International Journal of Science Engineering and Advance Technology

# The Process to disable ADHOC wireless sensor networks by depleting power using routing protocols

1 **Sri. M. Vamsi Krishna,** 2 **N.Santoshi Lakshmi**
1,2Dept. of CSE, Chaitanya Institute of Science & Technology, Kakinada, AP, India

**Abstract:**

The consequence 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. Whereas this is by no means a comprehensive list of routing protocols which are susceptible to Vampire attacks we analysis the covered protocols as a significant subset of the routing solution space and stress that our attacks are probable to apply to other protocols. Assuming that packet giving out drains at least as much energy from the victims as from the attacker a incessantly recharging adversary can keep at least one node enduringly disabled at the cost of its own functionality. However recall that sending any packet automatically constitutes augmentation allowing few Vampires to attack many honest nodes. Dual-cycle networks with mandatory sleep and awake periods are evenly susceptible to Vampires during active duty as long as the Vampire's cycle switching is in sync with other nodes. Vampire attacks may be damaged 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. Though this security is only successful when duty cycle groups outnumber Vampires given that it only takes one Vampire per group to carry out the attack.

**Keywords:** Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks.

**Introduction:**

We present a sequence of increasingly damaging Vampire attacks appraise the susceptibility of several example protocols and recommend how to recover flexibility. In source routing protocols we be evidence for how a malicious packet source can denote paths through the network which are distant longer than most favourable wasting energy at in-between nodes that forward the packet based on the integrated source route. In routing schemes where forwarding decisions are made autonomously by each node as opposed to specified by the source we recommend how directional antenna and wormhole attacks can be used to distribute packets to many remote network positions forcing packet processing at nodes that would not usually receive that packet at all and thus increasing network-wide energy expenditure. Finally we show how an adversary can intention 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. All routing protocols employ at least one topology discovery period as ad hoc deployment entails no previous position knowledge. Limiting ourselves to irreversible but dynamically organized topologies as in most wireless sensor networks we further distinguish on-demand routing protocols where topology discovery is done at transmission time and static protocols where topology is discovered during an early setup phase with periodic rediscovery to grip rare topology changes.

**Related Work:**

Even in non power constrained systems reduction of resources such as memory CPU time and bandwidth may effortlessly cause problems. A popular instance is the SYN flood attack in which adversaries make numerous connection requests to a server which will assign resources for each connection request ultimately running out of resources while the adversary who assigns negligible resources remains operational since it does not aim to ever complete the connection handshake. Such attacks can be overcome or attenuated by

putting greater burden on the connecting entity e.g. SYN cookies which relieve of the early connection state onto the client or cryptographic puzzles. These solutions place smallest load on genuine clients who only commence a small number of connections but dissuade malicious entities who will challenge a large number. Note that this is actually a form of rate limiting and not always desirable as it punishes nodes that produce burst 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 adequately effectual to validate the surplus load on legitimate nodes.

**Existing Method:**

Networks already examine environmental conditions, factory performance and troop deployment to name a few applications. Protocols that make the most of power effectiveness are also inappropriate since they rely on cooperative node performance and cannot optimize out malevolent deed. The effort to protect routing attempts to guarantee that adversaries cannot cause path discovery to return an invalid network path but Vampires do not disturb or modify discovered paths instead by means of existing valid network paths and protocol compliant messages. Since Vampire attacks depend on amplification such solutions may not be adequately effective to validate the excess load on justifiable nodes.

**Disadvantages:**

They do not address attacks that affect long-term availability and power outages. Loss of productivity and various DOS attacks. Security level is low. Loss of information due to environmental disasters.

