ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Enhanced Data Transmission for Wireless Sensor Networks

Karthick.S, Senthil Kumar.V

KSR College of Engineering, Tiruchengode, Namakkal Dist, Tamilnadu, India

ABSTRACT—Low-power wireless sensor networks square measure associate degree exciting analysis direction in sensing and pervasive computing. previous security work in this space has targeted totally on denial of communication at the routing or medium access management levels. This paper explores resource depletion attacks at the routing protocol layer, that for good disable networks by quickly exhausting nodes' battery power. These "Vampire" attacks are specific to any specific protocol, however rather place confidence in the properties of the many common categories of routing protocols. we discover that all examined protocols square measure inclined to lama attacks, that square measure devastating, tough to observe, and square measure straightforward to carry out victimization as few united malicious business executive causing solely protocol- compliant messages. In the worst case, a single lama will increase network-wide energy usage by an element of O(N*N), wherever N in the variety of network nodes. we have a tendency to discuss strategies and trajectory to mitigate these forms of attacks, together with a replacement proof-of-concept protocol that demonstrably bounds the injury caused by Vampires throughout the packet forwarding section.

KEYWORDS—Denial of service, uncompromised node, no backtracking, device networks, wireless networks, security and routing.

I. INTRODUCTION

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. Due to their sensor organization, wireless sensor networks are particularly vulnerable to denial of service (DoS) attacks [75], and a great deal of research has been done to enhance survivability [2, 5, 13, 14, 50, 75].

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. In this paper we consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks,

since they drain the life from networks nodes. These attacks are distinct from previously-studied 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. While some of the individual attacks are simple, and power-draining and resource exhaustion attacks have been discussed before [53, 59, 68], prior work has been mostly confined to other levels of the protocol stack, e.g. medium access control (MAC) or application layers, and to our knowledge there is little discussion,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks.

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.

Contributions. 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 Ariadne [29], SAODV [78], and SEAD [28] do not protect against Vampire attacks. 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 behaviour and cannot optimize out malicious action. Second, we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary). Third, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

A. Classification

The first challenge in addressing Vampire attacks is defining them — what actions in fact constitute an attack? DoS attack in wired networks are frequently characterized by amplifica- tion [52, 54]: an adversary 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, the act of sending a message is in itself an act of amplification, leading to resource exhaustion, as long as the aggregate cost of routing a message (at the intermediate nodes) is lower than the cost to the source to compose and transmit it. 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. Safety from Vampire attacks implies that this ratio is 1. Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.

B. 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 sensor deployment implies

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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.

While for the rest of this paper we will assume that a node is permanently disabled once its battery power is exhausted, let us briefly consider nodes that recharge their batteries in the field, using either continuous charging or switching between active and recharge cycles. In the continuous charging case, power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge. Assuming that packet processing drains at least as much energy from the victims as from the attacker, a continuously- recharging adversary can keep at least one node permanently disabled at the cost of its own functionality. However, recall that sending any packet automatically constitutes amplifica- tion, allowing few Vampires to attack many honest nodes. We will show later that 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. Dual-cycle networks (with mandatory sleep and awake periods) are equally vulnerable to Vampires during active duty as long as the Vampire's cycle switching is in sync with other 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. However, this defense is only effective when duty cycle groups outnumber Vampires, since it only takes one Vampire per group to carry out the attack.

C. Overview

In the remainder of this paper, we present a series of increasingly damaging Vampire attacks, evaluate the vulner-ability 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 who 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. Lastly, we show how an adversary can target not only packet forwarding but also route and topology discovery phases — if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at every node in the network.

