Defending Against Energy Draining Attacks In Wireless Sensor Networks Using Time Slot-Based Method

[1] Ms. K.E.ESWARI MCA.,M.Phil.,M.E., [2] S.JEEVANANTHAM

[1]Associate Professor, Department of computer application, Nandha Engineering College, Erode-52
[2] Final year, Department of computer application, Nandha Engineering College, Erode-52
[1]Email id: eswari.eswaramoorthy@nandhaengg.org
[2]Email id: jeevanantham333@gmail.com

---***---

Abstract - *Ad-hoc low-power wireless networks are an exciting research direction in sensing and prevalent calculating. Previous secure work in this section has absorbed chiefly on rejection of contact at the routing or average access control levels. This paper explores resource reduction attacks at the routing protocol layer, 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 most popular classes of routing protocols. Find that all examined protocols are susceptible to Vampire attacks, which are devastating, challenging to detect, and are easy to carry out using as few as one malicious insider sending only protocol- compliant messages. In the wickedest case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. discuss methods to mitigate these types of attacks, with a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.*

***Key Words*: Denial of service, security, routing, ad-hoc net- works, sensor networks, wireless networks.**

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. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable — lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to their ad-hoc organization, wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks [4], and a great deal of research has been done to enhance survivability [4].

While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability — the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper consider how routing protocols, even those designed to be secure, lack protection from these attacks, which call Vampire attacks, since they drain the life from networks nodes. These attacks are distinct from previously-studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power-draining and resource exhaustion attacks have been discussed before [2], prior work has been mostly confined to other levels of the protocol stack, e.g. medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks.

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. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent. Contributions. This paper makes three primary contributions. First, thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. 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 Ariadne, SAODV, and SEAD 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 messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behaviour and cannot optimize out malicious action. Second, show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary). Third, modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

2. CLASSIFICATION

The first challenge in addressing Vampire attacks is defining them — what actions in fact constitute an attack? DoS attack in wired networks are frequently characterized by amplification: an adversary can amplify the resources it spends on the attack, e.g. use one minute of its own CPU time to cause the victim to use ten minutes. However, consider the process of routing a packet in any multi-hop 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. If consider 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 (at the intermediate nodes) is lower than the cost to the source to compose and transmit it. So, 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. Define a Vampire attack as the composition and trans- mission 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. Measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e. the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1. Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.

2.1 PROTOCOLS AND ASSUMPTIONS

In this paper consider the effect of 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 proposed by Parno. [2]. While this is by no means an exhaustive list of routing protocols which are vulnerable to Vampire attacks, 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, 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 re-discovery 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. Note that this is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Intelligent adversary placement or dynamic node compromise would make attacks far more damaging.

While for the rest of this paper will 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. Assuming that packet processing drains at least as much energy from the victims as from the attacker, a continuously- recharging adversary can keep at least one node permanently disabled at the cost of its own functionality. However, recall that sending any packet automatically constitutes amplification, allowing few Vampires to attack many honest nodes. Will show later that a single Vampire may attack every network node simultaneously, meaning that continuous recharging does not help unless Vampires are more resource-constrained than honest nodes. Dual-cycle networks (with mandatory sleep and awake periods) are equally vulnerable to Vampires during active duty as long as the Vampire's cycle switching is in sync with other nodes. Vampire attacks may be weakened by using groups of nodes with staggered cycles: only active-duty nodes are vulnerable while the Vampire is active; nodes are safe while the Vampire sleeps. However, this defence is only effective when duty cycle groups outnumber Vampires, since it only takes one Vampire per group to carry out the attack.

