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. 2, February 2014, pg.328 – 336

RESEARCH ARTICLE

VAMPIRE ATTACKS: PROTOCOL ROUTING INFRASTRUCTURE IN WIRELESS SENSOR NETWORKS

T.Nivethitha[1], S.Muthukrishnan[2], S. Navaneethakrishnan[3]

[1] PG Scholar, Electronics and communication, Sri Eshwar college of Engineering, Tamil Nadu, India
[2]Professor, Electronics and communication, Sri Eshwar college of Engineering, Tamil Nadu, India
[3]PG Scholar, Electronics and communication, Sri Eshwar college of Engineering, Tamil Nadu, India
Nivethitha1704@gmail.com, logisweety@gmail.com, navaneethan2eee@gmail.com

Abstract

Ad hoc low-power wireless networks square measure an 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. It explores resource depletion attacks at the routing protocol layer that for good disable networks by quickly exhausting nodes battery power. These "Vampire" attacks don't seem to be specific to any specific protocol, however rather trust the properties of the many standard categories of routing protocols. We discover that each one examined protocols square measure liable to lamia attacks, that square measure devastating, troublesome to observe, and are easy to hold out victimization as few in concert malicious business executive causation solely protocol-compliant messages. We have a tendency to discuss ways to mitigate these styles of attacks, as well as a brand new proof-of-concept protocol that incontrovertibly bounds the injury caused by Vampires during the packet forwarding section.

Keywords: WSN, Routing, malicious adversaries, lamia attacks

1. INTRODUCTION

Circumstantial wireless detector networks (WSNs) promise exciting new applications within the close to future, such as ubiquitous on-demand computing power, continuous property, and instantly deployable communication for military and 1st responders. Such networks already monitor environmental conditions, industrial plant performance, and troop preparation, to call a number of applications. As WSNs become a lot of and a lot of crucial to the everyday functioning of individuals and organizations, convenience faults become less tolerable—lack of convenience will create the difference between business as was common and lost productivity, power outages, environmental disasters, and even lost lives; thus high convenience of those networks could be an essential property, and may hold even below malicious conditions. Due to their circumstantial organization, wireless circumstantial networks are notably susceptible to denial of service (DoS) attacks and an excellent deal of analysis has been done to boost survivability]. While these schemes will forestall attacks on the short-term availability of a network, they are doing not address attacks that have an effect on semi-permanent availability—the most permanent denial of service attack is to completely expend nodes' batteries. This can be associate instance of a resource depletion attack, with battery power because the resource of interest. During this paper, we think about however routing protocols, even those designed to be secure, lack protection from these attacks, that we have a tendency to decision. Vampire attacks, since they drain the life from networks nodes. These attacks square measure distinct from antecedently studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they are doing not disrupt immediate convenience, but rather work over time to completely disable a network. Whereas a number of the individual attacks square measure easy, and power debilitating and resource exhaustion attacks are mentioned before previous work has been principally confined to alternative levels of the protocol stack, e.g., medium access management (MAC) or application layers, and to our information there's little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks. Vampire attacks don't seem to be protocol-specific, therein they are doing not suppose style properties or implementation faults of particular routing protocols, however rather exploit general properties of protocol categories like link-state, distance vector, source routing, and geographic and beacon routing. Neither do these attacks suppose flooding the network with large amounts of information, however rather try and transmit as very little data as do able to realize the most important energy drain, preventing a rate limiting answer. Since Vampires use protocol-compliant messages, these attacks square measure terribly troublesome to detect and forestall

CONTRIBUTIONS:

This paper makes 3 primary contributions. First, we tend to completely assess the vulnerabilities of existing protocols to routing layer battery depletion attacks. we tend to observe that security measures to forestall Vampire attacks are orthogonal to those accustomed shield routing infrastructure, then existing secure routing protocols such as Ariadne , SAODV , and SEAD don't defend against lamia attacks. Existing work on secure routing attempts to confirm that adversaries cannot cause path discovery to come associate invalid network path, however Vampires do not disrupt or alter discovered ways, instead victimization existing valid network ways and protocol-compliant messages. Protocols that maximize power potency are also inappropriate, since they admit cooperative node behavior and can't optimize out malicious action .Second, we show simulation results quantiying the performance of several representative protocols within the presence of one Vampire (insider adversary). Third, we have a tendency to modify associate existing sensor network routing protocol to incontrovertibly certain the damage from evil spirit attacks throughout packet forwarding.