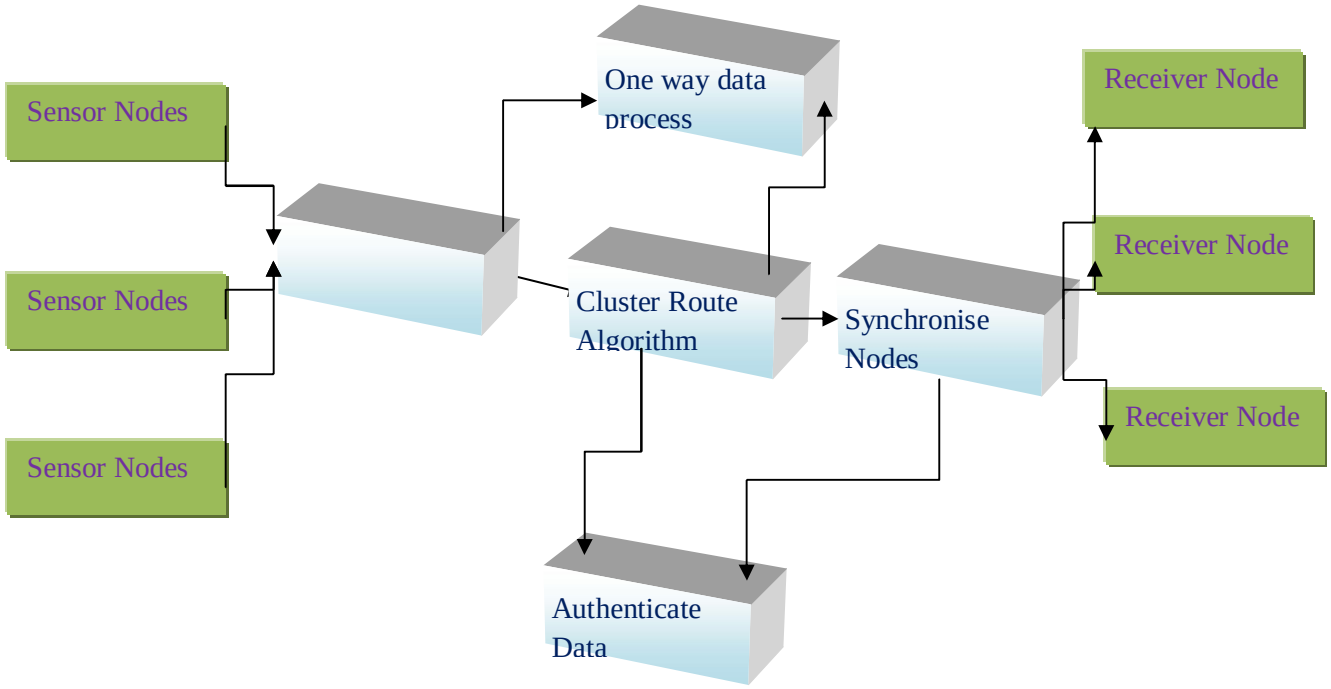
In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles as shown in Fig- ure 1(a). It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. Brief mentions of this attack can be found in other literature [10, 53], but no intuition for defense nor any evaluation is provided. In our second attack, also targeting

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



(a) An honest route would exit the loop immediately from node E to Sink, but a malicious packet makes its way around the loop twice more before exiting.(b) Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

Fig. 1. Malicious route construction attacks on source routing: carousel attack (a) and stretch attack (b).source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We call this the 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. An example is illustrated in Figure 1(b). Results show that in a randomly-generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while 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. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overheard packets, we assume that only messages originated by adversaries may have maliciously-composed routes.

We explore numerous mitigation methods to bound the damage from Vampire attacks, and find that while the carousel attack is simple to prevent with negligible overhead, the stretch attack is far more challenging. The first protection mechanism we consider is loose source routing, where any forwarding node can reroute the packet if it knows a shorter path to the destination. Unfortunately, this proves to be less efficient than simply keeping global network state at each node, defeating the purpose of source routing. In our second attempt, we modify the protocol from [53] to guarantee that a packet makes progress through the network. We call this the no- backtracking property, since it holds if and only if a packet is moving strictly closer to its destination with every hop, and it mitigates all mentioned Vampire attacks with the exception of malicious flooded discovery, which is significantly harder to detect or prevent. We propose a limited topology discovery period ("the night," since this is when vampires are most dangerous), followed by a long packet forwarding period during which adversarial success is provably bounded. We also sketch how to further modify the protocol to detect Vampires during topology discovery and evict them after the network converges (at

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

"dawn").

II. RELATED WORK

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 deplete their batteries faster. Newer research on "denial- of-sleep" only considers attacks at the medium access control (MAC) layer [59]. Additional work mentions resource exhaus- tion 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 re-
sources 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 ad- versary, 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, 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 who 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 no Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high (although with increased latency).

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 pack- ets [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.

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.