2.2 OVERVIEW

In the remainder of this paper, present a series of increasingly damaging Vampire attacks, evaluate the vulnerability of several example protocols, and suggest how to improve resilience. In source routing protocols, show how a malicious packet source can specify paths through the network which are far longer than optimal, wasting energy at intermediate nodes who forward the packet based on the included source route. In routing schemes where forwarding decisions are made independently by each node (as opposed to specified by the source), suggest how directional antenna and wormhole attacks can be used to deliver packets to multiple remote network positions, forcing packet processing at nodes that would not normally receive that packet at all, and thus increasing network-wide energy expenditure. Lastly, show how an adversary can target not only packet forwarding but also route and topology discovery phases — if discovery messages are flooded, an adversary can, for the cost of a single packet, consume energy at every node in the network. In our first attack, an adversary composes packets with purposely introduced routing loops. call it the carousel attack, since it sends packets in circles as shown in Figure 1. 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. Brief mentions of this attack can be found in other literature [2], but no intuition for defense nor any evaluation is provided. In our second attack, also targeting Source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. Call this the 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. An example is illustrated in Figure 2. Results show that in a randomly-generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overheard packets, assume that only messages originated by adversaries may have maliciously-composed routes. Explore numerous mitigation methods to bound the damage from Vampire attacks, and find that while the carousel attack is simple to prevent with negligible overhead, the stretch attack is far more challenging. The first protection mechanism consider is loose source routing, where any forwarding node can reroute the packet if it knows a shorter path to the destination.

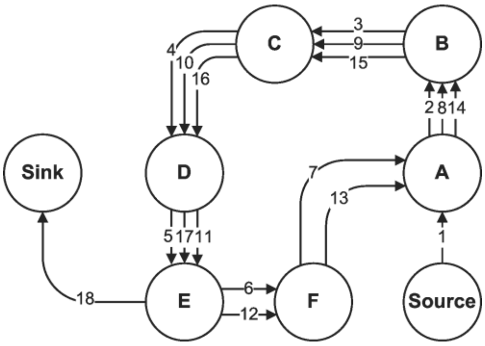

Fig -1: Carousel Attack

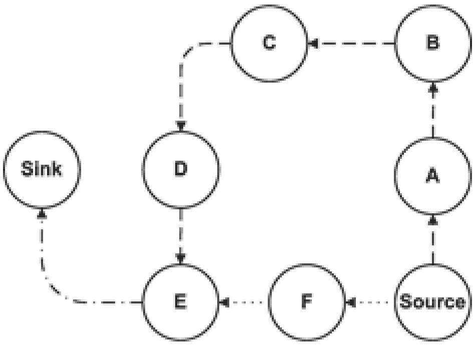

Fig -2: Stretch Attack

Unfortunately, this proves to be less efficient than simply keeping global network state at each node, defeating the purpose of source routing. In our second attempt, modify the protocol from [2] to guarantee that a packet makes progress through the network. Call this the no- backtracking property, since it holds if and only if a packet is moving strictly closer to its destination with every hop, and it mitigates all mentioned Vampire attacks with the exception of malicious flooded discovery, which is significantly harder to detect or prevent. Propose a limited topology discovery period ("the night," since this is when vampires are most dangerous), followed by a long packet forwarding period during which adversarial success is provably bounded. Also sketch how to further modify the protocol to detect Vampires during topology discovery and evict them after the network converges.

3. RELATED WORKS

The Research in Wireless Sensor Networks(WSN) is a task to researcher to makes the efficient service of the network. The Time synchronization is mainly used to find the service time of the networks. So, it using L-SYNC protocol which is mainly used for heterogeneous topologies, this protocol is scalable in unreliable and also in noisy environments. The denial-of-service (DoS) attacks against 802.11's MAC protocol. Such attacks, which prevent legitimate users from accessing the network, are a service delay problem in all networks, but they are particularly threatening in the wireless context. To re authenticate service due to (DOS) and any higher-level timeouts or back offs that may suppress the demand for communication. This paper is useful for send the data in secure path. During the data service if a node detects a link failure, it sends an unsolicited route reply, the neighbor node which it is forwarding traffic through the link. This route reply is propagated to each source that is sending traffic through the failed link, re-initiating the route discovery process. Hence, it is very useful to get efficient energy of network [1].

4. PROBLEM DESCRIPTION

The Vampire attack will attack the service of the network with any number of nodes which is infected. The node, which suddenly change the networks behavior is called as "Malicious node". The nodes energy will be affected by the malicious nodes. Routing path is introduced by using the shortest path routing algorithm. The path won't be changed by the intermediate nodes. It has a chance to happening vampire attack. The adversary nodes composes packets with purposely introduced routing loops.

