International Journal of Science Engineering and Advance Technology

A Sensor Network Routing Protocol To Clear The Damage From Vampire Attacks During Packet Forwarding

1**G.Lakshmi Narayana**, 2**CH.Koteswara Rao**

1,2Dept. of CSE, PACE Institute of Technology And Sciences., Ongole, Prakasam District,AP, India

ABSTRACT:

A reason creates and transmits it to the next hop toward the destination which broadcast it additional until the destination is reached consuming resources not only at the source node but also at each node the message moves through. If we believe the growing energy of an entire network intensification attacks are forever credible given that an opponent can write and send messages which are practiced by each node along the message path. A Vampire attack is the symphony and transmission of a message that sources more power to be enthusiastic by the network than if an open node transmitted a message of the same size to the same destination although using different packet headers. We compute the influence of the attack by the ratio of network energy used in the compassionate case to the energy used in the malicious case i.e. the relation of network-wide power operation with malicious nodes present to energy process with only honest nodes when the number and size of packets sent remains steady. Safety from Vampire attacks involves that this ratio is Energy use by malicious nodes is not measured since they can forever unilaterally drainpipe their own batteries. However believe the procedure of routing a packet in any multihop network.

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

INTRODUCTION:

Vampire attacks with the indemnity of malicious flooded discovery which is by a long way harder to notice or stop. We recommend a limited topology discovery period “the night” since this is when vampires are most treacherous followed by a long packet forwarding period during which adversarial success is provably circumscribed. An copious mitigation methods to clear the harmed from Vampire attacks and find that while the carousel attack is easy to stop with unimportant overhead the stretch attack is far more challenging. The first protection method we consider is loose source routing where any forwarding node can forward the packet if it knows a shorter path to the destination. Unfortunately this confirms to be less capable than simply keeping global network state at each node overcome the purpose of source routing. In our second attempt we adjust the protocol to guarantee that a packet makes development through the network. We call this the no-backtracking property since it holds close if and only if a packet is moving sternly closer to its destination with every hop and it alleviates all declared.

RELATED WORK:

Although Vampires will bump up energy procedure even in minimal-energy routing scenarios and when power conserving MAC protocols are used. These attacks cannot be forbidden at the MAC layer or through cross-layer feedback. Attackers will produce packets which confer more hops than necessary so even if nodes expend the minimum required energy to put on the air packets each packet is still more expensive to send out in the presence of Vampires. Our work can be thought of attack-resistant minimal-energy routing where the adversary’s goal comprises lessening energy investments. Present work in minimal-energy routing which aspires to augment the life span of power-constrained networks by means of less energy to transmit and receive packets e.g. by minimizing wireless transmission distance likewise orthogonal. These protocols focus on supportive nodes and not malicious scenarios.

EXISTING METHOD:

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. Protocols that make the most of power effectiveness are also inappropriate since they rely on cooperative node performance and

cannot optimize out malevolent deed. Networks previously scrutinize environmental conditions, factory performance and troop deployment to name a few applications.

DISADVANTAGES:

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

PROPOSED METHOD:

Protocols that maximize power efficiency are also inapt since they depend on cooperative node behaviour and cannot optimize out malicious action. 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. 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.

ATTACKS ON STATELESS PROTOCOLS:

The burden is on the source to make sure that the route is suitable at the time of sending and that every node in the route is a physical neighbour of the previous route hop. This approach has the benefit of necessitate very little forwarding logic at intermediate nodes and permits for complete routes to be sender authenticated using digital signatures. In these systems the source node states the complete route to a destination within the packet header so intermediaries do not make independent forwarding decisions depending quite 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.

MITIGATION METHODS:

When a loop is detected the source route could be accurate and the packet sent on but one of the attractive features of source routing is that the route can itself be signed by the source.
The carousel attack can be prohibited totally by having forwarding nodes check source routes for loops. While this appends extra forwarding logic and thus more overhead we can expect the increase to be valuable in malicious environments. The ns-2 DSR protocol does implement loop detection but confusingly does not use it to ensure routes in forwarded packets5.

ATTACKS ON STATEFUL PROTOCOLS:

Routes in link-state and distance-vector networks are built dynamically from many autonomous forwarding decisions so adversaries have limited power to affect packet forwarding making these protocols protected to carousel and stretch attacks. In fact any time adversaries cannot specify the full path the potential for Vampire attack is reduced. In link-state protocols nodes keep a evidence 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 keep track of the next hop to each destination indexed by a route cost metric e.g. the number of hops. In this scheme only routing updates that modify the cost of a given route need to be propagated..

DATA-VERIFICATION:

In data verification module receiver authenticates the path. For instance data approach with malicious node that is placed in malicious packet or else data placed in honest packet. This way user verifies the data's.

DENIAL OF SERVICE:

A denial-of-service attack or distributed denial-of-service attack is an attempt to make a machine or network resource busy to its intended users. Even though this means to carry out motives for and targets of a DoS attack may differ. It generally consists of efforts temporarily or indefinitely interrupts or hangs up services of a host connected to the Internet.