1.1 Overview

In the remainder of this paper, we tend to present a series of increasingly damaging lamia attacks, measure the vulnerability of many example protocols, and recommend how to improve resilience. In source routing protocols, we show however a malicious packet source will specify methods through the network that are so much longer than optimum, wasting energy at intermediate nodes United Nations agency forward the packet supported the enclosed source route.

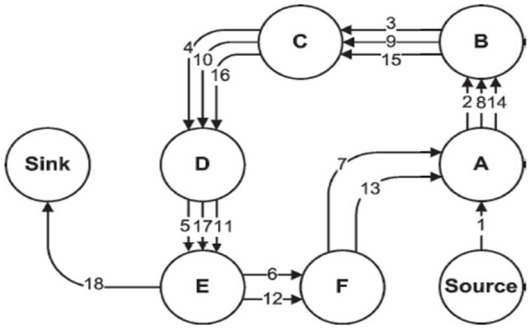


Fig -1 :A honest node would exit the loop immediately from node E to Sink, but the malicious packets makes its way around the loop twice more before exiting

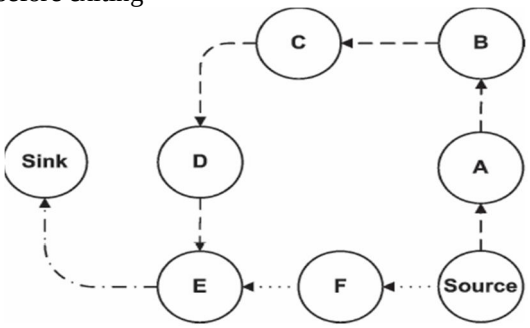


Fig -2: Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

In routing schemes, wherever forwarding selection are created severally by every node (as opposition nominal by the source), we recommend however directional antenna and hole attacks are often accustomed deliver packets to multiple remote network positions, forcing packet process at nodes that may not usually receive that packet in the least, and therefore increasing network-wide energy expenditure. Lastly, we tend to show however an adversary will target not solely packet forwarding however additionally route and topology discovery phases—if discovery messages are flooded, an person can, for the value of one packet, consume energy at every node within the network .In our initial attack, associate adversary composes packets with purposely introduced routing loops. we tend to call it the carousel attack, since it sends packets in a circle as shown in Fig. 1. It targets source routing protocols by exploiting the restricted verification of message headers at forwarding nodes, allowing one packet to repeatedly traverse identical set of nodes. Transient mentions of this attack will be found in other literature however no intuition for defense nor any analysis is provided. In our second attack, also targeting source routing, associate adversary constructs unnaturally long routes, doubtless traversing each node within the network. We call this the stretch attack, since it will increase packet path lengths, inflicting packets to be processed by variety of nodes that's freelance of hop count on the shortest path between the adversary and packet destination. An example is illustrated in Fig. 2. Results show that during a randomly generated topology, one assaulter will use a carousel attack to extend energy consumption by the maximum amount as an element of four, whereas stretch attacks increase energy usage by up to associate order of magnitude, reckoning on the position of the malicious node. The impact of those attacks will be further exaggerated by combining them, increasing the number of adversarial nodes within the network, or simply sending additional packets. though in networks that don't employ authentication or solely use end-to-end authentication, adversaries are absolve to replace routes in any overheard packets, we tend to assume that solely messages originated by adversaries may have maliciously composed routes. We explore various mitigation strategies to bound the damage from lamia attacks, and realize that while the carousel attack is easy to stop with negligible overhead, the stretch attack is much tougher. The first protection mechanism we have a tendency to take into account is loose source routing, where any forwarding node will reroute the packet if it knows a shorter path to the destination. Unfortunately, this proves to be less economical than merely keeping international network state at every node, defeating the aim of source routing. In our second try, we have a tendency to modify the protocol from to ensure that a packet makes progress through the network. We have a tendency to call this the no-backtracking property, since it holds if and providing a packet is moving strictly nearer to its destination with each hop, and it mitigates all mentioned lamia attacks with the exception of malicious flooded discovery, that is considerably harder to sight or forestall. we have a tendency to propose a restricted topology discovery amount ("the night," since this can be once vampires are most dangerous), followed by an extended packet forwarding period throughout that

adversarial success is incontrovertibly bounded. We have a tendency to additionally sketch the way to any modify the protocol to observe Vampires throughout topology discovery and evict them once the network converges (at "dawn").

