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, Issue 7, July 2014

Optimized Link State Routing In Wireless Ad Hoc Sensor Networks

Sreekanth Reddy Dandala, B Sowmya

M Tech Student, Department Of Computer Science and Engineering, INTELL Engineering College, Anantapur, Andhra Pradesh, India

Assistant Professor, Department Of Computer Science and Engineering, INTELL Engineering College, Anantapur, Andhra Pradesh, India

ABSTRACT: Ad hoc wireless sensor networks are an exciting research in intuiting and Ad Hoc computing. Previous mechanisms in this area are concentrated on the denial of communication and denial of Service at the routing process levels or MAC levels. The resource depletion attacks at the routing protocol layer, in which permanently disable the networks by quickly draining nodes' battery power. The "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. All the available protocols (link-state, distance vector, source routing etc.) are susceptible to Vampire attacks, and are easy to carry out as one malicious insider sending only protocol-compliant messages. There are numerous mitigation methods to bind the damage from Vampire attacks. The first protection mechanism 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. The second method is to modify an existing sensor network routing protocols (Ariadne, SAODV, and SEAD) to provably mitigate the damage from Vampire attacks during packet forwarding.

KEYWORDS: Denial Of Service, Routing, Ad Hoc Networks, Sensor Networks, Wireless Networks, Reduction Of Quality (ROQ), Ariadne, SAODV, SEAD.

I. INTRODUCTION

Wireless Ad Hoc Sensor Networks seeks to provide an opportunity for researchers from computer science, engineering and mathematical backgrounds to disseminate and exchange knowledge in the rapidly emerging field of ad hoc and sensor wireless networks. It will comprehensively cover physical, data link, network and transport layers, as well as application, security, simulation and power management issues in sensor, local area, satellite, vehicular, personal, and mobile ad hoc networks.As WSNs available today are more and more vigorous to the everyday functioning of people and organizations, The convenience faults become less tolerable lack of convenience can make the difference between business as usual and lost productivity, power outages, environmental Problems, and even vanishes the lives thus high accessibility of these networks is a precarious property, and should stand perfectly even under wicked environments. Since the Wireless Ad Hoc sensor networks implements the ad hoc organization, they are vulnerable to many types of attacks such as Denial of Service (DOS) Reduction of Quality (ROQ), Vampire attacks etc. A great deal of research has been done to prevent these types of attacks. These schemes can prevent the attacks on short term availability and does not address the long term availability.

II. RELATED WORK

It does not imply that power draining itself is novel, but rather that these attacks have not been severely defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion attackis "Resurrecting Duckling attacks".The Resurrecting Duckling attacks are also knows as the Denial of Sleep attacks or sleep deprivation torture attacks. In these types of attacks, Nodes try to spend most of the time in a sleep mode in which they only listen for radio signals once in a while. Once the battery of the node runs out, the attacker can stop and walk away, leaving the

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, Issue 7, July 2014

victim disabled. The methods to mitigate these types of attacks are based on Prioritization and Reservation mechanisms. In this process, if a server has a primary function and a distinct auxiliary function, then these functions can be prioritized and a reservation mechanism is performed to ensure that the higher priority node receives a guaranteed share of the resource regardless of the number of requests generated by the lower priority uses. Unfortunately this type of mitigations does not resolve these types of attacks completely. The non-power-constrained systems, this attacks includes the depletion of resources such as memory, CPU time, and bandwidth etc. a popular example is the SYN flood attack. TCP SYN flooding is a type of DoS attack that generates many bad TCP SYN packets. Connection between the client and the server using TCP is established by 3-way handshake protocol. In a TCP SYN-Flood attack, the client (attacker) initiates a 3-way handshake but never finishes and the server never sends final ACK packets. The counter measure to prevent these types of attacks is developed by Toronto which is called as GENESIS. This method allows the web servers to distinguish between legitimate and fake requests to the server in order to filter out bad requests that are generated and is somewhat difficult to implement. Another attack that can be thought of as path based is the wormhole attack, in this attack, an attacker records packets at one location in the network and tunnels them to another location, and retransmits, from there into the network. The mechanism, called packet leashes is used for detecting and defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance. This solution comes at a high cost and is not always applicable. First, one flavor of Packet Leashes depend on on tightly synchronized clocks, which are not used in most off the wireless devices. Second, the authors assume that packet travel time dominates the processing time, which may not be borne out in modern wireless networks, particularly low power wireless sensor networks.

