World Journal of Engineering Research and Technology

WJERT

www.wjert.org

SJIF Impact Factor: 5.924

VAMPIRE BITES HINDER WIRELESS AD HOC SENSOR NETWORKS

[*1]Dr. Selvi M. and [2]Dr. R. Balakrishna

[1]Associate Professor, Dept. of CSE, Raja Rajeswari College of Engineering.

[2]Dean & Professor, Dept of CSE, Raja Rajeswari College of Engineering.

Article Received on 14/05/2021 **Article Revised on 13/05/2021** **Article Accepted on 02/09/2021**

***Corresponding Author**
Dr. Selvi M.
Associate Professor, Dept. of CSE, Raja Rajeswari College of Engineering.

ABSTRACT

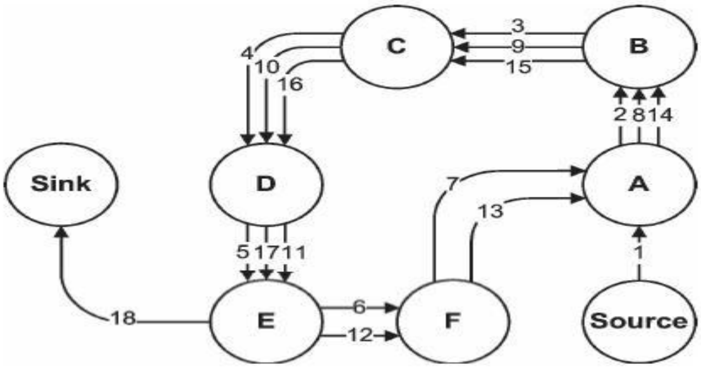
New research in areas like sensing andpervasive computing focuses on wireless networks with no administrative requirements. Security researchers previously focused mostly on cutting down connectivity by controlling routing or MAC layers. The study looks at how resource depletionattacks at the routing protocol layer can rapidly drain node battery power, making networks useless. Many major routing protocols suffer from "Vampire" assaults. These attacks include a variety of components and can affect many routing protocols. We've learned that Vampire attacks, which arepowerful, hard to detect, and simple to execute with just one bad actor providing protocol-compliantmessages, are capable of devastating all of the protocols that we're looking at. A single Vampire can single-handedly wreck network-wide energy usage by an order of magnitude, where N is the number of nodes in the network. In this paper, we will detail a new protocol for the forwarding phase of a Vampire- type network device that is capable of proving itslimits.

INTRODUCTION

Military and first responders are going to love the new applications for ad hoc wireless sensor networks (WSNs) that can include everywhere-on-demand processing capacity, continuous connectivity, and easily deployable communication systems in the near future. Many possible uses of such networks exist already, including monitoring environmental conditions, industrial performance, and military deployment, among others. The increasing importance of WSNs in daily life means that the degree of network reliability is more important than ever—in some circumstances, a network's in operability may mean the difference between business as usual and lost productivity, power outages, environmental disasters, and even lives lost; this means that maintaining high network availability is critical, even when malicious conditions are a possibility. Wireless ad hoc networks have been widely studied, due to their high vulnerability to DoS attacks and have so developed defensive techniques. While these methods can stop attacks on network availability in the near term, they don't address long- term availability – the most prevalent sort of attack being to drain the batteries of nodes, which fully drains a network's long-term availability. Here's a visual illustration of a resource depletion attack, which uses the battery as the resource. Even routing protocols, which are supposed to be robust, are subject to attacks we call Vampire attacks, because they leech the resources of nodes in a network.

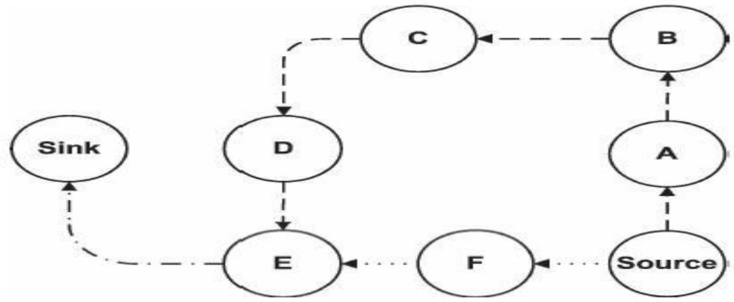
In our work, we explain an increase in the severity of Vampire attacks, analyse various example procedures for their vulnerability, and give advice for how to avoid being taken advantage of and how to be resilient. We can see this waste in how a packet will travel down a path much longer than it needs to (when intermediary nodes forward the packet based on its source route).

When the attack starts, the adversary adds routingloops into packets they send.
The carousel attack is what we call it.



(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.

Our next attack exploits the fact that adversaries can craft their own routes which go via everynode in the network. This is what we call thestretch attack.



