Vampire Attack Mitigation in Wireless Sensor Networks: A Survey

Bhavesh Dhake and Amit Nerurkar

Department of Computer Science, Vidyalankar Institute of Technology, Mumbai, India
{bhavesh.dhake, amit.nerurkar}@vit.edu.in

Abstract. Energy is critical for intermediate sensor nodes in a Wireless Sensor Network (WSN). Security in WSN is a tough problem due to the ad hoc structure of nodes in a network. A vampire attack, a new type of attack, disables a network by depleting the battery life of sensor nodes in the network. Vampire assaults are really not protocol-specific, but instead, leverage the characteristics of several commonly used routing protocols. These assaults do not operate on deluging the network with vast amounts of data, but also about transmitting the least amount of data as effectively in order to achieve the greatest energy drain and hence prevent a rate binding solution from being implemented. Because Vampire Attacks exploit protocol-adaptable communications, they are difficult to detect and avoid. It contains the Stretch and Carousel attacks, which harm nodes and can potentially bring the entire system down by consuming the battery power. It is tough to locate vampire assaults in the network. It is really difficult to spot, and it is disastrous. A simple network vampire can raise network-wide energy usage.

Keywords: Vampire Attack, WSN, DOS, Issues, Mitigations

1 Introduction

1.1 Wireless Sensor Networks

A sensor network is made up of a huge number of sensor nodes that are spread out across a vast territory and feature extremely low powered sensor nodes. Wireless Sensor Networks have several uses in information and telecommunications. Sensor nodes are incredibly tiny devices that can gather and broadcast information about sound, light, motion, temperature, and other perceived data to other nodes using wireless communication. Wireless Sensor Networks use short-range broadcast communication with multi-hop routing, as well as dense deployment and sensor node cooperation. They also change topology on a frequent basis due to fading and node failures, and their energy storage, computing power, memory, and transmission power are severely constrained.

WSNs are becoming more critical to daily operations of people and organisations, and flaws in availability are becoming less tolerable - unavailability can mean the difference between business and productivity loss, power outcomes, environmental crises, and innocent lives; thereby, high network accessibility is a significant feature that should retain even in severe environments. Sensor nodes are useful for continuous

stable sensing, event detection, area sensing, and actuator local control [5]. The wireless design and micro-sensing capability of the sensor network open up a variety of new application areas. Wireless Sensor Networks have the potential to be very useful in military communications, computation, reconnaissance, monitoring, and guidance systems. Environmental phenomena have a variety of uses, including tracking the migrations of animals, birds, and insects, identifying forest fires, mapping the biocomplexity of the environment, and detecting floods. Some sensor network health applications include providing interfaces for debilitated, homogenized patient monitoring, administration of drugs in hospitals, and tracking strength of the material, as well as constructing virtual keyboards, inventory control, supervising product quality, and establishing smart office spaces. There is a seemingly limitless range of applications for Wireless Sensor Networks, limited only by the human imagination. Because of their ad-hoc nature, wireless ad-hoc networks are extremely resistant to Denial of Service (DoS) assaults. While these schemes address assaults on network availability in the near term, they do not address attacks on network availability in the long run. The most inevitable denial of service assault is complete control of node batteries. This is a resource depletion assault in which battery power is the target resource.

1.2 WSN Routing Protocols

Because of the multiple variables that distinguish sensor networks from traditional communication and wireless ad-hoc networks, routing in sensor networks is extremely difficult. To begin with, it is impossible to create a universal addressing system for the deployment of a huge number of sensor nodes. As a result, sensor networks are incompatible with typical IP-based protocols. Second, unlike traditional communication networks, practically all sensor network applications need the flow of sensed data from several sources to a single sink. Third, because several sensors may offer the same data in the vicinity of an event, produced data traffic has a high degree of redundancy. Such redundancy must be used by routing systems to improve energy and bandwidth utilisation. Finally, because sensor nodes have limited transmit power, on-board energy, processing capabilities, and storage, careful resource management is required. As a result of these variances, a slew of novel solutions to the problem of data routing in sensor networks have been proposed. These routing strategies take sensor node properties, as well as application and architectural needs, into consideration.

