DEPLETION OF NODE BATTERY LIFE FOR DENIAL OF SERVICE IN WIRELESS ADHOC SENSOR NETWORK

K.Mahalakshmi, (M.E) and V.Senthilvel,M.E.,(Ph.D*)
Affiliated to Anna University,Chennai,Department of Computer Science and Engineering
Arulmigu Meenakshi Amman College of Engineering,
Thiruvannamalai Dt,Tamilnadu,India.
maha.jawahar@gmail.com

Abstract - *Ad-hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels Here,I have focused on resource depletion attacks at the routing protocol layer, which permanently disable the networks by quickly draining node's battery power. These "Vampire" attacks are not specific to any protocol, but rather they rely on the properties of many popular classes of routing protocols. It is found that all the examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. In worst case scenario, even a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks ,namely the carousel and stretch attacks with a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.*

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

I. INTRODUCTION

The Wireless Sensor Networks(WSN) is built of "nodes" which are spatially distributed from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors to monitor the physical and environmental conditions such as temperature , sound , pressure, etc. The more modern networks are bi-directional. Adhoc Wireless Sensor Networks promises exciting new applications such as ubiquitous on-demand computing power, continuous connectivity and instantly - deployable communication for the responders. Such networks monitor environmental conditions, factory performance, troop deployment, civilian applications as well as assist in the national effort to increase alertness to potential terrorist threats etc. Wireless ad-hoc sensor networks are particularly vulnerable to denial of service (DoS) attacks [5]. Depending upon the duration of attacks, attacks are classified as short-term attack and long-term attack. The focus is on the long term attack which leads to permanent denial of service by entirely depleting the node batteries. This is an instance of a resource depletion attack, which uses the battery power as the resource of interest. Here I focus on routing protocols, which are 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. 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. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.There are three primary contributions in this paper. First, a thorough

evaluation of the vulnerabilities of existing protocols to routing layer battery depletion attacks. It is observed that the security measures for preventing the Vampire attacks are orthogonal to those used to protect routing infrastructure 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 behavior and cannot optimize out malicious action. Secondly, the simulation results quantify the performance of several representative protocols in the presence of a single Vampire (insider adversary). Finally modifying an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding. Two ways to classify wireless ad hoc sensor networks are whether or not the nodes are individually addressable, and whether the data in the network is aggregated. Here I focus on the major two types of attacks that are used for Denial of Service communication

A. Carousel attack

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route. It is observed from the Fig.1.1. the thick path shows the honest path and thin shows the malicious path

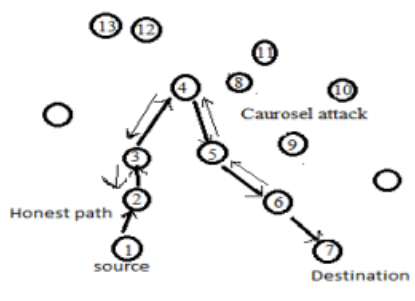

Fig. 1.1 Carousel attack

B. Stretch attack

Another attack in the same vein is the stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. In the example given below honest path shown with thick lines and adversary or malicious path with thin lines. The honest path is very less distant but the malicious path is very long to make more energy consumption.

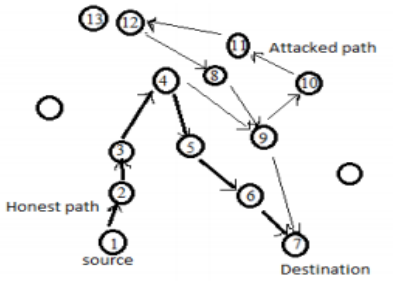

Fig. 1.2. Stretch attack

II. RELATED WORK

The carousel attack can be prevented entirely by having forwarding nodes check source routes for loops. While this adds extra forwarding logic and it increase more overhead. The routes in link-state and distance-vector networks are built dynamically from many independent forwarding decisions. Adversaries have limited power to affect packet forwarding, making these protocols immune to carousel and stretch attacks. Using a directional antenna they can still waste energy by restarting a packet in various parts of the network. Another attack on all previously-mentioned routing protocols is spurious route discovery. Every node will forward route discovery packets meaning it is possible to initiate a flood by sending a single message.

Drawbacks of the existing system

1. Adding extra forwarding logic increases overhead
2. Adversaries have limited power.
3. Usage of directional antenna.
4. Spurious route discovery.
5. Possibility of flooding.

III. PROPOSED SYSTEM

Here a clean slate secure sensor network routing protocol by Parno , Luk , Gaustad and Perrig (“PLGP” from here on) consists of a **topology**

discovery phase, followed by **a packet forwarding phase** ,with the former optionally repeated on a fixed schedule to ensure that topology information stays current. In discovery phase each node has limited view of the network, each node knows only itself and discovers their neighbours using local broadcast.

Nodes build a tree of neighbour relationships and group membership that will later be used for addressing and routing. During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop. **No-backtracking property**, is satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space

Advantages of proposed system

1. No usage of forwarding logic or directional antennas.
2. Ensuring security by authenticating the users.
3. High efficiency.
4 .No flooding
5. Timely delivery of packets.