(b) Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

EXISTING SYSTEM

Work on secure routing attempts to ensure that adversaries cannot construct an erroneous networkpath via path discovery; this is to prevent them from intercepting network traffic and thereby exploitingnetwork vulnerabilities. Protocols that aim to be moreenergy efficient are likewise a bad idea since they rely on the nodes being willing to cooperate, and are therefore unable to defend against attacks. The route exhaustion attack is both old and new. Though some of the individual attacks are basic, and we've previously seen draining and exhausting attacks, the majority of previous work has focused on lower layers in the protocol stack such as the medium access control (MAC) or application layers, while information on the routing-layer resource exhaustion threat has been sparse. The simultaneous occurrence of two kinds of attacks, carousel and stretch, is possible. To begin, an adversary builds packets that contain self-repeating loops for routing. The assault is referred to as a carousel because it sends packets in a round manner. Source routing protocols are undermined by insufficient verification of header information because of which a same packet can get routed through the same set of nodes. Though other publications discuss this technique in a superficial way, neither an understanding of its defence nor a comprehensive look at its attack has been shared. We will examine one more attack that affects source routing today. In this attack, an attacker creates routes that are so long they would theoretically go through every single node on the network. The stretch attack has a nickname — it's named after its effect: an increase in the number of intermediate nodes alongthe packet's path. This enlarges the possible pathstaken by the packet between its origin and its final destination, which would have previously been more predictable based on the single shortest route to the packet's destination.

PROPOSED SYSTEM

We have analysed the operations of a vampire node, which utilises packets and RREQ flooding to bring its broadcast rate to the same as other nodes on the network and consequently create an overabundance of hire energy. We find this illustrated in Figure 1. The proposed study was done because network node energy variancechanges throughout the course of the day and night. First, a list of nodes suspected of having communication or energy capabilities is drawn up by comparing their broadcast and energy levels. If a node's consumption is higher than the variance it has been assigned, it is put aside and then evaluated for consumption. A suspected vampire node is found if the rate of energy use falls, and is removed.

The following is a description of the proposed algorithm, which will identify threats on a scheduled basis. Using the formula, compute the variance of the broad cast of all nodes in the network at the current moment.

$$\mathbf{V_{BrT1} = 1/n\sum_{I=1}^{n} (Bri - \mu)2}$$

Where VBrT1 = variance of broadcast of nodes at time T1

μ=is the mean value

Identify a group of nodes that have broadcasted more VBrT1 than what can be expressed by using the symbol. set of nodes ΔBrT1 = n1,n2…….

Determine the variance of energy levels across all nodes at the same time T1 by referring to thefollowing formula:

$$\mathbf{V_{ErT1} = 1/n\sum_{I=1}^{n} (Eri - \mu)2}$$

Where VErT1 = variance of broadcastof nodes at time T1

Prepare a series of nodes with higher energy thanVErT1, which can be referenced by set of nodes ΔErT1 = n1,n2…….

To find the set of nodes, people on the network aresuspected.

ΔT1 = ΔErT1 n ΔBrT1

The probability of having confirmed "suspected" nodes is assessed by measuring energy variance at time T2. Compute the network's final set of suspects.

ΔT = ΔT1 n ΔT2

In order to find and eliminate a malicious node from the network, we are temporally removing a suspicious node from the network. Compute Vermillion and Vibrancy Compute the different for time T2 and T1.

diffT2T1= VErT2 - VErT1

Compute the different for time T3 and T2

$\mathrm{diffT3T2} = \mathrm{VErT3} - \mathrm{VErT2}\Delta\mathrm{T2}$

If $\mathrm{diffT2T1} > \mathrm{diffT3T2}$,

Remove node from network permanently Therefore, suspected node becomes a node of vampire. If there are several suspected nodes, alternate temporary deletion is repeated and one of them turns into an attacker node in the same process.

CONCLUSION

A literature review in this paper investigates how different stateless and stateful routing protocols fail under a vampire attack, and also compares the approaches others have taken to find solutions for vampire assaults. The idea is that the suggested methodology will give WSNs the ability to easilydetect and correct vampire attacks. It also allows for WSNs to deal with changes in their topology. Because of the proposed method, a vampire attacker will be detected based on its network node packet broadcast rates and energy metrics. The recommended method will be used to experiment with a new way in the near future, which will involve the usage of NS2 network simulator and will provide results regarding the vampire network environment, including results for energy consumption, PDR, and throughput.

REFERENCES

1. I.F. Akyildiz, W. Su*, Y. Sankarasubramaniam, E. Cayirci 2001, Wireless sensor networks: asurvey, Elsevier Computer Networks.
2. Jamal N. Al-Karaki Ahmed E. Kamal, Routing Techniques in Wireless Sensor Networks: A Survey.
3. Rajkumar, Sunitha K R, Dr.H.G.Chandrakanth 2012, A Survey on Security Attacks in Wireless Sensor Network, International Journal of Engineering Research and Applications.
4. Jaydip Sen, Routing Security Issues in Wireless Sensor Networks: Attacks and Defenses, Innovation Lab, Tata Consultancy Services Ltd.
5. Wood, A.D. &Stankvic, J.A. 2002 Denial of service in sensor networks. IEEE Computer, 35(10): 54-62.
6. Karlof, C. & Wagner, D. 2003 Secure routing in wireless sensor networks: attacks and countermeasures. Proceedings of the 1st IEEE International Workshop on Sensor

Network Protocols and Applications.

7. Eugene Y. Vasserman and Nicholas Hopper 2013, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. IEEE transactions on mobile computing.
8. B. Umakanth1, J. Damodhar2 2013, Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks, International Journal of Engineering Trends and Technology (IJETT).
9. V.Subha1, P.Selvi 2014, Defending against vampire attacks in wireless sensor networks, International Journal of Computer Science and Mobile Computing.
10. V.Sharmila1 2014, Energy Depletion Attacks: Detecting and Blocking in Wireless Sensor Network, International Journal of Computer Science and Mobile Computing.