Abstract –

Wireless sensor network is a correspondence network over the sensors nodes. A sensor node gathers data about the physical condition. In Wireless Sensor Network, we concentrate on the Vampire Attacks. The vampire Attack is the asset exhaustion Attack at layer of network to lessening the battery energy of any node. In this paper of Time based detection and counteractive action of Vampire Attacks in WSN, we concentrate on Carousel assault and Stretch attacks. Our proposed conspire intends to detecting the malicious assailants and afterward keeping them from participating in the correspondence procedure. A calculation is proposed to recognize and keep such attacks from depleting energy of the nodes. The execution of the network has been investigated based on bundle conveyance proportion, throughput, and energy utilization.

Keywords— Vampire attack, Wireless Sensor Network attack, WSN, Clustering, Node, Routing.

I. Introduction

Wireless sensor network contains number of sensors that are appropriated over a wide geographical area. A few applications utilizes a constitute network which is shaped via independent sensor [1]. The applications are auxiliary wellbeing checking, human services observing, modern checking, in a flash deployable correspondence for military, on-request figuring, stock following, control administration, production line execution, control, brilliant detecting along these lines data or information assembling and handling, seismic detection and acoustic detection[2].The life of network assumes a vital part in such applications. Many looks into concentrate on expanding the life expectancy of WSN [3]. One new sort of asset (energy) consumption assault is known as vampire assault [5] which depletes the battery energy of the node to cripple the entire network. This node persistently sends messages to different nodes so every node in the network loses energy nearer causing the disappointment of the entire network soon. The vampire assault can focus on any directing convention and does not particular to specific convention. They are hard to identify in light of the fact that they don't change the first message. There are two sorts of vampire attacks expressed in [5] Carousel assault and Stretch assault. In merry go round assault a progression of circle is framed between the source and the sink node. So the course length is expanded and goes past the utmost of nodes in the network. Because of this energy utilization of nodes increments and subsequently limits the network lifetime. In extend assault, falsely long course from source to sink is made by a foe making bundles navigate a bigger course and depleting additional energy.

II. Related Work

David R. Raymond, Randy C. Marchany, Michael I. Brownfield and Scott F. Midkiff, talked about foreshewing of rest attack[6], in which a sensor node's energy supply is focused on. Attacks of this write can lessen the sensor lifetime from years to days and disturbingly affect a sensor network. This paper proposed three commitments for sensor network security. To start with, it characterizes foreshewing of rest attacks on WSN MAC conventions based on an aggressor's learning of the MAC convention and capacity to infiltrate the network. Second, it investigates potential attacks from each assault characterization, both displaying their effects on sensor networks running four driving WSN MAC conventions and breaking down the productivity of executions of these attacks on three of the conventions. At long last, it proposed a system for shielding against foreshewing of rest attacks and gives particular methods that can be utilized against every refusal of rest helplessness. Bryan Parno, Mark Luk, Evan Gaustad and Adrian Perring[7] have
presented another protected steering convention for sensor networks. Our convention requires no exceptional equipment and gives message conveyance even in a situation with dynamic enemies. Outline another sensor network steering convention with security and proficient yet exceedingly flexible to dynamic attacks our convention appoints a network deliver to every node and sets up directing tables utilizing a recursive gathering calculation. For a given topology, the calculation continues altogether deterministically, avoiding attacks on steering data and constraining a subverted node's capacity to perform malicious activities. The current secure directing conventions presented either an unsuitable level of multifaceted nature or an over the top execution punishment. Jing Deng, Richard Han, Shivakant Mishra[6], had proposed an Intrusion tolerant directing convention for wireless sensor networks (INSENS). INSENS builds sending tables at every node to encourage correspondence between sensor nodes and a base station. It limits calculation, correspondence, stockpiling, and data transmission necessities at the sensor nodes to the detriment of expanded calculation, correspondence, stockpiling, and transfer speed prerequisites at the base station. The extent of harm incurred by gatecrashers is additionally constrained by limiting flooding to the base station and by having the base station arrange its bundles utilizing one-way grouping numbers. Jing Deng, Richard Han and Shivakant Mishra, have examined Denial of administration (DoS)[8] attacks can cause extreme harm in asset obliged, wireless sensor networks. In WSNs, an enemy can dispatch with little exertion a way based refusal of administration (PDoS) assault that will have a serious far reaching impact on the WSN, crippling nodes on all branches downstream of the way, because of the tree-organized topology of WSNs. To guard against a PDoS assault, a middle of the road node must have the capacity to recognize spurious parcels or replayed bundles, and after that reject them. Rahul C.Shah and Jan M.Rabaey[9] have examined sensor networks has prompted various steering plans that utilization the restricted assets accessible at sensor nodes all the more proficiently. These plans normally endeavor to locate the base energy way to upgrade energy utilization at a node. In this paper tended to least energy ways may not be ideal from the perspective of network lifetime and long haul availability. To improve these measures, proposed another plan called energy mindful directing that utilizes problematic ways infrequently to give considerable additions. This paper proposed new convention named energy mindful directing. This convention to build the survivability of networks, it might be important to utilize imperfect ways once in a while. To accomplish this, various ways are found amongst source and goals, and every way is doled out a likelihood of being picked, contingent upon the energy metric. Each time information is to be sent from the source to goal, one of the ways is arbitrarily picked relying upon the probabilities. Likewise unique ways endeavor persistently, enhancing resistance to nodes moving around the network. Utilizing probabilistic sending to send movement on various courses gives a simple method to utilize different ways without including much many-sided quality or state at a node. Jae-Hwan Chang and Lindros Tassiulas[10] had broadened the most extreme lifetime directing issue to incorporate the energy utilization at the recipients amid gathering. In wireless sensor networks where nodes work on restricted battery energy, the proficient usage of the energy is critical. One of the principle attributes of these networks is that the transmission control utilization is firmly combined with the course determination. The energy effectiveness has been considered in wireless adhoc network directing, however the customary steering objective was to limit the aggregate expended energy in achieving the goal.

