Proficient Protocol for Vampire Attacks in Wireless Ad Hoc Sensor Networks

#Gugulothu Veeranna[1], *M.Tech,Computer Science & Engineering, E mail:* veeru3390@gmail.com
#Mohd. Fasi Ahmed Parvez[2], Assoc. prof. and HOD, *Department of CSE, E mail:* parvez40509@gmail.com
#Syed Abdul Moeed[3], Assoc. prof., *Department of CSE, E mail:* abdulmoeedsyed@gmail.com
 # Balaji Institute Of Engineering &Sciences, Warangal, Telangana, India

Abstract: **Wireless ad-hoc sensor networks have great long-term economic potential, ability to transform our lives, and pose many new system-building challenges. Sensor networks also pose a number of new conceptual and optimization problems. Some, such as location, deployment, and tracking, are fundamental issues, in that many applications rely on them for needed information. Adhoc sensor wireless networks have been drawing interest among the researches in the direction sensing and pervasive computing. The security work in this area is priority and primarily focusing on denial of communication at the routing or medium access control levels. In this paper the attacks which are mainly focusing on routing protocol layer that kind of attacker is known as resource depletion attacks. These attacks causing the impact of persistently disabling the networks by drastically draining the node's battery power. These "Vampire" attacks are not impacting any specific kind of protocols. Finding of vampire attacks in the network is not a easy one. It's very difficult to detect, devastating .A simple vampire presenting in the network can increasing network wide energy usage. We discuss some methods and alternative routing protocols solution will be avoiding some sort of problems which causing by vampire attacks.**

Keywords*:* Sensor Networks; Wireless Networks; Adhoc Networks, Routing Protocols.

1. 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.

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.

Protocols:

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

www.ijrct.org

All rights reserved, editor@ijrct.org

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.

2. Related Work

The sensor nodes in the wireless sensor networks are usually mainly depending on the battery power. To saving the power of nodes must be used a number of techniques. In the one cause of energy loss in wireless sensor network node in the idle consumption, when the nodes are not participating in the processing of transmitting/receiving any information but listening and waiting for information from other nodes. There also an energy loss because of packet collusion, where all packets ate involved in the collision are discarded and must be retransmitted. A third cause of energy loss is repeating the process of receiving and transmitting the same packets as a periodically these can be seen as protocol overhead. In This paper handling these kinds of problem and trying to finding the better solution of the existing one. This paper focusing on saving energy in the layer of routing protocols.

Vampire attacks not protocol specific. It's not depending upon the design or implementation faults particularly routing protocols. The routing algorithms that has been using in the concepts that are link-state, distance vector, source routing, geo graphic and beacon. In these we do not want to transmitting large amount of data for largest energy drain like flooding attacks. Rather this try to transmit little amount of data. Vampire attacks based on protocol compliant messages so, it's much detected and prevent. The vampire attacks do not able to address that attacks long-term availability. The chance of happening permanent denial of attacks in the network is to entirely deplete the nodes battery power. In this paper we have to focus on how routing protocols, designed to be secure and how this lack protection from these kinds of attacks, since the nodes depleting its power.

Vampire attack happens in the network in the sense, any of the nodes in the network which is affected or infected and this nodes behavior is abruptly changing for the network behavior, this kind of nodes are called "Malicious node". If malicious nodes present in the network energy that have been using by each and every nodes will increases drastically. The malicious node has been place in the network uniquely. First In between the routing nodes, and the second placed in the Source node itself. The chance of placing a malicious node in the routing path this makes causing damage in network. Source node identifying the particular packets and selected packets are identified for the routing to the destination. The routing path is discovering by source node by using shortest path routing algorithm and the path shouldn't be changeable by the intermediate nodes. In this type of occasion there is a chance to happening attack. The adversary composes packets with purposely introduced routing loops. This is one of the major problems of the network where the consuming energy of each and every node in the network will increase. This process continues for the particular period of time, transmitting the process in the loop and wasting every nodes power which is presently in the routing path. The main problem these kinds of attackers are it's not easily identified if it attacked or affected the network. It will take some long time to identify and make ensure that it presented in the network.