1.2 ATTACKS ON STATELESS PROTOCOL

Here, we tend to present straight forward but antecedently neglected attacks on source routing protocols, like DSR. In these systems, the supply node specifies the complete route to a destination at intervals the packet header, thus intermediaries do not create freelance forwarding selections, relying rather on a route nominal by the source. To forward a message, the intermediate node finds itself within the route and transmits the message to subsequent hop. The burden is on the supply to confirm that the route is valid at the time of causing, which each node within the route could be a physical neighbor of the previous route hop. This approach has the advantage of requiring little or no forwarding logic at intermediate nodes, and permits for entire routes to be sender exploitation digital signatures, as in Ariadne. We evaluated each the carousel and stretch attacks (Fig. 1) in a very arbitrarily generated 30-node topology and a single arbitrarily designated malicious DSR agent, exploitation the ns-2 network machine [1]. Energy usage is measured for the minimum variety of packets needed to deliver one message, thus causing additional messages will increase the strength of the attack linearly till information measure saturation.1 We independently computed resource utilization of honest and malicious nodes and located that malicious nodes didn't use a disproportionate quantity of energy in winding up the attack. In different words, malicious nodes aren't driving down the accumulative energy of the network strictly by their own use of energy. Not with standing, malicious node energy consumption information are omitted for clarity. The attacks are carried out by arbitrarily designated somebody exploitation the smallest amount intelligent attack strategy to get average expected injury estimates. Additional intelligent adversaries' exploitation additional info about the network would be ready to increase the strength of their attack by choosing destinations designed to maximize energy usage.

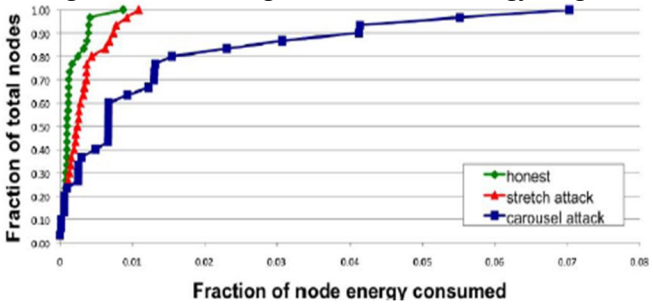


Fig -3:Per-node energy usage for both the attacks is shown

CAROUSEL ATTACKS: During this attack, associate degree resister sends a packet with a route composed as a series of loops, specified identical node seems within the route repeatedly. This strategy may be used to increase the route length on the far side the quantity of nodes within the network, solely restricted by the quantity of allowed entries within the supply route.2 associate degree example of this type of route is in Fig. 1. Overall energy consumption will increase by up to an element of 3.96 per message. On average, a indiscriminately placed carousel assaulter in our example topology will increase network energy consumption by an element of 1:48 0:99. The reason for this huge variance is that the attack does not continuously increase energy usage—the length of the adversarial path could be a multiple of the honest path that is in turn; full of the position of the resister in relevance the destination, that the adversary's position is very important to the success of this attack.

STRETCH ATTACKS: Another attack within the same vein is that the stretch attack, wherever a malicious node constructs by artificial means long source routes, inflicting packets to traverse a bigger than optimal range of nodes. An honest supply would choose 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 might not receive in honest scenarios. an example of this sort of route is in Fig. 2.

2. MITIGATION STRATEGIES

The carousel attacks are often prevented entirely by having forwarding nodes check supply routes for loops. While this adds further forwarding logic and so a lot of overhead, we can expect the gain to be worthy in malicious environments. The ns-2 DSR protocol will implement loop detection, however bewilderingly doesn't use it to examine routes in forwarded packets.5 once a loop is detected, the source route might be corrected and therefore the packet sent on, but one of the attractive options of source routing is that the route ca itself be signed by the source . Therefore, it's better to simply drop the packet, particularly considering that the sending node is probably going malicious (honest nodes shouldn't introduce loops). An alternate answer is to change however intermediate nodes method the supply route. To forward a message, a node should verify consecutive hop by locating itself within the source route. If a node searches for itself from the destination backward instead from the supply forward, any loop that has the present node are going to be mechanically truncated (the last instance of the native node are going to be found within the supply route instead of the first). No extra processing is needed for this defense, since a node should perform this check anyway—we solely alter the method the check is completed .The stretch attack is tougher to forestall. Its success rests on the forwarding node not checking for optimality of the route. If we tend to decision the no optimization case "strict" supply routing, since the route is followed precisely as specified in the header, we are able to outline loose supply routing, where intermediate nodes could replace half or all of the route within the packet header if they understand of a stronger route to the destination. This makes it necessary for nodes to discover and cache best routes to a minimum of some fraction of different nodes, partly defeating the as-needed discovery advantage. Moreover, caching should be done rigorously lest a maliciously suboptimal route be introduced. We tend to simulated the loose supply routing defense mistreatment random-length suboptimal ways in at random generated network topologies of up to 1,000,000 nodes, with diameter 10-14..The amount of nodes traversed by loose source routed packets is suboptimal by a minimum of an element of ten, with some routes approaching an element of fifty. Only a few messages encountered a node with a stronger path to the destination than the originally appointed long supply route. Therefore we tend to conclude that loose supply routing is worse than keeping international state at each node. Alternatively, we are able to sure the damage of carousel and stretch attackers by limiting the allowed supply route length based on the expected most path length within the network, however we might want the simplest way to work out the network diameter.6 whereas there square measure appropriate algorithms there has been little work on whether or not they may yield correct leads to the presence of adversaries. If the number of nodes is understood prior time, graph-theoretic techniques is wont to estimate the diameter.

