireless sensor networks, IEEE/ACM Transactions on Networking 12 (2004), no. 4.

[12] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.

[13] Jing Deng, Richard Han, and Shivakant Mishra, Defending against path-based DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.

[14] , INSENS: Intrusion-tolerant routing for wireless sensor net-works, Computer Communications 29 (2006), no. 2.

[15] Sheetalkumar Doshi, Shweta Bhandare, and Timothy X. Brown, An on-demand minimum energy routing protocol for a wireless ad hoc network, ACM SIGMOBILE Mobile Computing and Communications Review 6 (2002), no. 3.

[16] John R. Douceur, The Sybil attack, International workshop on peer-to-peer systems, 2002.

[17] Hans Eberle, Arvinderpal Wander, Nils Gura, Sheueling Chang-Shantz, and Vipul Gupta, Architectural extensions for elliptic curve cryptography over GF(2m) on 8-bit microprocessors, ASAP, 2005.

[18] T. English, M. Keller, Ka Lok Man, E. Popovici, M. Schellekens, and W. Marnane, A low-power pairing-based cryptographic accelerator for embedded security applications, SOCC, 2009.

[19] Laura M. Feeney, An energy consumption model for performance anal-ysis of routing protocols for mobile ad hoc networks, Mobile Networks and Applications 6 (2001), no. 3.

[20] Martin Feldhofer, Sandra Dominikus, and Johannes Wolkerstorfer,
Strong authentication for RFID systems using the AES algorithm, CHES, 2004.

[21]Rodrigo Fonseca, Sylvia Ratnasamy, Jerry Zhao, Cheng T. Ee, David Culler, Scott Shenker, and Ion Stoica, Beacon vector routing: Scalable point-to-point routing in wireless sensornets, NSDI, 2005.

[22] Steven Galbraith, Keith Harrison, and David Soldera, Implementing the tate pairing, Algorithmic number theory, 2002.

[23] Sharon Goldberg, David Xiao, Eran Tromer, Boaz Barak, and Jennifer Rexford, Path-quality monitoring in the presence of adversaries, SIG-METRICS, 2008.

[24] Andrea J. Goldsmith and Stephen B. Wicker, Design challenges for energy-constrained ad hoc wireless networks, IEEE Wireless Communications 9 (2002), no. 4.

[25] R. Govindan and A. Reddy, An analysis of internet inter-domain topology and route stability, INFOCOM, 1997.

[26] Mina Guirguis, Azer Bestavros, Ibrahim Matta, and Yuting Zhang,
Reduction of quality (RoQ) attacks on Internet end-systems, INFOCOM, 2005.

[27] J.L. Hill and D.E. Culler, Mica: a wireless platform for deeply embedded networks, IEEE Micro 22 (2002), no. 6.

[28] Yih-Chun Hu, David B. Johnson, and Adrian Perrig, SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks, IEEE workshop on mobile computing systems and applications, 2002.

[29] Yih-Chun Hu, Adrian Perrig, and David B. Johnson, Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002.