III. SCOPE OF RESEARCH

The existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network paths. The Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol compliant messages they drain the life of the nodes.Some of the disadvantages of existing system are below:

- Power outages
- Due to Environmental disasters, loss in the information
- Lost productivity
- Various DOS attacks
- Secure level is low
- Existing works does not address attacks that affect long-term availability.

IV. PROPOSED METHODOLOGY

A. *Thoroughly evaluate the vulnerabilities of existing protocols to routing layer Vampire attacks(Carousal and Stretch Attacks):*

- Create a network setup is setup along with the Sink, Source and with Six nodes namely Node A, B, C, D, E, F and assigned a unique Identity number to each node.
- The static protocols are used, to discover the network topology during an initial setup phase.
- The On demand Routing Protocols are used to discover the network topology change occurred during the transmission time.

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, Issue 7, July 2014

- The first type of attack is the Carousel attack. In this attack an adversary composes the packets with purposely introduced routing loops.
- It targets source routing protocols by exploiting the limited verification of message headers during the forwarding of packets at each node.This process allows a single packet to repeatedly traverse the same set of nodes continuously.
- A single attacker can use a carousel attack to increase energy consumption at each node by as much as a factor of 4.
- The second type of attack to evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks is the Stretch attack. In this an adversary constructs artificially long routes, potentially traversing every node in the network.
- This 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.
- The stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node

B. *Show the Show the simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary).*

- The energy levels of each node in the network are identified and the simulation results will be shown in the presence of vampire attacks.
- 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.

C. *Modify an existing sensor network routing protocol to provably bind the damage from Vampire attacks during packet forwarding.*

- The secured transmission between the nodes by overcoming the vampire attacks will be implemented.
- In this process, we can modify the existing sensor network protocol (Ariadne, SAODV, SEAD etc...) such that the new honest route in the network between the nodes which does not affect with the vampire attacks is determined.
- The data will be transmitted among the different nodes in the honest route and this process will mitigate the effect of vampire attacks.

V. PSEUDO CODE

Pseudo Code for packet forwarding without modifying the protocol:

```
Step 1: Function Foreward_Packet (p)
Step 2: S ← extract_Source_Address (p);
Step 3: C ← closest_next_node(s);
Step 4: If is_neighbour(c) then forword (p, c);
        Else
        R ← next_hope_to_non_neighbor(c);
```

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, Issue 7, July 2014

Step 5: Forword (p, r);

Pseudo Code for packet forwarding after modifying the protocol:

/* No backtracking property is used to provably avoid the Vampire attacks.*/

Step 1: Function Secure_foreward_Packet (p)
Step 2: S ← extract_Source_Address (p);
Step 3: a ← extract_attestation (p);
Step 4: If (not verify_source_sig (p)) or
Step 5: (empty (a) and not is_neighbour(s)) or (not saowf_verify (a)) then
Step 5: /* drop (p) */
Step 6: For each node in a do
Step 7: Prevnode <- node;
Step 8: if (not are neighbors (node, Prevnode)) or
Step 9: (not making progress (Prevnode, node)) then
Step 10: return;
Step 11: /* drop (p) */
Step 12: C ← closest_next_node(s);
Step 13: P <- saowf_append (p);
Step 14: If is_neighbour(c)
Then
Step 15: forward (p, c);
Else
Step 16: forward (p, next_hot_to_non_neighbor(c));

VI. SIMULATION RESULTS

The simulation studies involve the deterministic of a network topology with 30 nodes as shown in Fig.1. Energy usage is measured for the minimum number of packets required to dispense a single message, so distribution of more messages increases the strength of the attack linearly until bandwidth saturation. We individually 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.