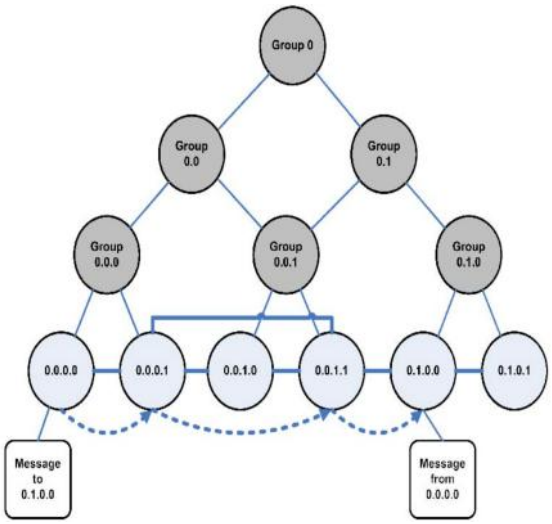
**Proposed Method:**

Modifying an existing sensor network routing protocol to provably bind the damage from Vampire attacks during packet forwarding. Thorough estimation of the vulnerabilities of existing protocols to routing layer battery depletion attacks and observation of security procedures to avoid Vampire attacks are orthogonal to those used to protect routing infrastructure and so existing secure routing protocols such as Ariadne, SAODV and SEAD do not protect against Vampire attacks. Protocols that maximize power efficiency are also inapt since they depend on cooperative node behaviour and cannot optimize out malicious action. Illustration of simulation consequences quantifying the presentation of several representative protocols in the presence of a single Vampire insider adversary.

**Advantages:**

Boost up the Battery power. Secure level is High. Protect From The Vampire Attacks.

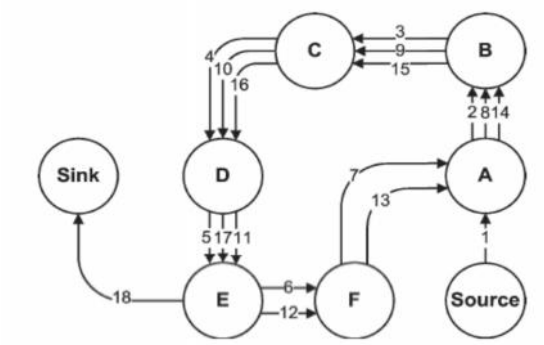
**The Final Address Tree For A Fully Converged Six-Node Network:**




Every node learns each other's effective addresses and cryptographic keys. The final address tree is demonstrable after network convergence and all forwarding decisions can be separately verified. Moreover assuming each justifiable network node has a exclusive certificate of membership assigned before network deployment nodes who effort to join multiple groups produce clones of themselves in multiple locations or otherwise deceive during discovery can be recognized and expelled.

 ISSN 2321-6905

**Malicious Route Construction Attacks On Source Routing:**




(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.

It aims source routing protocols by exploiting the incomplete verification of message headers at forwarding nodes allowing a single packet to repeatedly traverse the same set of nodes. In our second attack also targeting source routing an adversary constructs unnaturally long routes potentially traversing every node in the network. We call this the stretch attack since it augments 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 adversary composes packets with deliberately introduced routing loops. We call it the carousel attack since it transmits packets in circles.

**Data-Verification:**

For occurrence data approach with malicious node that is positioned in malicious packet or else data located in honest packet. This way user verifies the data's. In data verification module receiver validates the path.

**Denial Of Service:**

A denial-of-service attack or dispersed denial-of-service attack is an attempt to create a mechanism otherwise network resource engaged to its intended users. It commonly consists of efforts temporarily or indefinitely interrupts or hangs up services of a host connected to the Internet.

**User Module:**

In user module validate user and create a new path any time. For security purpose if user gives the wrong details then a wrong node path is displayed or else it displays correct node path.

**Stretch Attack:**

An honest source would select the route Source affecting four nodes including it but the malicious node selects a longer route affecting all nodes in the network. These routes cause nodes that do not recline along the honest route to consume energy by forwarding packets they would not receive in honest scenarios. Stretch attack where a malicious node creates synthetically long source routes cause packets to traverse a larger than optimal number of nodes.