Deng et al. discuss path-based DoS attacks and defenses in [13], including using one-way hash chains to limit the number of packets sent by a given node, limiting the rate at which nodes can transmit packets. While this strategy may pro- tect 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-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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
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]). While the authors propose a defense against wormhole and directional antenna attacks (called "Packet Leashes" [30]), their solution comes at a high cost and is not always applicable. First, one flavor of Packet Leashes relies on tightly synchronized clocks, which are not used in most off-the-shelf devices. Second, the authors assume that packet travel time dominates processing time, which may not be borne out in modern wireless networks, particularly low- power wireless sensor networks.

III. ATTACKS ON STATELESS PROTOCOLS

Here we present simple but previously neglected attacks on source routing protocols, such as DSR [35]. In these systems, the source node specifies the entire route to a destination within the packet header, so intermediaries do not make independent forwarding decisions, relying rather on a route specified by the source. To forward a message, the intermediate node finds itself in the route (specified in the packet header) and transmits the message to the next hop. The burden is on the source to ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbor of the previous route hop. This approach has the advantage of requiring very little forwarding logic at intermediate nodes, and allows for entire routes to be sender-authenticated using digital signatures, as in Ariadne [29].

We evaluated both the carousel and stretch attacks (Fig- ure 1) in a randomly-generated 30-node topology and a single randomly-selected malicious DSR agent, using the ns-
2 network simulator [1]. Energy usage is measured for the minimum number of packets required to deliver a single message, so sending more messages increases the strength of the attack linearly until bandwidth saturation.[1] We independently computed resource utilization of honest and malicious nodes and found that malicious nodes did not use a disproportionate amount of energy in carrying out the attack. In other words, malicious nodes are not driving down the cumulative energy of the network purely by their own use of energy. Nevertheless
malicious node energy consumption data is omitted for clarity. The attacks are carried out by a randomly-selected adversary using the least intelligent attack strategy to obtain average expected damage estimates. More intelligent adversaries using more information about the network would be able to increase the strength of their attack by selecting destinations designed to maximize energy usage.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. ATTACKS ON STATEFUL PROTOCOLS

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.

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 mis-forward packets, forcing packet forwarding by nodes who 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. 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.

Directional antenna attack. Vampires have little control over packet progress when forwarding decisions are made independently by each node, but they can still waste energy a directional antenna adversaries can deposit a packet in arbitrary parts of the network, while also forwarding the packet locally. This consumes the energy of nodes that would not have had to process the original packet, with the expected additional honest energy expenditure of O(d), where d is the network diameter, making $\frac{d}{}$ the expected length of the path to an arbitrary destination from the furthest point in the network. This attack can be considered a half-wormhole attack [30], since a directional antenna constitutes a private communication channel, but the node on the other end is not necessarily malicious.[7] It can be performed more than once, depositing the packet at various distant points in the network, at the additional cost to the adversary for each use of the directional antenna. Packet Leashes cannot prevent this attack since they are not meant to protect against malicious message sources, only intermediaries [30].

Malicious discovery attack. Another attack on all

previously-mentioned routing protocols (including stateful and stateless) is spurious route discovery. In most protocols, every node will forward route discovery packets (and sometimes route responses as well), meaning it is possible to initiate a flood by sending a single message. Systems that perform as-needed route discovery, such as AODV and DSR, are particularly vulnerable, since nodes may legitimately initiate discovery at any time, not just during a topology change. A malicious node has a number of ways to induce a perceived topology change: it may simply falsely claim that a link is down, or claim a new link to a non-existent node. Security measures, such as those proposed by Raffo et al. in [58] may be sufficient to alleviate this particular problem. Further, two cooperating malicious nodes may claim the link between them is down. However, nearby nodes might be able to monitor communication to detect link failure (using some kind of neighborhood update scheme). Still, short route failures can be safely ignored in networks of sufficient density. More serious attacks become possible when nodes claim that a long- distance route has changed. This attack is trivial in open networks with unauthenticated routes, since a single node can emulate multiple nodes in neighbor relationships [16], or falsely claim nodes as neighbors. Therefore, let us as- sume closed (Sybil-resistant) networks where link states are authenticated, similar to route authentication in Ariadne [29] or path-vector signatures in [70]. Now our adversary must present an actually changed route in order to execute the attack. To do this, two cooperating

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

adversaries communicating through a wormhole could repeatedly announce and withdraw routes that use this wormhole, causing a theoretical energy usage increase of a factor of O(N) per packet. Adding more malicious nodes to the mix increases the number of possible route announce/withdrawal pairs. Packet Leashes [30] cannot prevent this attack, with the reasoning being similar to the directional antenna attack — since the originators are them- selves malicious, they would forward messages through the wormhole, and return only seemingly valid (and functional) routes in response to discovery. This problem is similar to by restarting a packet in various parts of the network.