Flat-based routing, hierarchical routing, and location-based routing are three types of routing protocols in WSNs based on network structure [5]. In flat-based routing, all nodes in the network have similar functionality and play equal responsibilities, but in hierarchical-based routing, each node is assigned different functions. Sensor node positions are utilised to route data in the network in the case of location-based routing. If some network parameters may be modified to accommodate the present network condition and energy capability of network nodes, a routing protocol is said to be adaptable. Furthermore, such protocols may be classified depending on how they work, with query-oriented, multipath-oriented, negotiation-based, and QoS-based routing techniques being the most common. Reactive, proactive, and hybrid routing are all ways to categorize protocols depending on the route discovery process from source to

destination. The route in reactive routing is discovered on demand, that is, immediately before the message is delivered, whereas the route in proactive routing is determined ahead of time, regardless of when the message is sent. Hybrid procedures combine these two approaches. Table-driven routing approaches are recommended over reactive protocols for static nodes. The process of route discovery and path building in reactive protocols consumes some energy. Cooperative routing protocol is a new form of routing protocol that has been identified. There is one central node in cooperative routing where all data from all nodes in the network is pooled and processed, minimising route costs in terms of energy usage. Many alternative methods rely on location and time data.

1.3 WSN-Related Problems

Design Issues. A number of challenges occur during the design of a WSN. The first is Fault-Tolerant Communication, in which sensor nodes regularly get damaged and inefficient due to deployments in an uncontrolled or dangerous environment. Then there is Low Latency, in which the actions handled by the structure are critical and must be detected by the operative as quickly as feasible. As a result, incidents must be detected and reported as quickly as feasible by the platform. Third, scalability, where the number of sensor nodes scattered throughout the sensing zone might be in the hundreds, thousands, or even millions. It is difficult to construct a large-scale Wireless Sensor Network and work efficiently with a big number of nodes. Followed by Node Heterogeneity - It is more difficult to establish a sensor network with heterogeneous nodes than with homogeneous nodes. And finally followed by Transmission Media and Coverage problems which shows the level of service that a given sensor network can deliver [4].

Topology Issues. Geographic Routing, a theory that relies on geographic position information, is one of the difficulties. It is primarily meant for wireless networks and is based on the assumption that the origin sends a transmission to the destination geographic location rather than the network address. The following are some examples: Sensor Holes - A routing hole in a sensor network is a position in which nodes are either inaccessible or otherwise unable to engage in real-time data routing for a plethora of reasons. Detecting holes is particularly difficult since old Wireless Sensor Networks are made up of ultralight, minimal nodes that have no idea where they are. Finally, the Coverage Topology - Coverage issue displays how well sensors monitor or track an area. In recent years, the research community has focused on sensor network coverage and connection issues. This problem may be represented as a decision problem, with the goal of deciding whether every site in the sensor network service area has at least k sensors, where k is a given value.

2 Background Theory

2.1 WSN Security Issues

Security has become the most critical consideration in the design and execution of a network. Security in a sensor network is extremely difficult since the performance of a WSN is dependent on its security. The essential security factors required to construct a secure Wireless Sensor Network are as follows.

Data Integrity. The significance of data integrity in mitigating loss of data or leakage cannot be exaggerated: in order to protect your data from hostile external influences, you should first assure that insiders are efficiently managing it. Organizations can guarantee that private content is never falsely labeled or kept wrongly by having robust data validation and error control, thereby exposing you to danger. This may have major implications for the integrity of information in various applications, such as healthcare monitoring and traffic analysis, among others.

Authentication of Data. It is the process of verifying the origin and integrity of data, and it is commonly associated with communication, messaging, and integration. It consists of two parts: authenticating that you are receiving data from the proper source and confirming the data integrity. Any data delivered via a fully verified and protected connection is regarded as genuine. Confirming data integrity at the same time is also a recommended practice. In sensor networks, every sensor node and access point must verify that the information captured was sent by the originator and not by an illegal authority that has consented to accept fraudulent data from normal nodes. In sensor networks, information security from unauthorized parties is critical to preventing unlawful access to information. Otherwise, the conversation may be eavesdropped on.

Data Freshness. Given that all sensor networks transmit some type of time-varying measurement, ensuring secrecy and authentication is not enough; we must also verify that each message is fresh. Colloquially, data freshness showed that the data distribution is current and that no attacker has repeated previous messages. We differentiate between two types of freshness: weak freshness, which offers limited message ordering but no delayed information, and strong freshness, which gives a detailed order on a request-response pair as well as delay prediction. Sensor measurements necessitate low freshness, yet high freshness is advantageous for network time synchronization. One type of network layer assault is a replay attack, in which the adversary seizes packets and sends them later to confuse the network. So, while constructing a WSN, it is vital to retain data freshness, which implies that recent data should not be sent again by nodes, or in other words, data should not be resent in the network.