III. Problem Statement

Vampire attacks are assault in networks; it is the piece and transmission of a message that makes more energy be devoured by the network, than if a legitimate node transmitted a message of indistinguishable size to a similar goal i.e. Vampire assault implies making and sending messages by malicious node which causes more energy utilization by the network prompting moderate exhaustion of node's battery life. Vampire assault occurs in the network in the sense, any of the nodes in the network which is influenced or contaminated and this nodes conduct is suddenly changing for the network conduct, this sort of nodes are called "Malicious node". In the event that malicious nodes show in the network energy that have been utilizing by every last nodes will increments radically. The malicious node has been put in the network exceptionally. To start with in the middle of the directing nodes, and the
second set in the Source node itself. The steering way is found by source node by utilizing most brief way directing calculation and the way ought not be alterable by the moderate nodes. In this sort of event there is an opportunity to happening assault. The enemy creates parcels with deliberately presented steering circles. This is one of the real issues of the network where the devouring energy of every last node in the network will increment. The principle issue these sorts of assailants are it's not effectively distinguished on the off chance that it assaulted or influenced the network. It will require some long investment to recognize and make guarantee that it exhibited in the network. We additionally examine this vampire attacks and distinguished issues by grouping it based on kind of convention utilized amid parcel directing inside network.

IV. Proposed Methodology:

Security Against Vampire Attacks The forwarding phase of PLGP is modified to provably avoid the above mentioned attacks. First we introduce the 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. More formally: Definition 1: 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.) If a network satisfies this property, that network is resistant to vampire attacks. i.e., no-backtracking implies vampire resistance. PLGP protocol does not satisfy no-backtracking. The proposed system concentrates on a secure data transmission from the adversary nodes in the sensor network. In order to build a secure network, the network should be an extinct to adversary nodes. So we implement Intrusion Detection System (IDS) in the network. An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports. Here we are using Networkbased IDSs which uses the network traffic as the audit data source, relieving the burden on the hosts that usually provide normal computing services. We implemented a 50 node network topology using NS-2 simulation in that 8 nodes are IDS nodes that continuously monitors the nodes and reports the malicious activities in the network if exists any. The number of nodes monitored by each IDS node depends on the application of the system. In our system each IDS node monitors 6 nodes that is it looks like a cluster with 7 nodes. IDS provides authentication to the system by using public key cryptosystem. There exists a key-server in the system which distributes the public key to all the nodes in the system which is a randomly generated number. The IDS node distributes the ID-based key to its neighboring nodes which is obtained by using a random function. The nodes after receiving the ID-based key it shows its acceptance by sending an acknowledgment message signed (attested) by itself. Each node after receiving the message it signs with its own key so that a malicious node cannot falsely claim to be sender of the message. The IDS keeps on monitoring the network and eliminates the attacker if any exist in the network by verifying with the attestation key. When IDS receives any request packet from any node, it calculates the shortest path between the sender and destination and it checks i)the attestation of packet i.e. source and destination address and signature chain and ii) is the node logically closer to the destination than the previous node in the chain. This way IDS can enforce the forward progress of a packet, then IDS transmits the next closest hop IP address and port number in the shortest path to the requested node if the attestation were valid otherwise it discards the packet at the node itself to mitigate the vampire attacks.

V. Result Analysis

This section describes the comparative performance of proposed approach and existing approach. Performance of comparative study is evaluated in terms of Consumed Energy, Packet Delivery Ratio, Throughput, and Routing Overhead.

a- Comparative Consumed Energy

Ad-hoc nodes contain fixed amount of initial energy, the measurement of energy shows how long a network device in live in network. Figure 3 shows comparatively estimated consumed energy for attack, existing approach and proposed approach. Blue line show the energy consumption during attack, the red line shows the energy consumption during the proposed approach and the green line shows the energy consumption of existing approach.
Fig 1: Comparative Consumed Energy

