G. Vijayanand *et al*, International Journal of Computer Science and Mobile Applications,

Vol.2 Issue. 1, January- 2014, pg. 115-120 **ISSN: 2321-8363**

OVERCOME VAMPIRE ATTACKS PROBLEM IN WIRELESS AD-HOC SENSOR NETWORK BY USING DISTANCE VECTOR PROTOCOLS

[1]G. Vijayanand, [2]R. Muralidharan

[1]Assistant Professor, Dept. of Computer Science & Engineering, Muthayammal Engineering College, Namakkal, TamilNadu
(gvijayanand.mec@gmail.com)

[2]Dept. of Computer Science & Engineering, Muthayammal Engineering College, Namakkal, TamilNadu
(muralidharan.cse2010@gmail.com)

Abstract

Adhoc sensor wireless networks has 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 is mainly focusing on routing protocol layer that kind of attacker is known as resource depletion attacks. This 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

Over the last couple of years wireless communication has become of such fundamental importance that a world without it is no longer imaginable for many of us. Beyond the established technologies such as mobile phones and WLAN, new approaches to wireless communication are emerging; one of them are so called ad hoc and sensor networks. Ad hoc and sensor networks are formed by autonomous nodes communicating via radio without any additional backbone infrastructure. A Wireless Sensor Network (WSN) can be defined as a network of small embedded devices, called sensors, which communicate wirelessly following an ad hoc configuration. They are located strategically inside a physical medium and are able to interact with it in order to measure physical parameters from the environment and provide the sensed information. The nodes mainly use a broadcast communication and the network topology can change constantly due, for example, to the fact that nodes are prone to fail. Because of this, we should keep in mind that nodes should be autonomous and, frequently, they will be disregarded. This kind of device has limited power, low computational capabilities and limited memory. One of the main issues that should be studied in WSNs is their scalability feature, their connection strategy for communication and the limited energy to supply the device.

1.1 Wireless Adhoc Network

An ad hoc wireless network is a collection of wireless mobile nodes that self-configure to form a network without the aid of any established infrastructure, as shown in without an inherent infrastructure, the mobiles handle the necessary control and networking tasks by themselves, generally through the use of distributed control algorithms. Multihop connections, whereby intermediate nodes send the packets toward their final destination, are

supported to allow for efficient wireless communication between parties that are relatively far apart. Ad hoc wireless networks are highly appealing for many reasons. They can be rapidly deployed and reconfigured. They can be tailored to specific applications, as implied by Oxford's definition. They are also highly robust due to their distributed nature, node redundancy, and the lack of single points of failure.

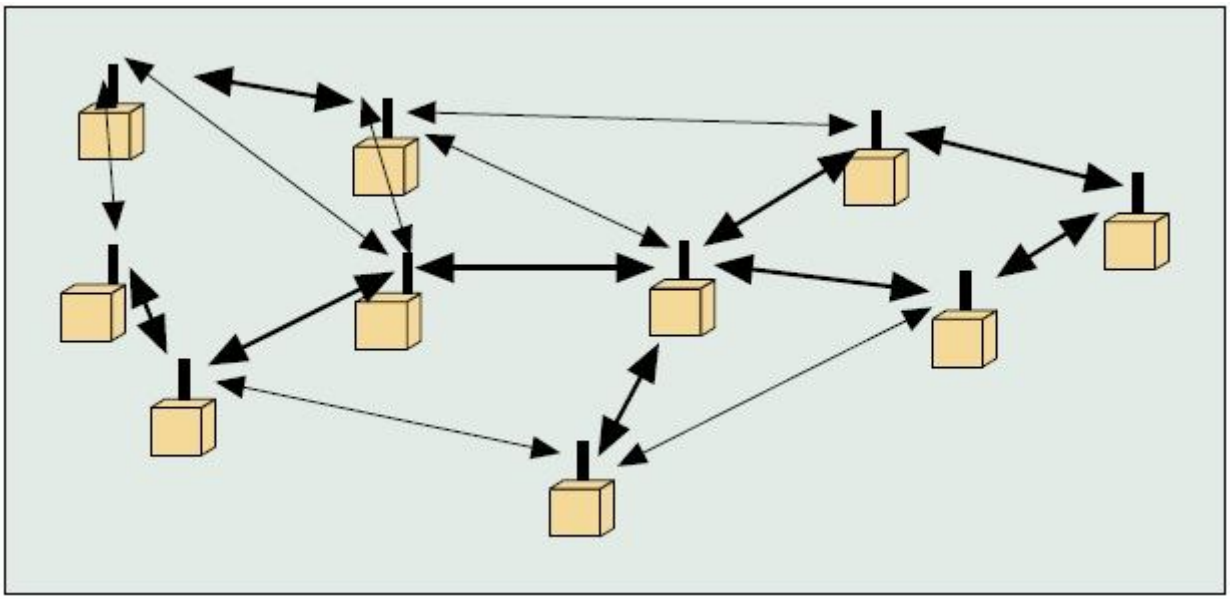

Fig 1.Adhoc Network Structure

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.