V. PROVABLE SECURITY AGAINST VAMPIRE ATTACKS

Here we modify the forwarding phase of PLGP to provably avoid the above-mentioned attacks. First we introduce the no- backtracking property, satisfied for a given packet if and only

```
Function Secure Forward Protocols
  s ← extract_source_address(p);
  a ← extract_attestation(p);
  if (not verify_source_sig(p)) or (empty(a) and not is_neighbor(s)) or (not
  saowf_verify(a)) then
      return ;                          /* drop(p) */
  foreach node in a do
      prevnode ← node*node;
      if (not are_neighbors(node, prevnode)) or
      (not making_progress(prevnode, node)) then
          return ;                      /* drop(p) */

  c ← closest_next_node(s);
  p′ ← saowf_append(p);
  if is_neighbor(c) then forward(p′, c);
  else forward(p′, next_hop_to_non_neighbor(c));
```

last considerably longer than setup, PLGP offers performance comparable to BVR in the average case.

PLGPa includes path attestations, increasing the size of every packet, incurring penalties in terms of bandwidth use, and thus radio power. Adding extra packet verification re- quirements for intermediate nodes also increases processor utilization, requiring time and additional power. Of course there is nothing to be gained in completely non-adversarial environments, but in the presence of even a small number of malicious nodes, the increased overhead becomes worthwhile when considering the potential damage of Vampire attacks.

The bandwidth overhead of our attestation scheme is min- imal, as chain signatures are compact (less than 30 bytes). Comparatively, a minimum-size DSR route request packet with no route, payload, or additional options is 12 bytes [35]; we used 512-byte data packets in our simulations. The additional bandwidth, therefore, is not significant, increasing per-packet transmit power by about 4.8µJ , plus roughly half for addi- tional power required to receive [66].

Energy expenditure for cryptographic operations at inter- mediate hops is, unfortunately, much greater than transmit or receive overhead, and much more dependent on the specific chipset used to construct the sensor. However, we can make an educated guess about expected performance and power costs. Highly-optimized software-only implementations of AES-128, a common symmetric cryptographic primitive, require about 10 to 15 cycles per byte of data on modern 32-bit x86 processors without AES-specific instruction sets or cryptographic co- processors [6]. Due to the rapid growth in the mobile space and increased awareness of security requirements, there has been significant recent work in evaluating symmetric and asymmetric cryptographic performance on inexpensive and low-power devices. Bos et al. report AES-128 performance on 8-bit microcontrollers of 124.6 and 181.3 CPU cycles per byte [9], and Feldhofer et al.report just over 1000 cycles per byte using low-power custom circuits [20]. Surprisingly, although asymmetric

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

cryptography is generally up to two orders of magnitude slower than symmetric, McLoone and Robshaw demonstrate a fast and low-power implementation of an asymmetric cryptosystem for use in RFID tags [47]. Their circuitry uses 400 to 800 cycles per round (on 8- and 16-bit architectures, respectively) in the high-current configuration (comparable in terms of clock cycles to AES for RFID [20], but with half to one-tenth the gates and vastly less power), and 1088 cycles when using about 6 times less current.