IV. RESULT ANALYSIS

As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet.

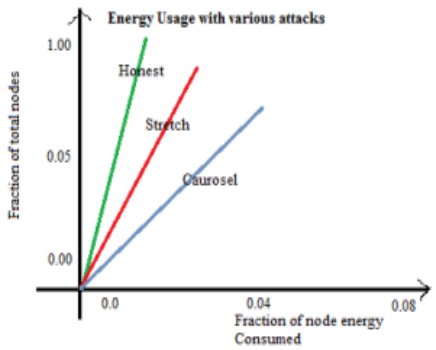

Fig 4. Node energy distribution under various attack scenarios.

While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected, destination.(4-9-10-11-12-8-9—long route). with some losing almost 10 percent of their total energy reserve per message. Per-node energy usage under both attacks is shown in figure 4.

On referring the architecture diagram below, each node acts as an individual node. The neighbour node is identified within the network. When a message is transmitted the node forwards a local broadcast message to its neighbor node. A tree is formed on identifying these neighbor nodes. The packets are then forwarded to the shortest identified path among the formed tree by satisfying the property of no- backtracking algorithm

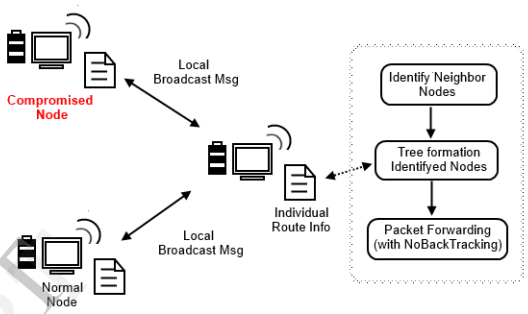

Fig. 4.1.Architecture diagram

A. Finding Neighbors

Initially the neighbor nodes are discovered within the network. When a message is transmitted this module forwards a local broadcast message to its neighbor node. The neighbor nodes on receiving this broadcast message sends an acknowledgement to the sender node and from this acknowledgement message the sender node identifies the neighbor node. Only the neighbor nodes are involved in transmitting the message.

B. Tree Formation

Each node after identifying its neighbor node forms a local tree structure. Similarly each node is within a network forms a local tree and a final tree is formed recursively when the tree structure reaches it convergence.

C. Transmission History

The nodes maintain a history of previous packet transmission done by each node. This history

consists of the hop count of previous route and it keeps on updating this history through which attack immunity of our system can be improved.

D. Packet Forwarding

Finally packets are forwarded using the above formed tree structure. Here each node has independent route constructed from the tree structure. And also checks for the condition to match **No Backtracking.**

No Backtracking Algorithm

Begin
Send broadcast message Pk(B) for node detections
Identify neighbor nodes when receive an acknowledgement Pk(B)a
Creates tree structure using the neighbor node list <Tn>
After creation of tree each node share their tree structure <Tn>
Update individual tree structure <Tu>
Check for convergence
If convergence = true
Stop updating
Else
Begin
Share tree structure <Tu>
Update tree structure <Tu>
End
Maintains transmission history
Check Packet hop count Hn
If hop count (Hn) = Previous hop Count (Hp)
Drop packet
Else
Transfer packet
End

Algorithm explanation

- Initially a local broadcast message is sent to detect the neighbor nodes.
- The identified neighbor nodes in turn sends an Acknowlegement message to the broadcasted node.
- Now create a tree structure with the shortest path using the neighbor node list and share this tree structure.
- Update the individual tree structure after each and every new tree is formed.
- Check for convergence.
- If convergence is true , then stop updating else goto step 4.
- Maintain a transmission history using the packet hop count
- If hopcount equals previous hopcount then drop the packet,else transfer the packet.

During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address (see Figure 4.4). Thus every forwarding event (except when a packet is moving with group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination

V. CONCLUSION

A large part of this phase, I have been dedicated to explain 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. I have defined the PLGP protocol the first sensor network routing protocol that provably bounds damage from Vampire attacks. I have explained the working procedure, algorithm and proving its efficiency theoretically by comparing it with the existing system models.

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 ondemand 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, International 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 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 networks,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 pathbased 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 networks, 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-topeer systems, 2002.
[17] Hans Eberle, Arvinderpal Wander, Nils Gura, Sheueling Chang-Shantz, and Vipul Gupta, Architectural extensions for elliptic curve cryptography over GF(2m) on 8-bit icroprocessors, ASAP, 2005.

AUTHORS PROFILE

Mahalakshmi. K, received B.E degree in Computer Science Engineering from Madras University in 2004.Currently she is pursuing Master degree program in Computer Science Engineering, Arulmigu Meenakshi Amman College of Engineering, Thiruvannamalai Dt, Near Kanchipuram, Anna University, India. She is interested in distributed network security, privacy and anonymity and web services Ph- +91 9600342211