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, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks

K.Sivakumar[1], P.Murugapriya[2]

II-M.TECH, Department of IT, Sasurie College of Engineering, Vijayamangalam, Tirupur, Tamilnadu, India[1]

Asst. Professor, Department of IT, Sasurie College of Engineering, Vijayamangalam, Tirupur, Tamilnadu, India[2]

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. This proposed optimal energy boost-up protocol (OEBP) analyzes the routing table and verify the attacks which permanently disable networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. This enhanced work increases the Quality of service in the network and it will regulates all the nodes activity.

I. INTRODUCTION

AD hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications.

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.

1.1Classification

The first challenge in addressing Vampire attacks is defining them what actions in fact constitute an attack? DoS attacks in wired networks are frequently characterized by amplification an adversary can amplify the resources it spends on the attack, e.g., use 1 minute of its own CPU time to cause the victim to use 10 minutes. However, consider the process of routing a packet in any multihop network: a source composes and transmits it to the next hop toward the destination, which transmits it further, until the destination is reached; consuming resources not only at the source node but also at every node the message moves through.

We define the cumulative energy of an entire network, amplification attacks are always possible, given that an adversary can compose and send messages which are processed by each node along the message path. So, the act of sending a message is in itself an act of amplification, leading to resource exhaustion, as long as the aggregate cost of routing a message is lower than the cost to the source to compose and transmit it. So, we must drop amplification as our definition of maliciousness and instead focus on the cumulative energy consumption increase that a malicious node can cause while sending the same number of messages as an honest node.

Vampire attack as the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious.

1.2 Protocols and Assumptions

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. While this is by no means an exhaustive list of routing protocols which are vulnerable to Vampire attacks, we view the covered protocols as an important subset of the routing solution space, and stress that our attacks are likely to apply to other protocols.

All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, where topology discovery is done at transmission time, and static protocols, where topology is discovered during an initial setup phase, with periodic rediscovery to handle rare topology changes. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Furthermore, adversary location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was deployed, and cannot control their final positions.

While assume that 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.

1.3Contributions

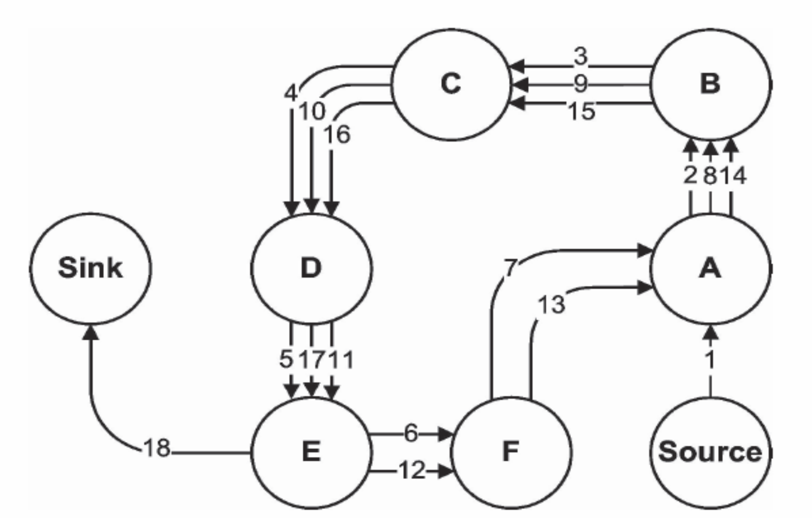
We are using three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing Infrastructure and so existing secure routing protocols such as do not protect against Vampire attacks. 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 message.

II. RELATED WORK

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.

(a) Carousel attack:

1. adversary composes packets with purposely introduced routing loops
2. sends packets in circles
3. targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes.



(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.

(b) Stretch attack:

- An adversary constructs artificially long routes, potentially traversing every node in the network
- 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

Honest hop count = 3

Malicious hop count = 6

III. PROTOCOL AND TECHNIQUE

We show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

Clean-Slate Sensor Network Routing:

- PLGP: a clean-slate secure sensor network routing protocol by Parno et al.
- The original version of the protocol is vulnerable to Vampire attacks.
- PLGP consists of a topology discovery phase, followed by a packet forwarding phase.
- Discovery deterministically organizes nodes into a tree that will later be used as an addressing.

- When discovery begins, each node has a limited view of the network—the node knows only itself. Nodes discover their neighbors using local broadcast, and form ever expanding "neighborhoods," stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbor relationships and group membership that will later be used for addressing and routing.

3.1 Data-Verification

In data verification module, receiver verifies the path. Suppose data come with malicious node means placed in malicious packet. Otherwise data placed in honest packet. This way user verifies the data's.

3.2 Denial of service

In computing, a denial-of-service attack or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

3.3 User Module

In user module, verify user and any time create a new path. In security purpose user give the wrong details means display wrong node path otherwise display correct node path.

3.4 Attack Module

Stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. An honest source would select 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 would not receive in honest scenarios.

3.5 Optimal energy Boost-up protocol (OEBP)

This predicts the vampire attacks based on the existing behavior and finds optimal path optimal topology discovery. Schedules the energy consumption and need of energy if any node performs

IV. CONCLUSION FUTURE ENHANCEMENT

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 small number of weak adversaries, admeasured 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.

V. FUTURE ENHANCEMENT

- Proof submission algorithm
- Topology discovery based on the attacks

- Topology reconfiguration

  This predicts the vampire attacks based on the existing behavior and finds optimal path and optimal topology discovery. Schedules the energy consumption and need of energy if any node performs vampire. Topology verification.

REFERENCES

1. Deng. J. Han. R. and Mishra. S. “Defending against Path-Based DoS Attacks in Wireless Sensor Networks”, proc.ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

2. Doshi. S. Bhandare. S. and Brown. T.X. “An On Demand Minimum Energy Routing Protocol for a wireless Ad Hoc Network,” ACM SIGMOBILE mobile computing and communication. Rev. vol. 6, no. 3, pp, 50-66, 2002.

3. Douceur. J.R. ”The Sybil Attacks”, proc. Int’l Workshop Peer-to-Peer Systems, 2002.

4. Feency. L.M. “An Energy Consumption model for Performance Analysis of Mobile Ad Hoc Networks,” mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

5. Park. K. and Lee. H. ”On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attacks,” proc. IEEE INFOCOM,2001.

6. Johnson. D.B. Maltz. D.A. and Broch. J. “DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networking, Addison-Wesley, 2001.

7. Karlof. C. and Wagner. D. “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” Proc. IEEE lnt’l Workshop Sensor Network Protocols and Applications, 2003.

8. Karp. B. and Kung. H.T. “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, pro. ACM MobiCom, 2000.

9. Raffo. C. Adjih. T. Clausen, and P. Muhlethaler, “An Advanced Signature System for OLSR”, pro. Second ACM Workshop Security of Ad Hoc and Sensor Networks, 2004.

10. Goldsmith. A.J. and Wicker. S.B. “Design Challenges for Energy Constrained Ad Hoc Wireless Networks”, IEEE Wireless Comm., vol. 9, no. 4, pp. 8-27, Aug. 2002.