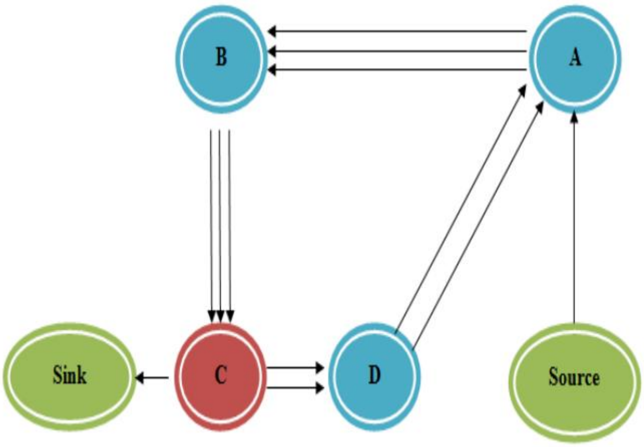

Fig -3: Carousel Attack

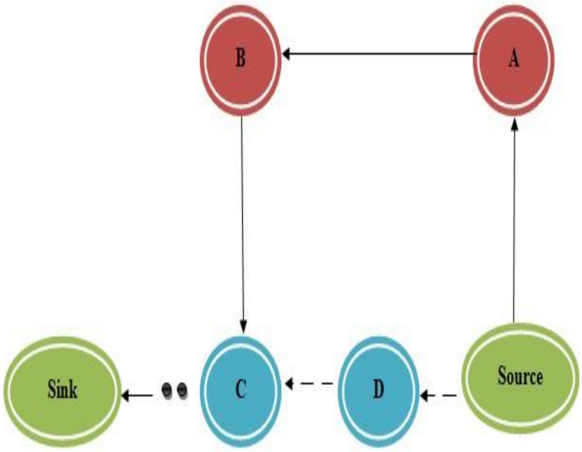

Fig -4: Stretch Attack

Therefore, it is a problem of the network which drains the nodes energy. The single packets can be repeatedly traverse to the same set of nodes and delay the service of network. If the process is continue for the certain period of time and looping of nodes will waste the each nodes battery power. The carousel attack happens through malicious node and loop the nodes itself and delay the service fig 3. Then, the stretch attack will reroute the packets fig 4. Identifying the vampire attack in the network is very difficult and also to detect.

5. PROPOSED METHODOLOGY

The proposed system includes all the existing system implementation. In addition, secure synchronization is carried out. The new system eliminates the synchronization problem by calculating the transmission schedule using the weight information based on the proposed algorithm steps. In addition, synchronizing all the neighbor nodes which belong to various clusters, must to attain the stable state of the network. Present some techniques for synchronizing the nodes that periodically broadcast content and presence updates to co-located nodes over an ad hoc network. The new algorithms are synchronize the periodic transmissions of nodes. Hence, these allows nodes to save battery power.

5.1 Advantages Of The Proposed System

- In addition to Vampire attack, Inflation attack scenario is also prevented.
- Weight based synchronization if works with correct weight information chooses the correct cluster for the given node.
- Future peak detection scenario makes the correct cluster identification and avoids the inflation attack induced by the malicious nodes which sends wrong weight information.
- The suspicious node can be tracked easily since it does not satisfy the node behaviors of neighbor nodes.

5.1 Weight Based Synchronization

The Weight based synchronization is used to know the weight of the nodes [3].To calculate the weight it using Network flow concept. The Network flow is also using many terms like Residual capacity of the path and augmenting path. The Ford-Fulkerson Algorithm is used to find the residual capacity of the path. The residual capacity of the node makes better nodes power. The weight will be calculated with its maximum flow of data.

5.2 The Future Peak Detection

The Future peak detection is used to calculate the sending time of packets. To find the time of data transfer it using L-SYNC [3]. The L-SYNC is a synchronization protocol which has better precision in secure synchronization.

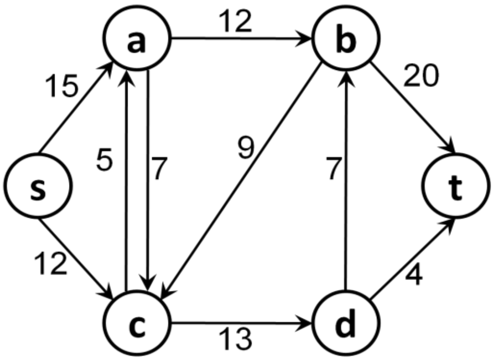

Fig -5: Example Network flow

This is very useful to find the time of data transfer in the network.