Chain signatures are a somewhat more exotic construction, and require bilinear maps, potentially requiring even more costly computation than other asymmetric cryptosystems. Bi- linear maps introduce additional difficulties in estimating over- head due to the number of "pairings"from which implementers can choose. Kawahara et al. use Tate pairings, which are almost universally accepted as the most efficient [22], and show that their Java implementation has similar mobile phone performance as 1024-bit RSA [62] or 160-bit elliptic curve (ECC) [8] cryptosystems [38]. Scott et al. show that modern
32-bit smartcards can compute Tate pairings in as little as
150ms — comparable efficiency to symmetric cryptogra- phy [65]. Furthermore, English et al. show how to construct hardware to perform bilinear map operations in about 75,000 cycles at 50MHz (1.5ms) using 5.79µJ [18].[12] When using specialized hardware for bilinear map computation, power requirements for chain signature-compatible cryptographic op- erations are roughly equivalent to for transmission of the
30-byte chain signature. Assuming a node performs both signature verification as well as a signature append operation, adding attestations to PLGP introduces roughly the same overhead as increasing packet sizes by 90 bytes, taking into account transmit power and cryptographic operations. Without specialized hardware, we estimate cryptographic computation overhead, and thus increased power utilization, of a factor of
2–4 per packet on 32-bit processors, but mostly independent of the route length or the number of nodes in the network: while the hop record and chain signature do grow, their size increase is negligible. In other words, the overhead is constant (O(1)) for a given network configuration (maximum path length), and cannot be influenced by an adversary. Fortunately, hardware cryptographic accelerators are increasingly common and inexpensive to compensate for increased security demands on low-power devices, which lead to increased computational load and reduced battery life [17, 18, 20, 33, 39, 46, 47, 49, 56]. In total, the overhead on the entire network of PLGPa (over PLGP) when using 32-bit processors or dedicated crypto- graphic accelerator is the energy equivalent of 90 additional bytes per packet, or a factor $O(x\lambda)$, where λ is the path length between source and destination and x is 1.2–7.5, depending on average packet size (512 and 12 bytes, respectively). Even without dedicated hardware, the cryptographic computation required for PLGPa is tractable even on 8-bit processors, although with up to a factor of 30 performance penalty, but
this hardware configuration is increasingly uncommon.

VI. SECURING THE DISCOVERY PHASE

Without fully solving the problem of malicious topology discovery, we can still mitigate it by forcing synchronous dis- covery and ignoring discovery messages during the intervening periods. This can lead to some nodes being separated from the network for a period of time, and is essentially a form of rate limiting. Although we rejected rate limiting before, it is acceptable here since discovery should consume a small fraction of running time compared to packet forwarding. We can enforce rate limits in a number of ways, such as neighbor throttling [35] or one-way hash chains [14]. We can also optimize discovery algorithms [32] to minimize our window of vulnerability. If a network survives the high-risk discovery period, it is unlikely to suffer serious damage from Vampires during normal packet forwarding.

While PLGPa is not vulnerable to Vampire attacks during the forwarding phase, we cannot make the same claim about discovery. However, we can give some intuition as to how to further modify PLGPa to bound damage from malicious discovery. (The value of that bound in practice remains an open problem.)

The major issue is that malicious nodes can use directional antennas to masquerade neighbors to any or all nodes in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

the network, and therefore look like a group of size one, with which other groups will try to preferentially merge. Merge requests are composed of the requested group's ID as well as all the group members' IDs, and the receiving node will flood this request to other group members. Even assuming groups generate signed tokens that cost no energy to verify, a Vampire would be able to flood its group with every group descriptor it knows, and use its directional antenna to snoop on broadcasts outside their neighbor range, relaying merge requests from entirely honest groups. Since each Vampire will start as a group of one, other groups will issue merge requests, which the Vampire can deny. In PLGP, denials are only allowed if another merge is in progress, so if we modify the reject message to include the ID of the group with which the merge is in progress (and a signature for non-repudiation), these messages can be kept and replayed at the end of the topology discovery period, detecting and removing nodes who incorrectly deny merge requests. Therefore, Vampires reject legitimate merge requests at their own peril. Any group containing a Vampire can be made to serially join with a "group" composed only of each Vampire in the network (all of them would have to advertise themselves as neighbors of each group). Even wholly honest groups can be fooled using directional antennas: Vampires could maintain the illusion that it is a neighbor of a given group. Since join events require multiparty computation and are flooded throughout the group, this makes for a fairly effective attack. PLGP already provides for the discovery of such subterfuge upon termination of topology discovery: a node who is a member of multiple groups will be detected once those groups join (and all groups are guaranteed to merge by the end of the protocol).

Since PLGP offers the chance to detect active Vampires once the network converges, successive re-discovery periods become safer. This is more than can be said of other protocols, where malicious behaviour during discovery may go undetected, or at least unpunished. However, the bound we can place on malicious discovery damage in PLGPa is still unknown. Moreover, if we can conclude that a single malicious node causes a factor of k energy increase during discovery (and is then expelled), it is not clear how that value scales under collusion among multiple malicious nodes.