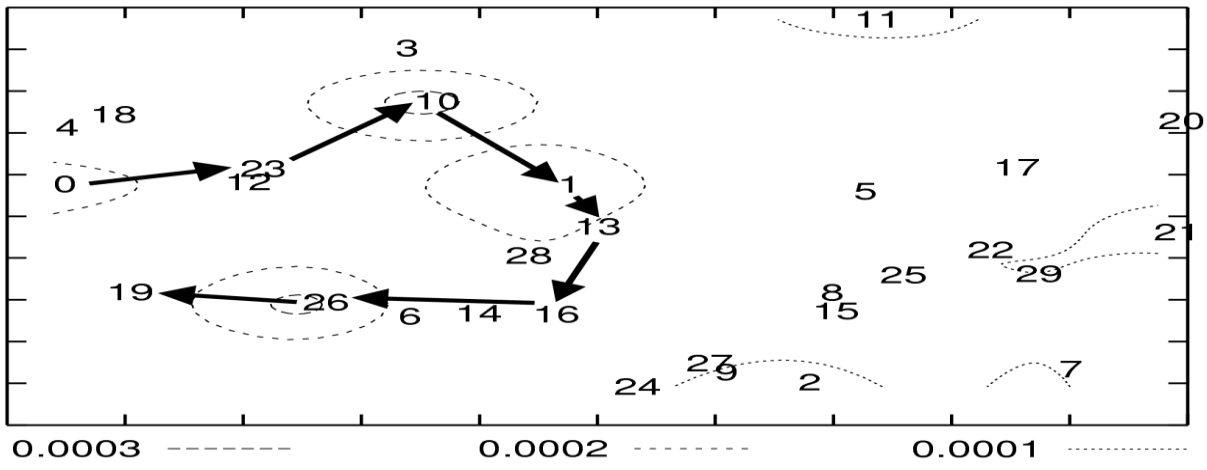

Fig.1. Ad Hoc Network of 30 Nodes

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, Issue 7, July 2014

Fig 1 depicts the honest scenario, the energy usage when node 0 sends a single packet to node 19 in an example network topology with only honest nodes. This is the scenario in which the nodes communicate without the presence vampire attacks. The above figure depicts the Energy map of the network in terms of fraction of energy consumed per node. Black arrows show the packet path through the network. Each dotted line represents an "energy equivalence zone," similar to an area of equal elevation on a topological chart. Each line is marked with the energy loss by a node as a fraction of total originalcharge.

The simulation results of a 30 node network topology in the presence of the vampire attacks (Carousal Attacks and Stretch Attacks) is shown in the below figure.