3. Ad hoc On Demand Routing Protocol

Ad hoc On Demand Routing Protocol belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbor's and the

All rights reserved,

costs to reach them. A node maintains its own routing table, storing all nodes in the network, the distance and the next hop to them. If a node is not reachable the distance to it is set to infinity. Every node sends its neighbor's periodically its whole routing table. So they can check if there is a useful route to another node using this neighbor as next hop. When a link breaks a Count-To-Infinity could happen. AODV is an 'on demand routing protocol' with small delay. That means that routes are only established when needed to reduce traffic overhead. AODV supports Unicast, Broadcast and Multicast without any further protocols. The Count-To-Infinity and loop problem is solved with sequence numbers and the registration of the costs.

In AODV every hop has the constant cost of one. The routes age very quickly in order to accommodate the movement of the mobile nodes. Link breakages can locally be repaired very efficiently. In a multicast routing table the IP address and the sequence number of the group are stored. Also the leaders IP address and the hop count to him are stored as well as the next hop in the multicasting tree and the lifetime of it. To join a multicast group a node has to send an RREQ to the group address with the join flag set. Any node in the multicast tree which receives the RREQ can answer with a RREP. Like this a requester could receive several RREP from which he can choose the one with the shortest distance to the group. A MACT (Multicast ACTivation) Message is send to the chosen tree node to activate this branch. If a requester does not receive a RREP, the node supposes that there exists no multicast tree for this group in this network segment and it becomes the group leader. A multicast RREP contains additional the IP of the group leader and the hop count to the next group member. The group leader broadcasts periodically a group hello message (a RREP) and increments each time the sequence number of the group. When two networks segments become connected, two partitioned group trees have to be connected. Every group member receiving two group hello messages from different leaders will detect a tree connection. Then this node emits an RREQ with the repair flag set to the group. If a node in the group tree does not receive any group hello or other group message it has to repair the group tree with a RREQ and has to ensure that not a RREP from a node in its own sub tree is chosen. If a group member wants to leave the group and it is a leaf it can prune the branch with a MACT and the flag prune set. If it is not a leaf it must continue to serve as a tree member.

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.

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.

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.

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.

Attack Module

Stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. 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.

Stateful Protocol and their Attacks

A stateful protocol is where nodes are aware of their topology, forwarding decisions, its state. It need the server to store and record the transaction so they can be recalled or resumed. Two significant classes are link state and distance –vector. Example of link-state is OLSR and example of distance-vector is DSDV. Both these protocols are proactive, which routes to all reachable nodes in the network and minimizes the initial delay. OLSR keeps the record of up and down state of links and flood routing updates. DSDV is also known as Distributed Bellman-Ford or

www.ijrct.org

All rights reserved,

RIP (Routing Information Protocol). Every node maintains a routing table that contains all available destinations, the next node to reach to destination, the number of hops to reach the destination and periodically send table to all neighbors to maintain topology. Both these protocols are not vulnerable to carousel and stretch attacks. In fact, any time adversaries cannot indicate the full path, the potential for Vampire attack is reduced. Two types of attacks in stateful protocol are directional antenna attack and malicious discovery attack. Directional antenna attack: In this he vampires have little control over the packets progress, but they still waste energy by restarting a packet in various parts of network. Malicious Discovery Attack: It is also called as spurious rote discovery. Both AODV and DSR are vulnerable to this attack since nodes may initiate discovery at any time, not just during the topology change. This type of attack becomes serious when nodes claim that long distance route has changed. This attack is trivial in open networks. Packet leashes cannot prevent this type of attack. This is similar to route flapping in BGP.

Stateless Protocols and their Attacks

A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. It is communication protocol that treats ach request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses. It is called Stretch attack, since it 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 carousel on the other hand sends packets in circles. It 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.