2.1 BEACON BASED PROTOCOLS

Some recent routing analysis has moved within the direction of coordinate- and beacon-based routing, like GPSR and BVR ,that use physical coordinates or beacon distances for routing, severally. In GPSR, a packet could encounter a dead finish, that could be a localized house of borderline physical distance to the target, however while not the target actually being accessible (e.g., the target is separated by a wall or obstruction). The packet should then be diverted (in GPSR, it follows the contour of the barrier that stops it from reaching the target) till a path to the target is available. In BVR, packets area unit routed toward the beacon closest to the target node, then move faraway from the beacon to succeed in the target. every node makes freelance forwarding selections, and therefore a lamia is restricted within the distance it will divert the packet. These protocols conjointly fall victim to antenna attacks within the same manner as link-state and distance-vector protocols .

2.2 CLEAN SLATE DETECTOR NETWORK ROUTING

In this section, we tend to show that a clean-slate secure device network routing protocol by Parno et al. ("PLGP" from here on) will be changed to demonstrably resist lamia attacks during the packet forwarding section. the initial version of the protocol, though designed for security, is vulnerable to lamia attacks. PLGP consists of a topology discovery phase, followed by a packet forwarding section, with the former optionally recurrent on a set schedule to confirm that topology info stays current. (There isn't any on demand discovery.) Discovery deterministically organizes nodes into a tree which will later be used as an addressing scheme. once discovery begins, every node contains restricted view of the network—the node is aware of solely itself. Nodes discover their neighbors exploitation native broadcast, and form ever increasing "neighborhoods," stopping once the complete network could be a single cluster. Throughout this method, nodes build a tree of neighbor relationships and cluster membership that

will later be used for addressing and routing. At the tip of discovery, every node ought to calculate the same address tree as different nodes. All leaf nodes within the tree are physical nodes within the network, and their virtual addresses correspond to their position within the tree (see Fig. 4). All nodes learn every others' virtual addresses and cryptographic keys. the ultimate address tree is verifiable once network convergence, and every one forwarding choices may be independently verified. moreover, forward every legitimate network node contains a distinctive certificate of membership (assigned before network deployment), nodes who try to join multiple teams, manufacture clones of themselves in multiple locations, or otherwise cheat throughout discovery will be known and evicted.

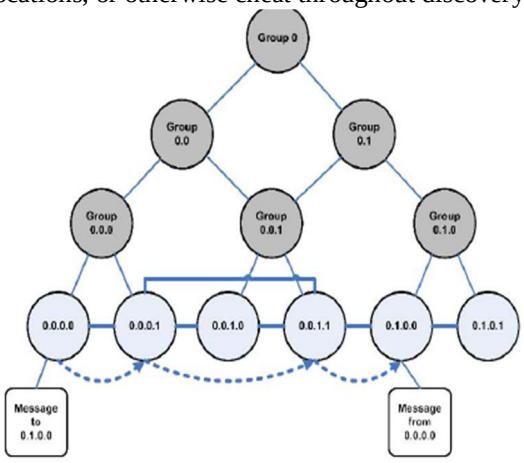


Fig -4 : The address tree for a fully converged six-node network.

