International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Vampire Attack: Energy Efficient Trust Based Solution

Pritam M. Channawar[1], Dr. Y. V.Chavan[2]

[1]Department of Computer Engineering, Padmabhushan Vasantdada Patil Institute of Technology, University of Pune, India

[2]Principal, Department of E&TC, Padmabhushan Vasantdada Patil Institute of Technology, University of Pune, India

Abstract: ***In sensing and common computing ad hoc low-power wireless networks are an exciting research direction. Earlier security scheme in this area has focused mainly on denial of communication at the routing or medium access control levels. This paper redefines resource depletion attacks at the routing protocol layer. This attack permanently disables networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but depend on the properties of many popular classes of routing protocols. We discussed all protocols are susceptible to Vampire attacks, which are dangerous, difficult to detect, and are very easy to carry out using very few such as one malicious insider sending only protocol-compliant messages. With this, a single Vampire can increase network-wide energy usage by a factor of O(N), here N in the number of network nodes in the network. Proposed algorithm finds the solution for carousal attack and stretch attack to achieve better security. Also trust based energy efficient technique is adopted to keep network active in vampire attack, it also help to detect and avoid malicious nodes in the routing phase.***

Keywords: Security, routing, ad hoc networks, medium access control, wireless networks.

1. Introduction

Ad hoc wireless sensor networks introduces exciting schemes in the future, such as all consumed on-demand computing power, continuous connectivity, quick deployable communication for military and first responders. These kinds of networks already monitor environmental conditions, factory performance, and malicious nodes' group deployment, to name a few applications. Now a days WSNs become more critical to the everyday functioning of people and organizations, also availability faults become less tolerable— unavailability can make the difference between business and lost productivity, power outcome, environmental crises, and lost lives; so high availability of these networks is an important property, and should hold even under critical conditions. Because of their ad hoc organization wireless ad hoc networks are specifically resistant to denial of service (DoS) attacks. While these scheme gives solution to attack on short term availability of network they do not work on attacks that affect long-term availability. The most unavoidable denial of service attack is to entirely grasp nodes' batteries. This is a type of a resource depletion attack, in which battery power as the resource of interest. We study how routing protocols, even those designed for security, less protection from these attacks, we call it as Vampire attacks, since they grasp the life from networks nodes. Vampire attacks are not protocol-specific, in which they do not depend on design properties or implementation faults of particular routing protocols. They exploit general properties of protocol class. The protocol classes are link state, distance vector, geographic and beacon routing.

2. Related Work

These attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very first mention of power exhaustion can be found in as "sleep deprivation torture." The proposed attack prevents nodes from entering a low-power sleep cycle, and thus depletes their batteries in high speed.

We present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several protocols, and suggest how to improve resilience. We show how a malicious packet source can specify paths through the network which are far longer than short, wasting energy at intermediate nodes that forward the packet based on the included source route. In routing concept, here forwarding decisions are made independently by each node (as opposed to specified by the source), we introduce how directional antenna and wormhole attacks can be used to deliver packets to multiple remote network locations, forcing packets processing at nodes that would not generally receive that packet at all, and then increasing network-wide energy expenses. Lastly, we target not only packet forwarding but also route and topology discovery phases. If discovery messages are overloaded, for the cost of a single packet, require energy at every node in the network.

In fist attack an adversary sends packets with purposely introduced routing loops. We call it as the carousel attack, because it sends packets in circles. In second attack, it also targeting source routing, an adversary constructs purposely long routes, potentially traversing every node in the network. We call this the stretch attack, because it increases packet path lengths, forcing packets to be passed by a number of nodes that is independent of hop count without the shortest path between the adversary and packet destination.

3. Attacks on Stateless Protocols

In this system, where network nodes are aware of the network topology and its state. They make local forwarding decisions based on that stored state. There are two important

classes of stateful protocols one is link-state and other is distance-vector.

In link-state nodes keep a track of the up-or-down state of links in the network, and also checks flood routing updates every time a link goes down. The distance vector keep track of next hop to every destination, indexed by a route cost metric, for example, the number of hops. In this only routing updates that change the cost of a given route need to be propagated.

4. Clean-Slate Sensor Network Routing

In this, routing protocol can be modified to provably oppose Vampire attacks through the packet forwarding phase. The original version of the protocol, rather designed for security, is insecure to Vampire attacks. PLGP contains two phases such as topology discovery phase and a packet forwarding phase.