USER MODULE:

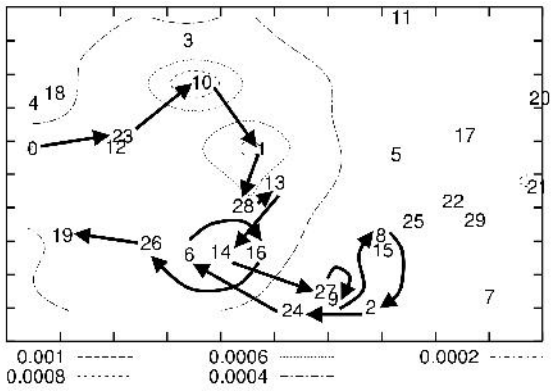
In user module validate user and create a new path any time. For security purpose if user gives the wrong details then a wrong node path is displayed or else it displays correct node path.

STRETCH ATTACK:

An honest source would choose the route Source affecting four nodes counting itself but the malicious node selects a longer route affecting all nodes in the network. These routes cause nodes that

do not lie down along the honest route to put away energy by forwarding packets they would not receive in honest scenarios. Stretch attack where a malicious node makes unnaturally long source routes cause packets to pass through a larger than optimal number of nodes.

ENERGY MAP OF THE NETWORK IN TERMS OF FRACTION OF ENERGY CONSUMED PER NODE:



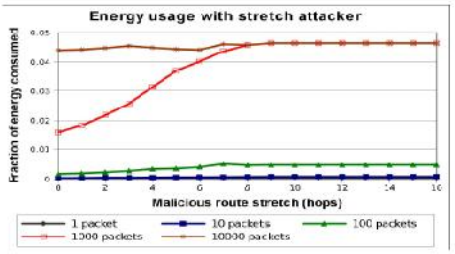
Malicious node 0 carries out a carousel attack sending a single message to node 19 which does not have to be malicious. Note the radical augment in energy usage along the original path.3 assuming the adversary limits the transmission rate to avoid saturating the network. The energy practice when node 0 sends a single packet to node 19 in an illustration network topology with only honest nodes. Black arrows indicate the path of the packet. In this attack an adversary sends a packet with a route composed as a series of loops such that the same node emerges in the route many times. This scheme can be used to augment the route length beyond the number of nodes in the network only limited by the number of allowed entries in the source route.2.

ALGORITHM USED:

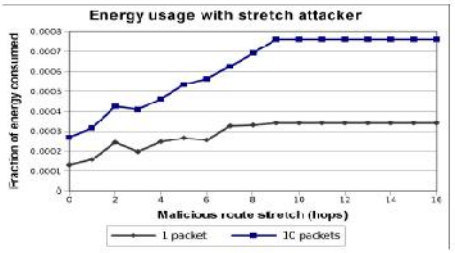
```
Function forward_packet(p)
s ← extract_source_address(p);
c ← closest_next_node(s);
if is_neighbor(c) then forward(p,c);
else
    r ← next_hop_to_non_neighbor(c);
    forward(p,r);
```

```
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:



(a) A malicious node transmitting 1, 10, 100, 1,000, and 10,000 messages with artificially long paths.



(b) Zoomed Figure (a), displaying only the 1 and 10-message data.

Growing maliciousness beyond nine has no consequence due to the diameter of our test topology. Network links become saturated at 10,000 messages per second even without the stretch attack but the opponent can attain the same effects by sending an order of magnitude fewer messages at a stretch attack maliciousness level of 8 or greater. This decreases cumulative network energy by 3 percent or almost the entire lifetime of a single node. It demonstrates network-wide energy consumption in the presence of a single randomly selected Vampire in terms of the "maliciousness" of the adversary or the induced stretch of the optimal route in number of hops. Therefore the stretch attack augments the efficiency of an adversary by an order of magnitude dropping its energy expenditure to compose and transmit

messages. With 100 messages the result is less severe.

CONCLUSION:

A node who is a member of multiple groups will be detected once those groups join and all groups are guaranteed to combine by the end of the protocol. Since PLGP presents the possibility to detect active Vampires once the network converges successive rediscovery 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 put on malicious discovery damage in PLGPa is still unknown. Vampires might uphold the illusion that it is a neighbour of a given group. Since join events necessitate combined calculation and are flooded throughout the group this makes for a fairly effective attack. PLGP already provides for the discovery of such manoeuvre upon termination of topology discovery.

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 inCryptography, 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.

Mr. GOTTIPATI LAKSHMI NARAYANA is a student of PACE INSTITUTE OF TECHNOLOGY AND SCIENCES ONGOLE, Presently he is pursuing his M.Tech [CSE] from this college and he received his B.Tech from RAO AND NAIDU Engineering College, affiliated to JNT University, Kakinada in the year 2012. His

area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr Ch. Koteswararao, well known Author and excellent teacher Received B.Tech in **Acharya Nagarjuna University** and M.Tech (CSE) from **Jawaharlal Nehru Technological University Kakinada (JNTUK)** is working as Associate Professor and HOD, Department of CSE, M.Tech Computer science engineering **Jawaharlal Nehru Technological University Kakinada University (JNTUK)**. He is an active member of ISTE. He has **11** years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences /journals. His area of Interest includes in **cryptography, Mobile Computing**, flavours of Unix Operating systems and other advances in computer Applications.