4. Destination Sequenced Distance Vector

DSDV routing is one of the properties of the ad-hoc network routing protocol. It is a table driven in the type of proactive based protocol routing scheme. Here using two types of routing algorithms one is 1).Link-state algorithm and second is 2).Distance vector routing algorithm.

4.1 Link-state algorithm

In link-state protocols, such as OLSR, nodes keep a record 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. Here, each node maintains a view of the network topology.

- Like the shortest-path computation method
- Each node maintains a view of the network topology with a cost for each link
- Periodically broadcast link costs to its outgoing links to all other nodes such as flooding

4.2 Distance vector routing algorithm

Distance vector protocols like DSDV keep track of the next hop to every destination, indexed by a route cost metric, e.g., the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated. Known also as Distributed Bellman-Ford or RIP (Routing Information Protocol).In this, every node maintains a routing table all available destinations, the next node to reach to destination, the number of hops to reach the destination periodically send table to all neighbors to maintain topology. DSDV is Destination Based process.

5. Conclusion

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. Here depending on the location of the adversary, network energy expenditure during the forwarding phase increases drastically. The proposed technique routing protocol are provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations and reduce the reimbursement. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

All rights reserved,

6 References

[1] Eugene Y.Vasserman, Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks.2011
[2] Imad Aad, Jean-Pierre Hubaux, and Edward W.Knightly, Denail of service resilience in ad hoc networks, mobicom,2004.
[3] Tuomas Aura, Dos-resistant authentication with client puzzles, Internationalworkshop on security protocols, 2001.
[4] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.
[5] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.
[6] K. Xing, S. Sundhar, R. Srinivasan, M. Rivera, J. Li and X. Cheng; Attacks and Countermeasures in Sensor Networks: A Survey; Computer Science Department, George Washington University; Springer, Network Security; 2005.
[7] T. A. Zia; A Security Framework for Wireless Sensor Networks; Doctor of Philosophy Thesis; The School of Information Technologies, University of Sydney; Feb 2008.
[8] M. Saxena; Security in Wireless Sensor Networks: A Layer-based Classification; Department of Computer Science, Purdue University.
[9] Eugene Y. Vasserman and Nicholas Hopper " Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks " Transactions On Mobile Computing, vol. 12,no. 2, pp.315-332 February 2013
[10] I. Aad, J.-P. Hubaux, and E.W. Knightly,"Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
[11] 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.
[12] T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.
[13] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103- 105, Oct. 2003.
[14] D. Tennenhouse, Proactive Computing, Communications of the ACM, vol.43, pp. 43-50, May 2000.
[15] G.J. Pottie, W.J. Kaiser, "Wireless Integrated Network Sensors," Communications of the ACM, vol.43, pp. 51-58, May 2000.

Gugulothu Veeranna

M.Tech in Computer Science Engineering from JNTU Hyderabad.His research areas includes Programming Languages, Data Base anagement Systems, Mobile Applications, Data Mining

SYED ABDUL MOEED

completed M.Tech in Computer Science and Engineering from JNTU-Hyderabad. Pursuing Ph.D. in the department of Computer Science and Engineering from 2012 at JNTU-Hyderabad. Having 8+ years of working experience as Assistant. Professor, and Placement Officer at Balaji Institute of Engineering & Sciences, Narsampet, Warangal., His research areas include Computer Graphics and image Processing, Computer Networks , Software Engineering, Databases, Programming Languages and Information Security,Network Security.

Fasi Ahmed Parvez working as Associate professor and HOD BALAJI INSTITUTE OF ENGINEERING SCIENCES-NARSAMPET, with

www.ijrct.org

All rights reserved,

12+ years of Experience. Completed M.Tech from JNTU Hyderabad in2010. SUBJECT INTERESTED are programming languages, database management system and data warehouse & data mining.

www.ijrct.org

www.ijrct.org

All rights reserved,

editor@ijrct.org