4.1 PLGP in the Presence of Vampires

In PLGP, forwarding nodes are not aware of what path a packet took and allow adversaries to divert packets to any part of the network. They do not know that path is logically further away from the destination than the malicious node. This makes PLGP resistant to Vampire attacks. Consider the directional antenna attack: In this, a receiving honest node may be far away from the packet destination than the malicious forwarding node, but the honest node has no path to tell that the packet it just received is going away from the destination. The honest node only have information is its own address and the packet destination address. Hence, the Vampire can transfer a packet away from its destination without detected. This packet will move at most $logN$ logical hops, and $O(\sqrt{2^i})$ physical hops at the i^{th} logical hop. It will give us a theoretical maximum energy increase of $O(d)$, here d is the network diameter and N is the number of nodes in network.

Function Forward_packet(p)
s← extract_source_address(p);
c← closest_nest_node(s);
if is_neighbor(c) **then** forward(p,c);
else
r← next_hop_to_non_neighbor(c);
forward(p,c);

5. Security Against Vampire Attacks

Here we modify the forwarding phase of PLGP to avoid the vampire attacks. In which first we study the no-backtracking property, which is satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. Formally

Definition:-*No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network.*

5.1 Problem Statement

Existing system does not offer fully satisfactory solution for Vampire attacks during the topology discovery phase, but introduce some information about damage limitations possible with further modifications to PLGPa. Calculation of damage bounds and defenses for topology discovery, as well as handling mobile networks, solution to this problem is proposed system.

5.2 Objectives

1) Repeatedly forwarding same packet
2) Dropping packet
3) Battery depletion
4) Deviation from proper route

5.3 Proposed System

In this system we propose new class of solution to handle above issues

1. In proposed routing protocol track of forwarded packet is kept so that same packet will not be forwarded again.
2. Proposed system attempt to avoid malicious nodes by using **packet to energy ratio.** In order to avoid excess energy consumption.
3. In case of node is dropping packets, an alternate path should be considered.

5.4 Solution Outline:

1. Adopt technique to avoid carousel attack.
2. Adopt technique to avoid stretch attack.
3. A factor of trust should be adopted.

6. Mitigation Methods

6.1 Prevention from Carousel violation

As the paper has now clearly illustrated the way in which carousel attacks develop in a network and its devastating effects on the network. We are now in position to now design a mechanism or technique by which we can minimize this attack. In a WSN network when packet of message is sent from source node (sender) to sink node (receiver), it is forwarded by intermediate nodes present in the network and this carries flow continues till it reaches the sink node. In the proposed system we overcome the carousel attack by performing various validation that ensures that packets doesn't go into infinite loop causing drainage of battery and crashing of network. For validation we define two function forward_packets(p) and verify_ packets(p) where p is packet.

Function forward-packet(P)
{
S ← extract_sender_address(P);
Get the list of all neighboring nodes.
Find particular node C.
C ←closest_neighbor_address( );
If(is_neighbor)
{

$E_{R(c)} = \alpha * P_R$
$E_{S(c)} = \beta * P_S$.
$E_{Remaining(c)} = E_{Total(c)} - (E_{S(c)}+E_{R(c)})$
If(!($EThreshold_{lower} <= E_{Remaining(c)} <= EThreshold_{upper}$))
{
C ←closest_neighbor_address( );
}
Else
{
Forward_packet(P);
}
Else
{
Find_neighbor(s);
Forward_packet(P);
}
}
The above algorithm is used for forwarding the packets by intermediate node. The algorithm extracts the information from source address, this includes IP address of source and destination, then node check whether the IP address his own node and with the destination node, if it matches this means the packet was sent to him only and the process terminates. There can be another condition that the IP address of node and destination doesn't matches, in this case it will forward the packet to closest node.

6.2 Energy Efficient Trust Value:

Every node in the network calculates the energy efficient trust value of each of its neighboring node. Node x calculates the trust of its neighboring node C by using following steps.
1. Get the list of all neighboring nodes.
2. Find particular node C.
3. Calculate the amount of energy consumed by node C for receiving and forwarding packet.
4. $E_{R(c)} = \alpha * P_R$
Here E_R= is the amount of energy consumed by node C to receive all incoming packet.
α= is the configurable parameter (amount of energy required to receive a packet).
P_R= No. of packets received.
5. $E_{S(c)} = \beta * P_S$.
Here E_s= is the amount of energy consumed by node C to send all outgoing packet.
β = is the configurable parameter.(amount of energy required to send a packet to next hop).
P_s= No. of packets sent.
6. $E_{Remaining(c)} = E_{Total(c)} - (E_{S(c)}+E_{R(c)})$
7. $EThreshold_{upper} = EThreshold_{Remaining} + \aleph . EThreshold_{upper}$
= Gives upper bound on threshold.
$EThreshold_{Remaining}$ = Gives average remaining threshold energy of the WSN.
$\aleph$ = Configurable parameter.
8. $EThreshold_{lower} = EThreshold_{Remaining} - \lambda . EThreshold_{lower}$= Gives lower bound on threshold.
λ = Configurable parameter.
9. $EThreshold_{lower} <= E_{Remaining(c)} <= EThreshold_{upper}$.