VII. CONCLUSION

In this paper we tend to outlined evil spirit attacks, a new category of resource consumption attacks that use routing protocols to for good disable ad-hoc wireless device networks by depleting nodes' battery power. These attacks don't depend upon specific protocols or implementations, however rather ex- create vulnerabilities in an exceedingly variety of standard protocol categories. we tend to showed {a variety and variety} of proof-of-concept attacks against representative samples of existing routing protocols employing a tiny number of weak adversaries, and measured their attack success on a randomly-generated topology of thirty nodes. Simulation results show that reckoning on the situation of the someone, network energy expenditure throughout the forwarding section will increase from between fifty to one,000 p.c. Theoretical worst-case energy usage will increase by the maximum amount as an element of O(N*N) per someone per packet, wherever N is that the network size. we tend to planned defenses against a number of the forwarding-phase attacks and delineate PLGPa, the primary device network routing protocol that demonstrably bounds injury from evil spirit attacks by validating that packets systematically create progress toward their destinations. we've got not offered a totally satisfactory answer for evil spirit attacks throughout the topology discovery section, however advised some intuition concerning injury limitations attainable with additional modifications to PLGPa. Derivation of harm bounds and defenses for topology discovery, likewise 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, Interna- tional 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

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

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(2^m) 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 Communi-cations 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.
[30] , Packet leashes: A defense against wormhole attacks in wireless ad hoc networks, INFOCOM, 2003.
[31] , Rushing attacks and defense in wireless ad hoc network routing protocols, WiSE, 2003.
[32] Yangcheng Huang and Saleem Bhatti, Fast-converging distance vector routing for wireless mesh networks, ICDCS, 2008.
[33] D. Hwang, Bo-Cheng Lai, P. Schaumont, K. Sakiyama, Yi Fan, Shenglin Yang, A. Hodjat, and I. Verbauwhede, Design flow for HW/SW accel-eration transparency in the thumbpod secure embedded system, Design automation conference, 2003.
[34] L. Iannone, R. Khalili, K. Salamatian, and S. Fdida, Cross-layer routing in wireless mesh networks, International symposium on wireless com-munication systems, 2004.
[35] David B. Johnson, David A. Maltz, and Josh Broch, DSR: the dynamic source routing protocol for multihop wireless ad hoc networks, Ad hoc networking, 2001.
[36] Chris Karlof and David Wagner, Secure routing in wireless sensor networks: attacks and countermeasures, IEEE international workshop on sensor network protocols and applications, 2003.
[37] Brad Karp and H.T. Kung, GPSR: Greedy perimeter stateless routing for wireless networks, MobiCom, 2000.
[38] Y. Kawahara, T. Takagi, and E. Okamoto, Efficient implementation of Tate pairing on a mobile phone using Java, International conference on computational intelligence and security, 2006.
[39] Manuel Koschuch, Joachim Lechner, Andreas Weitzer, Johann Groschdl, Alexander Szekely, Stefan Tillich, and Johannes Wolkerstorfer, Hard-ware/software co-design of elliptic curve cryptography on an 8051 microcontroller, CHES, 2006.
[40] Alexander Kröller, Sándor P. Fekete, Dennis Pfisterer, and Stefan Fis- cher, Deterministic boundary recognition and topology extraction for large sensor networks, Annual ACM-SIAM symposium on discrete algorithms, 2006.
[41] Aleksandar Kuzmanovic and Edward W. Knightly, Low-rate TCP- targeted denial of service attacks: the shrew vs. the mice and elephants, SIGCOMM, 2003.
[42] Yu-Kwong Kwok, Rohit Tripathi, Yu Chen, and Kai Hwang, HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks, Networking and mobile computing,
2005.
[43] Xiaojun Lin, N.B. Shroff, and R. Srikant, A tutorial on cross-layer optimization in wireless networks, Selected Areas in Communications,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)
Organized by
Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IEEE Journal on 24 (2006), no. 8.
[44] Xiapu Luo and Rocky K. C. Chang, On a new class of pulsing denial- of-service attacks and the defense, NDSS, 2005.
[45] Morteza Maleki, Karthik Dantu, and Massoud Pedram, Power-aware source routing protocol for mobile ad hoc networks, ISLPED, 2002.