Data Availability. Data availability refers to the timeliness and dependability of data access and utilization. It consists of data accessibility. The availability of information

refers to its accessibility and continuity. Information with minimal availability issues may be regarded as supplemental rather than essential. Information with high availability concerns is regarded as vital and must be accessible in order to avoid harmful consequences. It ensures that network services are always available, even in the event of a Denial-of-Service attack.

2.2 Vampire Attack

A Vampire Attack is a type of Denial-of-Service attack, in which the rogue node forms and sends messages, causing additional energy to be used. It depletes resources at each sensor node by depleting each node battery lifetime. This does not have an immediate impact on network accessibility; rather, they generate a message with little data and a significant energy depletion. This operates slowly over time, degrading network operations by draining node battery power. It sends out little complaint messages in order to deactivate entire network, making it challenging to detect and prevent. Vampire assaults aren't protocol-specific in the sense that they really do not depend on particular routing protocol design or construction flaws, but rather on basic properties of protocol classes including link-state, distance vector source routing, geographic routing, and beacon routing. These assaults do not concentrate on overloading the network with massive amounts of data, but instead on delivering as little information as necessary to cause the greatest energy depletion, impeding a yield-limiting approach. Vampire Attacks are difficult to recognise and avoid because they employ protocol-compliant communications.

The first difficulty in dealing with Vampire Attacks is recognising which behaviours encompasses an assault. DoS assaults on wired networks are frequently characterised by amplification: a malicious actor might, for example, increase the resources used on the assault by using 60 seconds of its own CPU time to cause the victim to invest 600 seconds. In any multi-hop network, consider the following routing strategy for a packet: An origin composes and broadcasts the message to another hop closer to the destination, which then transmits it further until it reaches the target, utilising capabilities not just at the origin node but also at each node through which the message passes [3]. Given that an attacker may construct and send messages that are evaluated by every node along the message channel, amplification attacks are always conceivable when considering the total energy of the network. As a result, sending is an act of amplification that leads to resource burnout as long as the entire cost of forwarding a signal is less than the cost of composing and transmitting it to the source. As a consequence, amplification as a measure of maliciousness must be abandoned in favour of the total amount of energy spent by a compromised node while transmitting the similar number of messages as a genuine node.

A Vampire assault is defined as the generation and delivery of a signal that uses more transmission power than if a genuine node delivered the same size message to the same target destination but with modified packet headers. The ratio of network energy used in the relatively harmless case to network energy used in the malevolent case is used to assess the strength of the attack, i.e., the proportion of network-wide power usage with malevolent nodes involved to energy usage with only genuine nodes when

the size and number of packets sent remain constant. Due to the lack of Vampire Attacks, this ratio is one. Carousel attacks and stretch attacks are two sorts of Vampire Attacks on Stateless protocols.

Carousel Attacks. In this assault, a packet is sent by a malicious user with a path that involves a series of loops, such that the very same node appears numerous times in the route. It increases the length of the route beyond the node count of the network, which is constrained by the amount of valid items in the source route. This approach might be used to extend the length of the route beyond the number of network nodes, with just the permissible entries in the origin route limiting it. Try to be aware of the huge increase in energy use along the initial trip. Considering that the attacker limits the transmission rate in order to avoid overloading the network, the conceptual limit of this attack is an increase in energy usage factor of O(n), where n is the longest route distance. Whole energy consumption increases by up to 3.96 times each message. The increase in standard deviation is explained by the fact that the invasion often does not increase power consumption — the size of the hostile path is a multiple of the genuine path, which is influenced by the role of the malicious user in comparison to the target destination, so the location of the malicious user is critical to the success of this invasion.

Stretch Attacks. A malicious actor creates arbitrarily long routes, potentially traversing almost each and every node in the network; this is known as the Stretch Attack because it lengthens packet paths, causing packets to be handled by a number of nodes regardless of the number of hops along the shortest route between the adversary and packet goal. Stretch Attacks, depending on where the rogue node is placed, can raise energy use by an absolute scale or more. Combining several assaults, increasing the number of hostile nodes in the network, or just delivering more packets can all help to increase their efficacy. The potential limit of a stretch assault is a packet that passes through each and every network node, resulting in an increase in energy usage of factor O(min(X, n)), where X is the number of network nodes and n is the maximum path length allowed. Because of the hop count, each packet that may go is limited by the number of network nodes, this attack may do less destruction per packet than the carousel attack. Adversaries, on the other hand, can combine both carousel and stretch attacks to retain the packet in the network for a longer period of time: the resulting stretched cycle may be traversed again in a loop.