In above equation if remaining energy is less than the lower bound then that node may drop the packet, so such nodes are omitted in further transmission. Also, if remaining energy of node is more than the upper bound then such node is detected as malicious, as these nodes only receive packets and drops the received packet.

The verify_packets(p)function will check whether the packet has already arrived in the intermediate node or not. For this we are continuously tracking the message for duplication in node, as soon as the same packet arrives at node it will discard the packet and prevent duplicate packets to enter in the network. Research is being carried out to perform more number of validation using log file so that we can make network more secured from these violations.

6.3 Prevention from Stretch Violation

The algorithm designed for overcoming the stretch is an unconventional way. The proposed technique uses cryptography algorithm RSA 128-bit. In this algorithm there are two keys public key and primary key. As we have already studied the Stretch attack in which packets travels a longer route and continues till its TTL value expires. Thus receiver never receives the sent packets. The problem in designing the algorithm was that message should receive within the TTL value limit from sender to receiver. This is the reason that we first make the channel secured for transmitting the packets and then exchanges of packets are done. Using the principle of RSA algorithm the source generates the public key and private key. The private key is then sent to respective receiver. After receiving the private key, ACK signal is sent from receiver to sender. Receiving of ACK signal at the senders end indicate that a secured channel has been established between the sender (source) and receiver (sink).In the next stage the message is converted into cipher - text using public key and this cipher-text is sent from source in WSN network. Due to encrypted text, nodes are unable to read the message and this adds to security of packets. These messages after receiving at receiver are decrypted using private key and the message packets are obtained in its original form. In this way we conquer the issue in which the routing path is extended by visiting node that is unnecessary.

7. 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 implementation, but rather expose vulnerabilities in a number of popular protocol classes.

We proposed a solution to cover carousal attack, stretch attack and energy depletion problem with the help of efficient algorithm. Proposed algorithm gives better solution than the existing system for vampire attack.

References

[1] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, 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] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
[6] D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.
[7] W.C. Cheng, C. Chou, L. Golubchik, S. Khuller, and Y.C. Wan, "A Coordinated Data Collection Approach: Design, Evaluation, and Comparison," IEEE J. Selected Areas in Comm.,vol. 22, no. 10, pp. 2004-2018, Dec. 2004.
[8] A. Manjeshwar and D.P. Agrawal, "Teen: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp., Apr. 2001.
[9] A. Scaglione and S.D. Servetto, "On the Interdependence of Routing and Data Compression in Multi-Hop Sensor Networks," Proc. ACM MobiCom, 2002.
[10] M. Zhao, M. Ma, and Y. Yang, "Efficient Data Gathering with Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks," IEEE Trans. Computers, vol. 60, no. 3, pp. 400-417, http://doi.ieeecomputersociety.org/10.1109/TC.2010.140, Mar. 2011.
[11] Edwin prem kumar, Baskaran Kaliapermal, Elijah blessing Rajsingh "Research issues in Wireless sensor network Applications: A Survey"- *International Journal of information and electronics engineering*,Vol 2 No 5 September 2012
[12] Kazem sohraby *Applications of Sensor networks*. First edition 2012
[13] Yanli Yu,Keigiu Li, Ping Li "Trust Mechanism in wireless sensor networks :Attacks analysis and countermeasures", *Journal of networks and computer applications press 2011*.
[14] Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", *Journal of Network and Computer Applications.*

Author Profile

Pritam Channawar, Research Scholar Padmbhushan Vasantdada Patil Institute of Technology Bavdhan, University of Pune .She received B.E. in computer science and engg from MGM's college of Engineering Nanded, SRTM University Currently she is persuing M.E. in computer engineering from Padmbhushan Vasantdada Patil Institute of Technology Bavdhan, University of Pune.

Dr. Y. V. Chavan has completed his Bachelor of Engineering in Electronics and Master of technology in 1989 and 1999 respectively from Nagpur University. He has completed his Ph D (Sep 2011) from RGPV, a state technological University, Bhopal. Previously he worked as Lecturer in Electronics at Pravara Rural Engineering College Loni, Ahmednagar, (M.S.). He worked as Assistant Professor and Head of Department for Dept of E&TC at Amrutvahini College of Engineering, Sangamner, Ahmednagar (M.S.)-India. He also worked as Assistant Professor at Maharashtra Academy of Engineering, Alandi, Pune. He also worked as Vice-Principal at RSCOE, Tathawade, Pune. He is at presently working as Principal at PVPIT, Bavdhan, Pune. His area of interest is Modeling and Simulation and its implementation using VLSI.