[46] Yusuke Matsuoka, Patrick Schaumont, Kris Tiri, and Ingrid Ver- bauwhede, Java cryptography on kvm and its performance and security optimization using hw/sw co-design techniques, CASES, 2004.
[47] M. McLoone and M. Robshaw, Public key cryptography and RFID tags, CT-RSA, 2006.
[48] Timothy J. McNevin, Jung-Min Park, and Randolph Marchany, pTCP: A client puzzle protocol for defending against resource exhaustion denial of service attacks, Technical Report TR-ECE-04-10, Department of Electrical and Computer Engineering, Virginia Tech, 2004.
[49] V.P. Nambiar, M. Khalil-Hani, and M.M.A. Zabidi, Accelerating the AES encryption function in OpenSSL for embedded systems, ICED, 2008.
[50] Asis Nasipuri and Samir R. Das, On-demand multipath routing for mobile ad hoc networks, International conference on computer communications and networks, 1999.
[51] L.B. Oliveira, D.F. Aranha, E. Morais, F. Daguano, J. Lopez, and R. Dahab, TinyTate: Computing the Tate pairing in resource-constrained sensor nodes, NCA, 2007.
[52] Kihong Park and Heejo Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, INFOCOM, 2001.
[53] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.
[54] Vern Paxson, An analysis of using reflectors for distributed denial-of- service attacks, SIGCOMM Comput. Commun. Rev. 31 (2001), no. 3.
[55] Charles E. Perkins and Pravin Bhagwat, Highly dynamic destination- sequenced distance-vector routing (DSDV) for mobile computers, Conference on communications architectures, protocols and applications, 1994.
[56] R. Potlapally, S. Ravi, A. Raghunathan, R.B. Lee, and N.K. Jha, Impact of configurability and extensibility on IPSec protocol execution on embedded processors, International conference on VLSI design, 2006.
[57] Marcin Poturalski, Panagiotis Papadimitratos, and Jean-Pierre Hubaux, Secure neighbor discovery in wireless networks: Formal investigation of possibility, ACM ASIACCS, 2008.
[58] Daniele Raffo, Cédric Adjih, Thomas Clausen, and Paul Mühlethaler, An advanced signature system for OLSR, SASN, 2004.
[59] 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.
[60] David R. Raymond and Scott F. Midkiff, Denial-of-service in wireless sensor networks: Attacks and defenses, IEEE Pervasive Computing 7 (2008), no. 1.
[61] Jennifer Rexford, Jia Wang, Zhen Xiao, and Yin Zhang, BGP routing stability of popular destinations, IMW, 2002.
[62] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM 21 (1978), no. 2.
[63] Volkan Rodoplu and Teresa H. Meng, Minimum energy mobile wireless networks, IEEE Journal on Selected Areas in Communications 17 (1999), no. 8.
[64] 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.
[65] Michael Scott, Neil Costigan, and Wesam Abdulwahab, Implementing cryptographic pairings on smartcards, CHES, 2006.
[66] Rahul C. Shah and Jan M. Rabaey, Energy aware routing for low energy ad hoc sensor networks, WCNC, 2002.
[67] Suresh Singh, Mike Woo, and C. S. Raghavendra, Power-aware routing in mobile ad hoc networks, MobiCom, 1998.
[68] Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.
[69] Ivan Stojmenovic and Xu Lin, Power-aware localized routing in wireless networks, IEEE Transactions on Parallel and Distributed Systems 12 (2001), no. 11.
[70] Lakshminarayanan Subramanian, Randy H. Katz, Volker Roth, Scott Shenker, and Ion Stoica, Reliable broadcast in unknown fixed-identity networks, Annual ACM SIGACT-SIGOPS symposium on principles of distributed computing, 2005.
[71] Haibin Sun, John C. S. Lui, and David K. Y. Yau, Defending against low-rate TCP attacks: dynamic detection and protection, ICNP, 2004.
[72] Curtis Villamizar, Ravi Chandra, and Ramesh Govindan, BGP route flap damping, 1998.
[73] Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford, CAPTCHA: Using hard AI problems for security, Eurocrypt, 2003.
[74] Yue Wang, Jie Gao, and Joseph S.B. Mitchell, Boundary recognition in sensor networks by topological methods, Annual international conference on mobile computing and networking, 2006.
[75] Anthony D. Wood and John A. Stankovic, Denial of service in sensor networks, Computer 35 (2002), no. 10.
[76] Guang Yang, M. Gerla, and M.Y. Sanadidi, Defense against low-rate TCP-targeted denial-of-service attacks, ISCC, 2004.
[77] Jun Yuan, Zongpeng Li, Wei Yu, and Baochun Li, A cross-layer opti- mization framework for multihop multicast in wireless mesh networks, IEEE Journal on Selected Areas in Communications 24 (2006), no. 11.
[78] Manel Guerrero Zapata and N. Asokan, Securing ad hoc routing proto- cols, WiSE, 2002.