Vampire Attacks have the following effect on stateful protocols, such as AODV [8]. In the case of stateful routing, routes are identified on–demand rather than pre-discovered as in source routing, making vampire less effective; yet, vampire can waste network node energy by resuming packets in some parts of the network. The attacker node utilises directional antenna assault to redirect routes, causing network nodes to consume energy. Fake route discovery requests are another form of assaults that results in affecting both types of routing. Because discovery of the route necessitates the transmission of route request and response packets, hostile nodes can initiate route discovery

procedures at any time, resulting in packet deluge. This type of attack is also feasible with AODV and DSR.

3 Related Work

3.1 Literature Survey

The many sorts of Vampire assaults guarantee that the batteries of the nodes are depleted quickly and that they do not enter the low power sleep state. This type of power fatigue is known as "sleep deprivation torture." These assaults keep nodes from entering a power-reduced sleep cycle, causing their batteries to deplete faster. In the most recent study on "denial of sleep," only assaults at the medium access control (MAC) layer are considered. There is also discussion of source depletion at the MAC and transport layers, although suggested remedies include rate restriction and removing internal invaders. Despite a brief discussion of malevolent cycles (routing loops), no practical mitigation other than higher MAC efficiency and protocols directed away from source routing is described.

Other studies on Denial-of-Service in ad-hoc wireless networks have focused on adversaries that obstruct route development, disrupt communication, or deliberately establish routes via themselves in order to drop, manipulate, or observe packets. The impact of service disruptions or degradation on battery life and other discrete node assets has not been traditionally seen as a security concern. Protocols that describe security in terms of route discovery efficiency, guaranteeing that only legitimate network pathways are discovered, cannot guard against Vampire Attacks since Vampires do not utilise or return unlawful routes, nor can they hinder communication in the near term.

Vampire Attacks, as defined by Eugene Y. Vasserman [8], are attacks that drain network node energy and permanently disable wireless networks. In the worst-case scenario, a single Vampire can increase network-wide energy consumption by O (N), where N is the number of network nodes. The author addresses countermeasures for these types of assaults, including an unique concrete evidence protocol that limits the damage caused by Vampires during the packet forwarding phase. They built a rogue node and plotted a random topology of 30 nodes to demonstrate how sensitive this attack is to various routing methods. Work involved researching numerous vampire attack strategies for various protocols. The solution given in this study is PLGPa, which has been proved to be the first solution against vampire assaults in packet forwarding phase for network communications.

P. Rajipriyadharshini [7] describes a solution for vampire assaults as a Wireless Sensor Network, which is a communication network between sensor nodes. When selecting sensor nodes, the most significant aspect is energy. Wireless Sensor Networks necessitate an energy-saving solution. As a result, there is a significant amount of energy lost. To prevent this vampire attack, a new protocol called PLGP, a useful and secure protocol, is suggested together with the key management protocol called Elliptic Diffie-Hellman key exchange protocol.

B. Umakanth presented an EWMA (Energy Weight Monitoring Algorithm) solution for dealing with the consequences of these vampire-type attacks during the packet forwarding phase [12]. When energy of node hits a specific threshold, it becomes critical in the fight against DOS assaults. This approach is dependent on the sensors' energy levels. This procedure is divided into two stages: network configuration and communication. In the previous stage, the best routing path from origin to destination in the network was discovered. During this phase, the emphasis is mostly on balancing the load on the nodes and minimising energy usage for data transfer and resource sharing. The primary goal of the communication phase is to prevent repeatedly transmitting packets through the same node, which depletes batteries and causes network failure due to Vampire Attacks. Redundancy is reduced by aggregating data packets within the forwarding node and transferring the leftover packet through the shortest path to the destination. Aggregation is the act of copying and comparing the content of a packet to the data packet; if the copied and transmitted packets are identical, the node stops delivering the data packet.

V. Subha introduced Hybrid Key Management, a method that brings a novel authentication and key management technique [6]. It is both resilient and scalable in the face of constrained memory resources. It uses Low Power Routing to give robust security. Diffie-Hellman Elliptic Curve it is less heavyweight than standard Diffie-Hellman This method comprises establishing a group key for authentication and connecting the network. The load of key management is reduced by employing a distributed design. Second, during data transfer, this technique employs the Modified RSA algorithm for encryption and decryption. This approach, in particular, may be developed to a hybrid structure to increase network scalability. As a result, the enhanced method is fault-tolerant and effective in terms of network integrity and secrecy.