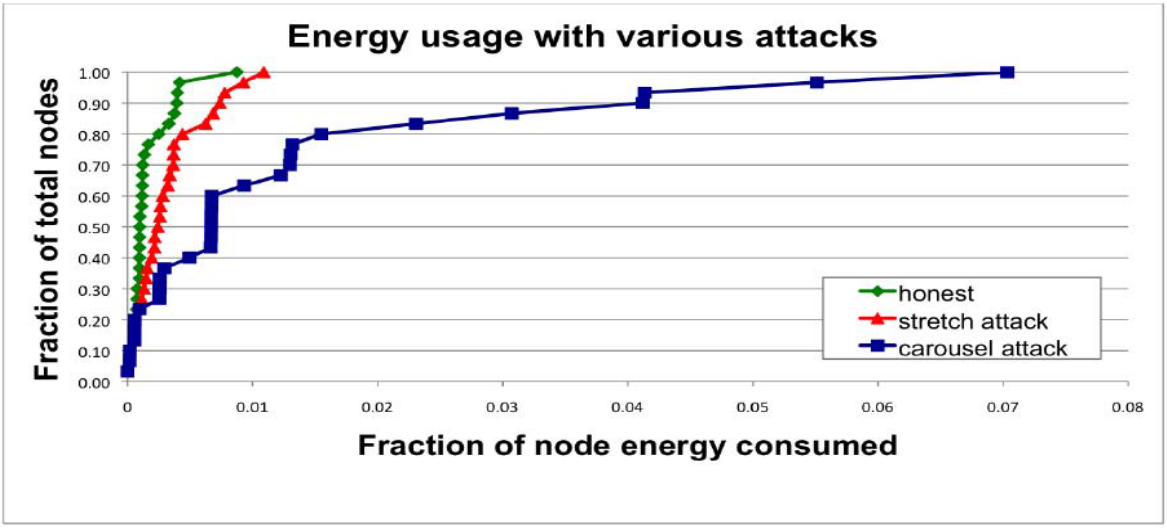

Fig.2. Energy distribution under various Vampire Attacks and after implementing mitigation methods of vampire attacks

In the presence of Carousal Attack, first type of vampire attacks, the nodes traversed by the packet are same as in the Fig 1, but the loop overall forwarding nodes roughly triples the route length (The packet traverses the loop more than one) from the figure Fig 2, we can clearly observe that the drastically increased energy consumption among the forwarding packets.

In the presence of Stretch Attack, second type of vampire attacks, the route diverts from the optimal path between source and destination, roughly doubling the route length. In this attack, the per node energy consumption increase is not as drastic. In this attack, the overall energy consumption is greater than that of Carousal Attacks, but spread more evenly over more network nodes. From Fig 2, we can clearly observe that the increased energy consumption among the forwarding packets.

VII. CONCLUSION AND FUTURE WORK

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

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, Issue 7, July 2014

destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. Derivation of damage bounds and defences for topology discovery, as well as handling mobile networks is left for future work.

REFERENCES

1. 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.
2. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.
3. 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.
4. 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.
5. 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.
6. 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.
7. A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy- Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.
8. J.L. Hill and D.E. Culler, "Mica: A Wireless Platform for Deeply Embedded Networks," IEEE Micro, vol. 22, no. 6, pp. 12-24, Nov./ Dec. 2002.
9. L. Xiaojun, N.B. Shroff, and R. Srikant, "A Tutorial on Cross-Layer Optimization in Wireless Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 8, pp. 1452-1463, Aug. 2006.
10. V. Paxson, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks," SIGCOMM Computing Comm. Rev., vol. 31, no. 3, pp. 38-47, 2001.
11. D.R. Raymond and S.F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.
12. R.L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Comm. ACM, vol. 21, no. 2, pp. 120-126, 1978.
13. A. Saxena and B. Soh, "One-Way Signature Chaining: A New Paradigm for Group Cryptosystems," Int'l J. Information and Computer Security, vol. 2, no. 3, pp. 268-296, Nov, 2008.
14. I. Stojmenovic and X. Lin, "Power-Aware Localized Routing in Wireless Networks," IEEE Trans. Parallel and Distributed Systems, vol. 12, no. 11, pp. 1122-1133, Nov. 2001.
15. J. Yuan, Z. Li, W. Yu, and B. Li, "A Cross-Layer Optimization Framework for Multihop Multicast in Wireless Mesh Networks," IEEE J. Selected Areas in Comm., vol. 24, no. 11, pp. 2092-2103, Nov. 2006.

BIOGRAPHY

Sreekanth Reddy Dandala is an M Tech student in Department of Computer Science and Engineering in INTELL Engineering College Anantapur affiliated to Jawaharlal Nehru Technological University - Anantapur, Andhra Pradesh, India. Area of interest is Sensor Networks and Network Security.

B Sowmya completed her M Tech in the Department of Computer Science and Engineering, and currently working as an Assistant professor in INTELL Engineering College Anantapur affiliated to Jawaharlal Nehru Technological University - Anantapur, Andhra Pradesh, India. Her Area of Interest is Networking, Internet Programming, and Network Security.