5.3 The Randomized Future Peak Detection

The Randomized future peak detection is used to set the nodes path. Using the NS-2, the number of nodes are set with its unique nodes id. The Routing path will be selected based on the efficient battery with secure synchronization. The content based multicasting protocol is mainly used to collect the content of packet transfer time and nodes weight to set path. The architecture diagram fig 6. Explains the whole process of the service which is given below,

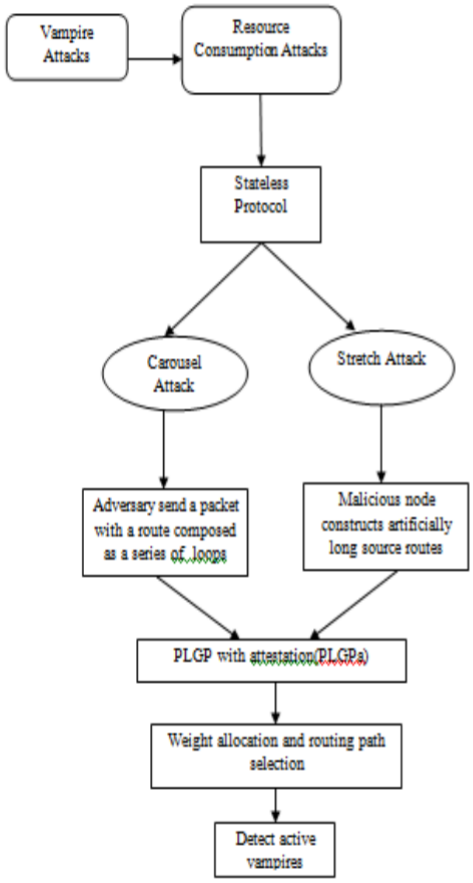
Vampire Attacks
Resource Consumption Attacks
Stateless Protocol
Carousel Attack
Stretch Attack
Adversary send a packet with a route composed as a series of loops
Malicious node constructs artificially long source routes
PLGP with attestation(PLGPa)
Weight allocation and routing path selection
Detect active vampires

Fig -6: Architecture Diagram

6. SIMULATION REQUIREMENT

The hardware required for the simulations are Intel Pentium 4 processor, 4 GB RAM and 20 GB hard disk drive. The software required are Ubuntu Operating System, NS2 simulator tool for running simulation and the language used is TCL and C++. The simulation is conducted with 40 nodes in a flat space size of 670 x 670 m. The maximum hop allowed is four and the moving speed of mobile node is limited to 20 m/s with a pause time of 100s. The total simulation time is 1000s and the traffic used is User Datagram Protocol with Constant Bit Rate (CBR) with a packet size of 512 B.

6.1 Parameters For Evaluation

The following parameters are considered for the performance evaluation of the network in the presence of the malicious nodes.

- Packet Delivery Ratio (PDR): The number of ratio of packets which is received by the destination node to the number of packets sent by the source node.
- Throughput: Average rate of successful number of packets delivery.
- Residual Energy: The residual energy used to promote the communication efficiency of the system and to ensure a balance energy consumption of each nodes in WSN.

6.2 Advantages

- The suspicious node can be tracked easily.
- It has an efficient path from source to sink.
- The services from source to sink can be prevent from attacks.

7. CONCLUSIONS

The 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. The vampire attacks doesn't depends on particular protocol. The proposed system eliminates the attackers hacking performances. It help us to get the efficient battery power and routing path selection.

REFERENCES

[1] L.M. Feeney, “An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks,”Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[2] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensornetwork routing: A clean-slate approach, CoNEXT, 2006.

[3] Masoume Jabbarifar, Alireza Shameli Sendi, Alireza Sadighian, Naser Ezzati Jivan, Michel Dagenais“A reliable and efficient time synchronization protocol for heterogeneous wireless sensor network”Journal,Nov 2010.

[4] Anthony D. Wood and John A. Stankovic, Denial of service in sensor networks, Computer 35 (2002), no. 10.