2. EXISTING SYSTEM

2.1 Routing Packets

The process of routing is done and initialized by the source node. The source node composes the route and transmitting the packet as mentioned route. The packet is forwarding each and every hops towards the destination. A vampire attacks as a composition and transmission of message this impact causes more energy to be consumed by the network that as well as the honest node transmitted a message of the identical amount to the same destination. Even though it's using the different packet headers. The energy wastage of the transmitting and receiving packets in the network while the malicious node present is higher compare the all honest nodes forwarding the packets to the appropriate destination.

3. PROBLEM DESCRIPTION

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 nodes 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 problem of the network where the consuming energy of each and every nodes in the network will increasing. Since it sends packets in circle, that shown in the fig.2.it targets source routing protocols by exploiting the limited verification of message heads at forwarding nodes, allowing single packets to repeatedly traverse the same set of nodes. 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 kind 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.

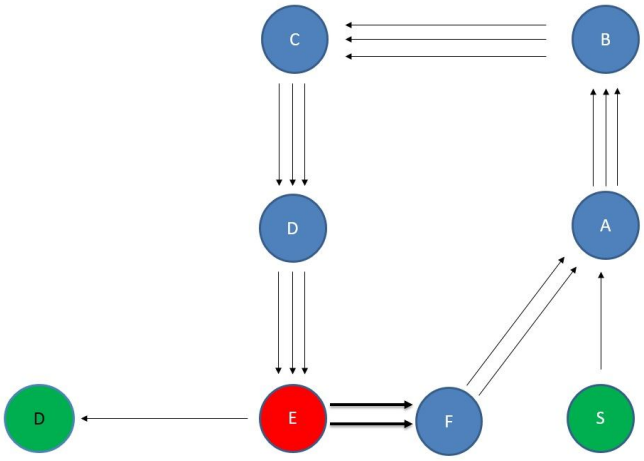

Fig: 2 Carousel attack

4. PROPOSED SYSTEM

4.1 Ad hoc On Demand Distance Vector Routing Protocol

AODV belongs to the class of Distance Vector Routing Protocols (DV). In a DV every node knows its neighbor's and the 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. To characterize the AODV with the five criteria used by Keshav AODV is distributed, hop-by-hop, deterministic, single path and state dependent.

One of the grate advantages of AODV is its integrated multicast routing. 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.

4.2 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.

4.2.1 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

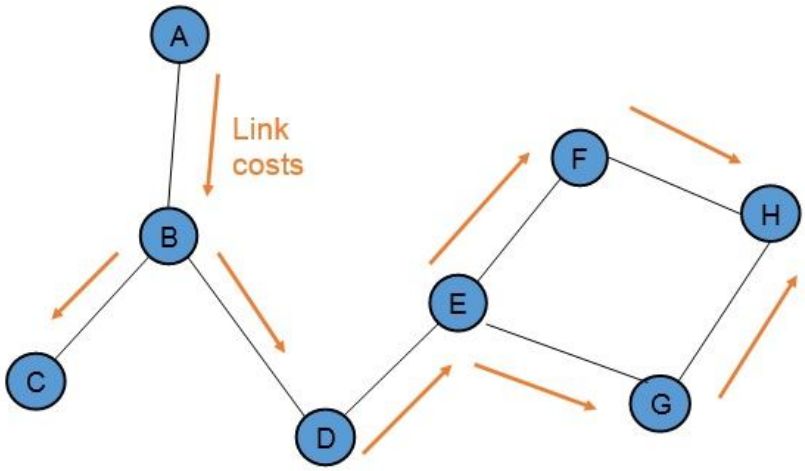

Fig: 3 Link state

4.2.2 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.

4.2.2.1 No-Backtracking

No-backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination In the logical network address space. No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network. (Maliciously induced route stretch is bounded to a factor of 1.).

A solution is to how intermediate nodes process the source route. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be automatically truncated (the last instance of the local node will be found in the source route rather than the first).The carousel attack problem which is solved by these algorithms.

From fig: PATH containing loops:

S->A->…E->…A->…-> E->D Before E loops back it checks Path in reverse, and sends to next node accordingly-> prevents Looping, sends to D on next hop.

4.2.2.2 Characteristics of DSDV

- DSDV is Proactive (Table Driven)

- Each node maintains routing information for all known destinations
- Routing information must be updated periodically
- Traffic overhead even if there is no change in network topology
- Maintains routes which are never used

4.2.2.3 Advantages

- Guarantee Loop Freeness
- Allow fast reaction to topology changes

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.

References

[1] 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

[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] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[6] J. Deng, R. Han, and S. Mishra,"Defending against Path-Based DoS Attacks in WirelessSensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[7] R.C. Shah and J.M. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks," Proc. IEEE Wireless Comm. And Network Conf. (WCNC), 2002.

[8] S. Singh, M. Woo, and C.S. Raghavendra, "Power-Aware Routing in Mobile Ad Hoc Networks," Proc. ACM MobiCom, 1998.