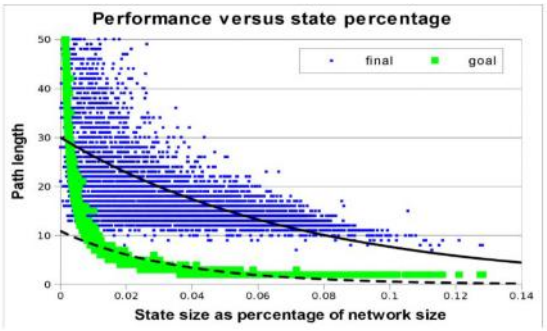
**Algorithm Used:**

Nodes may give up some local storage to keep a record of recent packets to avoid this attack from being carried out constantly with the same packet. Random direction vectors as suggested in PLGP would similarly improve the problem of imprecise cycles by avoiding the same malicious node during the succeeding forwarding round. Consistently traces that comprise malicious nodes should show the same network wide energy consumption by honest nodes as traces of a network with no malicious actors. The only noteworthy exceptions are when adversaries drop or mangle packets en route but since we are only worried with packets initiated by adversaries we can securely ignore this situation premangled packets achieve the same result they will be dropped by an truthful intermediary or destination.

```
Function forward_packet(p)
s ← extract_source_address(p);
c ← closest_next_node(s);
if is_neighbor(c) then forward(p,c);
else
    r ← next_hop_to_non_neighbor(c);
    forward(p,r);
```

```
Function secure_forward_packet (p)
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;
    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));
```

**Experimental Results:**




The dashed trend line symbolizes the expected path length of rerouted packets if each node stores log N network paths where N is the number of network nodes while the solid trend line represents the majority of actual network paths in a loose source-routing setup. The number of nodes traversed by loose source routed packets is suboptimal by at least a factor of 10 with some routes approaching a factor of 50. Only a few messages meet a node with a better path to the purpose than the originally assigned long source route. Therefore we terminate that loose source routing is worse than keeping global state at every node. Otherwise we can bound the harm of carousel and stretch attackers by limiting the allowed source route length based on the expected maximum path length in the network but we would need a way to decide the network diameter.

**Enhancement:**

We are extending secure transmission by using an efficient key management scheme for sensor networks. The proposed key management scheme utilizes the fact that a sensor only communicates with a small portion of its neighbors and thus greatly reduces the communication and computation overheads of key setup. A public key algorithm – Elliptic Curve Cryptography is used to further improve the key management scheme.

**Conclusion:**

Vampire attacks a new division of reserve consumption attacks that use routing protocols to enduringly immobilize ad hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations but rather depiction 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 deliberate their attack success on a randomly generated topology of 30 nodes. Simulation results show that depending on the location of the adversary network energy spending during the forwarding phase increases from between 50 to 1,000 percent. We have not offered a completely acceptable solution for Vampire attacks during the topology discovery phase but recommended some intuition about damage limitations possible with further modifications to PLGPa. Derivation of damage bounds and defences 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, 2012.
[2] I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
[3] 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.
[4] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.

[5] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
[6] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.
[7] D.J. Bernstein, "Syn Cookies," http://cr.yp.to/syncookies.html, 1996.
[8] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.
[9] J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.
[10] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
[11] J.-H. Chang and L. Tassiulas, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.
[12] T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.
[13] J. Deng, R. Han, and S. Mishra, "Defending against Path-Based DoS Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.
[14] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.
[15] S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.
[16] J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, 2002.
[17] H. Eberle, A. Wander, N. Gura, C.-S. Sheueling, and V. Gupta, "Architectural Extensions for Elliptic Curve Cryptography over GF(2m) on 8-bit Microprocessors," Proc. IEEE Int'l Conf' Application- Specific Systems, Architecture Processors (ASAP), 2005.
[18] T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and W. Marnane, "A Low-Power Pairing-Based Cryptographic Accelerator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.
[19] L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.
[20] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES), 2004.

**Authors:**

**Sri. M. Vamsi krishna,** well Known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra university is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications.

**Mrs. N.Santoshi Lakshmi**, is a student of Chaitanya Institute of Science & Technology, Madhavapatnam, Kakinada. Presently she is pursuing her M.Tech., [Computer Science & Engineering] from this college and she received her B.Tech. from Aditya Institution of Technology and Management, Tekkali, Srikakulam, affiliated to JNTU, Kakinada in the year 2005. Her area of interest includes Computer Networks, Advanced data structures and all current trends and techniques in Computer Science.