Above Fig 1 shows the fraction of consumed energy by Y axis in term of joule and X axis shows the nodes in the network during the simulation scenario. Simulation performed for attack, existing approach and proposed approach considering 20, 30, 40, 70 and 100 nodes. The energy of network is consumed 0.65, 0.3 and 0.23 joule when 20 nodes are considered with respect to attack, existing approach and proposed approach. Similarly energy consumption is 0.8, 0.37 and 0.33 joule when nodes are 30, energy consumption is 0.85, 0.43 and 0.4 joule when nodes are 40, energy consumption is 0.95, 0.64 and 0.58 joule when nodes are 70 and energy consumption is 1, 1 and 0.91 joule when nodes are 100 with respect to attack, existing approach and proposed approach. According to the obtained results the amount of energy consumption is less of proposed approach compare to existing approach and attack.

b- Comparative Packet Delivery Ratio

Number of packet sent by a source device and successfully received packets ratio is responsible for Packet Delivery Ratio. Fig 2 shows comparatively estimated Packet Delivery Ratio for attack, existing approach and proposed approach. Blue line shows the packet delivery ratio during attack, green line shows packet delivery ratio during existing approach and red line shows packet delivery ratio during proposed approach.

Fig 2: Comparative Packet Delivery Ratio

Above Fig 2 shows the packet delivery ratio by Y axis in term of percentage and X axis demonstrates the nodes in the network during the simulation scenario. Simulation performed for attack, existing approach and proposed approach considering 20, 30, 40, 70 and 100 nodes. The packet delivery ratio of network is 59, 72 and 80 percentages when 20 nodes are considered with respect to attack, existing approach and proposed approach. Similarly packet delivery ratio is 57, 63 and 78 percentage when nodes are 30, packet delivery ratio is 53, 65 and 74 percentage when nodes are 40, packet delivery ratio is 43, 59 and 69 percentage when nodes are 70 and packet delivery ratio is 42, 46 and 58 percentage when nodes are 100 with respect to attack, existing approach and proposed approach. According to the obtained results the amount of packet delivery ratio is more of proposed approach compare to existing approach and attack.

c- Comparative Throughput

Network throughput is the average data rate of successful data or message delivery over a communication link. Fig 3 shows comparatively estimated throughput for attack, existing approach and proposed approach. Blue line shows throughput for attack, red line shows throughput for existing approach and green line shows throughput for proposed approach.
Fig 3: Comparative Throughput

Above Fig 3 show the throughput by Y axis in term of percentage and X axis demonstrates the nodes in the network during the simulation scenario. Simulation performed for attack, existing approach and proposed approach considering 20, 30, 40, 70 and 100 nodes. The throughput of network is 2.8, 5.9 and 6.8 packets per second when 20 nodes are considered with respect to attack, existing approach and proposed approach. Similarly throughput is 2.7, 5.7 and 6.4 packets per second when nodes are 30, throughput is 2.5, 5.6 and 6.3 packets per second when nodes are 40, throughput is 2.6, 4.8 and 5.8 packets per second when nodes are 70 and throughput is 1.9, 3.8 and 5.3 packets per second when nodes are 100 with respect to attack, existing approach and proposed approach.

The number of packets flow in network increases therefore, the available bandwidth is reduces as the nodes increases in network. Proposed approach limits the amount of control message exchange during establishing connection between source and destination in comparison of existing approach. According to the obtained results throughput is more of proposed approach compare to existing approach and attack.

d- Comparative Routing Overhead

The amount of additional data injected in to network is known as routing overhead. Figure 4 shows comparatively estimated routing overhead for attack, existing approach and proposed approach. According to the obtained results the blue line shows the higher routing overhead which simulate the performance under attack and green line shows the routing overhead of existing approach. Red line shows the low routing overhead which is performance of proposed technique.

Fig 4: Comparative Routing Overhead

Above Fig 4 show the routing overhead by Y axis and X axis demonstrates the nodes in the network during the simulation scenario. Simulation performed for attack, existing approach and proposed approach considering 20, 30, 40, 70 and 100 nodes. The routing overhead of network is 200, 130 and 60 packets when 20 nodes are considered with respect to attack, existing approach and proposed approach. Similarly routing overhead is 230, 180 and 150 packets when nodes are 30, routing overhead is 270, 230 and 170 packets when nodes are 40, routing overhead is 380, 250 and 180 packets when nodes are 70 and routing overhead is 430, 280 and 220 packets when nodes are 100 with respect to attack, existing approach and proposed approach. According to the obtained results routing overhead is less of proposed approach compare to existing approach and attack.

VI. Conclusion

Vampire attacks has been defined as a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes’ battery power. Defenses against some of the forwarding-phase attacks has been proposed and PLGP-a, the first sensor network routing protocol that reduces the damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. The routing protocol has been used at the time of routing to make efficient energy utilization during the packet forwarding phase.

References


Authors:

Durga Venkatesh is presently pursuing M.Tech (CSE) department of computer science engineering from Baba Institute of Technology and Sciences, Visakhapatnam.

B S Venkata Reddy M.Tech, MBA, Ph.D. is working as an Associate Professor in the Department of Computer Science and Engineering in Baba Institute of Technology and Sciences.