Topology discovery: Discovery begins with a time limited period throughout which each and every node should announce its presence by broadcasting a certificate of identity, including its public key (from currently on brought up as node ID), signed by a trusty offline authority. every node starts as its own cluster of size one, with a virtual address zero. every node stores the identity of 1 or additional nodes through that it detected an announcement that another group exists. That node might have itself detected the information used, thus each node among a bunch will find yourself with a next-hop path to each multiple cluster, as in distance vector. Topology discovery takings during this manner till all network nodes square measure members of one group. By the tip of topology discovery, every node learns every different node's virtual address, public key, and certificate, since each cluster members is aware of the identities of all multiple cluster members and also network converges single cluster.

Packet Forwarding: Throughout the forwarding part, all decisions square measure created severally by every node. When receiving a packet, a node determines future hop by finding the foremost vital little bit of its address that differs from the message originator's address (see Fig. 4). Thus, every forwarding event (except once a packet is moving
within a bunch so as to achieve a entranceway node to proceed to future group) shortens the logical distance to the destination, since node addresses ought to be strictly closer to the destination.

2.3 PLGP IN THE PRESENCE OF VAMPIRE:

In PLGP, forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any **part** of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks. Consider for instance the now-familiar directional antenna attack: a receiving honest node may be farther away from the packet destination than the malicious forwarding node, but the honest node has no way to tell that the packet it just received is moving away from the destination; the only information available to the honest node is its own address and the packet destination address, but not the address of the previous hop (who can lie). Thus, the Vampire can move a packet away from its destination without being detected. The situation is worse if the packet returns to the Vampire in the process of being forwarded—it can now be rerouted again, causing something similar to the carousel attack. Recall that the damage from the carousel attack is bounded by the maximum length of the source route, but in PLGP the adversary faces no such limitation, so the packet can cycle indefinitely. Nodes may sacrifice some local storage to retain a record of recent packets to prevent this attack from being carried out repeatedly with the same packet. Random direction vectors, as suggested in PLGP, would

likewise alleviate the problem of indefinite cycles by avoiding the same malicious node during the subsequent forwarding round.

2.4 PROVABLE SECURITY AGAINST VAMPIRE ATTACKS:

Here, we have a tendency to modify the forwarding part of PLGP to incontrovertibly avoid the above-named attacks. First we have a tendency to introduce the no-backtracking property, satisfied for a given packet if and only if it systematically makes progress toward its destination in the logical network address house. a lot of formally: **Definition one**. No-backtracking is satisfied if each packet p traverses identical variety of hops whether or not or not an individual is present within the network. (Maliciously evoked route stretch is bounded to an element of one.) This doesn't imply that each packet within the network must travel identical variety of hops no matter supply or destination, however rather that a packet sent to node D by a malicious node at location L can traverse identical variety of hops as a packet sent to D by a node at location L that's honest. If we predict of this in terms of protocol execution traces, no-backtracking implies that for every packet within the trace, the amount of intermediate honest nodes traversed by the packet between supply and destination is freelance of the actions of malicious nodes. Equivalently, traces that include malicious nodes ought to show identical network wide energy utilization by honest nodes as traces of a network with no malicious actors. the sole notable exceptions area unit once adversaries drop or mangle packets en route, however since we have a tendency to area unit solely involved with packets initiated by adversaries, we will safely ignore this situation: "premangled" packets result—they can be born by associate degree honest negotiant or destination. No-backtracking implies evil spirit resistance. It is not right away obvious why no-backtracking prevents Vampire attacks within the forwarding part. Recall the rationale for the success of the stretch attack: intermediate nodes in an exceedingly source route cannot check whether or not the supply-defined route is perfect, or maybe that it makes progress toward the destination. once nodes create freelance routing decisions like in link-state, distance-vector, coordinate- based, or beacon-based protocols, packets cannot contain maliciously composed routes. To preserve no-backtracking, we have a tendency to add a verifiable path history to each PLGP packet, like route authentications in Ariadne and path-vector signatures in. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history at the side of PLGP's tree routing structure so each node will firmly verify progress, preventing any significant adversarial influence on the trail taken by any packet which traverses a minimum of one honest node. Whenever node n forwards packet p, it this by attaching a non –replayable attestation (signature). These signatures kinda series attached to each packet, permitting any node receiving it to validate its path. each forwarding node verifies the attestation chain to make sure that the packet has ne'er traveled far from its destination within the logical address space.

2.5 PERFORMANCE ISSUES

PLGP imposes exaggerated setup price over BVR, but compares favourably to in terms of packet forwarding overhead. whereas path stretch will increase by an element of one.5-2, message delivery success while not resorting to localized flooding is improved: PLGP ne'er floods, whereas BVR should flood 5-10 p.c of packets depending on network size and topology . PLGP conjointly demonstrates additional just routing load distribution and path diversity than BVR. Since the forwarding part ought to last significantly longer than setup, PLGP offers performance comparable BVR in the average case. PLGPa includes path attestations, increasing the scale of every packet, acquisition penalties in terms of information measure use, and therefore radio power.

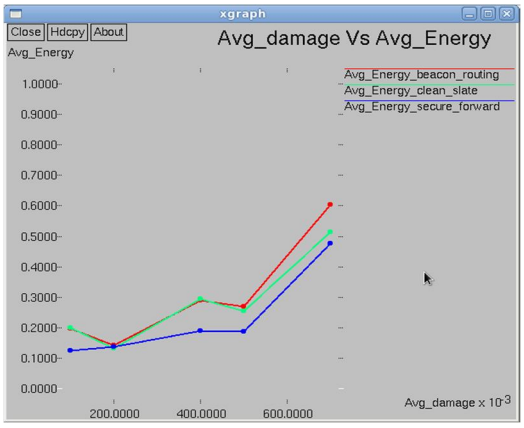
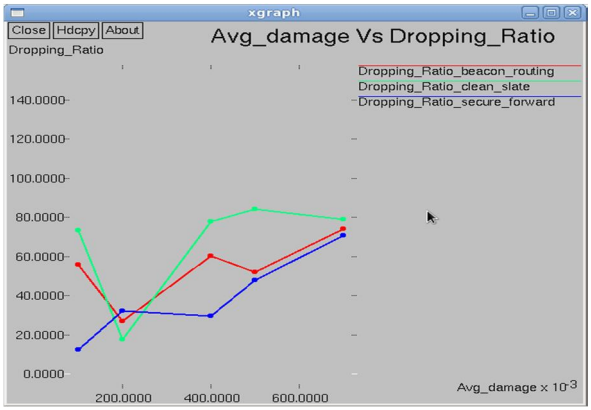


Fig -5 : comparison of damage with energy with respective to Beacon- routing, Clean-slate , secure forward routing.

Adding further packet verification requirements for intermediate nodes conjointly will increase processor utilization, requiring time, and extra power. The information measure overhead of our attestation theme is minimal, as chain signatures are compact (less than thirty bytes). relatively, a minimum-size DSR route request packet with no route, payload, or further choices is twelve bytes; we have a tendency to used 512-byte knowledge packets in our simulations.



The additional information measure, therefore, isn't important, increasing per-packet transmit power by concerning 4:8 J, plus roughly 0.5for added power needed to receive. Energy expenditure for crypto-logical operations at intermediate hops is, sadly, abundant larger than transmit or receive overhead, and far additional dependent on the particular chipset wont to construct the device. Even while not dedicated hardware, the crypto-logical computation needed for PLGPa is tractable even on 8-bit processors, though with up to an element of thirty performance penalty, however this hardware configuration is increasingly uncommon.

CONCLUSION

In this paper, we tend to outlined lamia attacks, a replacement category of resource consumption attacks that use routing protocols to permanently disable circumstantial wireless device networks by depleting nodes' battery power. These attacks don't depend on explicit protocols or implementations, but rather expose vulnerabilities in a very variety of standard protocol categories. we tend to showed variety of proof-of-concept attacks against representative samples of existing routing protocols employing a tiny variety of weak adversaries, and measured their attack success on a indiscriminately generated topology of thirty nodes. Simulation results show that depending on the situation of the human, network energy expenditure throughout the forwarding part will increase from between fifty to one,000 p.c. We proposed defenses against a number of the forwarding-phase attacks and delineated

PLGPa, the primary device network routing protocol that demonstrably bounds injury from Vampire attacks by corroboratory that packets systematically make progress toward their destinations. we've got no offered a completely satisfactory answer for lamia attacks during the topology discovery part, however instructed some intuition concerning injury limitations attainable with more modifications to PLGPa. Derivation of harm bounds and defenses for topology discovery, additionally as handling mobile networks, is left for future work.

ACKNOWLEDGEMENT

The authors would like to thank Prof.S.Muthukrishanan for his valuable guidance and the anonymous reviewers for their helpful comments on earlier drafts of the work.

REFERENCES

[1] "The Network Simulator – ns- 2,"http://www.isi.edu/nsnam/ns, 2012.
[2] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On- Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006..
[3] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001..
[4] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
[5] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