This research shows and analyzes various prevention and detection methodologies proposed against Vampire Attacks which are currently in use for WSNs.

4 Proposed Mitigations

Here we discuss some of the solutions that have been proposed and are in use in the industries for detection as well as prevention of Vampire Attacks in a WSN.

4.1 Energy variance discrepancy between network nodes

The action of a vampire intruder, which consumes network energy by overflowing packets and RREQs, causing the node of the vampire broadcast rate to be greater and its energy to be higher than those of other network nodes. This research is based on the difference in variance of network node energy at various times.

Initially, a catalog of suspicious nodes is generated based on transmission and energy values larger than their corresponding variances. Suspicious nodes are temporarily suspended from the network, and their energy use is examined. If the rate of energy consumption drops, the suspicious node transforms into a vampire node and is eliminated.

Using the suggested approach, we first compute the variance of broadcast of all network nodes at time t1 using the formula

$$V_{Bt1} = \frac{1}{n} \sum_{i=1}^{n} (B_i - \mu)^2$$

Then, gather a group of nodes that have broadcast more than VBt1. The variation of energy levels of all nodes at the same time t1 is then calculated using the formula

$$V_{Et1} = \frac{1}{n} \sum_{i=1}^{n} (E_i - \mu)^2$$

Prepare a similar collection of nodes with higher energy than VEt1. At time t2, the energy variance is determined in the same way, and we then identify the set of suspicious nodes in the network at times t1 and t2. Furthermore, we compute the difference between times t1, t2, and t3 in order to discover rogue nodes in the network and remove them from time t3 [5].

This technology is intended to offer dynamic detection and eradication of Vampire Attacks from WSNs, as well as work in WSN dynamic topology modification. This approach detects vampire attackers based on packet broadcast rate and energy metrics shared by network nodes.

4.2 Threshold concept for estimating trustworthy nodes

The threshold idea is used for trusted node estimate during route discovery stages to deliver solutions. Furthermore, in network contexts, the nodes are movable. To establish the malicious connection, the vampire attack uses packet flooding and RREQ flooding. As a result of this, the target node floods the packets even more, draining its energy and network performance. When the assault is launched, the number of broadcasts in the network is tallied and a threshold value is set. This value is used to flag the node as suspicious.

$$threshold = \sum_{i=1}^{N} \frac{number\ of\ broadcast}{N}$$

The network is then sampled, and the nodes' broadcast values are evaluated to the estimated threshold value. After categorizing the nodes into two groups, the dubious nodes are removed from active communication and the normal network continues to operate. During this time, average packet delivery ratio of each node is estimated.

$$PDR_t = \sum_{i=1}^{N} \frac{PDR}{N}$$

According to this suggested vampire attack solution, when Vampire Attacks are launched on the network, the performance of the network in terms of packet delivery ratio decreases while the number of broad casts increases [4]. The thresholding idea is used for trusted node estimate during route discovery stages to propose a solution. Furthermore, in network contexts, the nodes are movable. To establish the malicious connection, the vampire attack uses packet flooding and RREQ flooding. As a result of this, the target node floods the packets even more, draining its energy and network

performance. As a result, when the assault is launched, the number of broadcasts in the network is tallied and a threshold value is set. This value is used to flag the node as suspicious.

4.3 Using Routing Loops for Early Detection and Avoidance

In a conceptual network address space, a packet is considered fulfilled if it makes consistent progress toward its destination. No-backtracking is achieved if each packet goes across the same number of nodes regardless of whether an intrusion is present or not in the network. Nodes maintain track of the cost required by the route. The lack of retracing does not imply vampire resistance. The no-backtracking criterion is not satisfied by PLGP: Packets in PLGP are transmitted via the shortest path, which is the tree permitted by the physical topology. A good piece of advise given through this research is to employ PLGP with attestations (PLGPa).

Each PLGP packet must contain a route history that can be verified. PLGPa employs this packet background in conjunction with the PLGP tree routing structure to allow each node to securely certify progress while preventing any major hostile effect on the course taken by each packet that goes through at least one genuine node. Such signatures form a chain that is connected to each packet, allowing each node that receives it to confirm the journey of the packet. Each transmitting node examines the authentication chain to ensure that the packet did not leave its intended target destination in a conceptual address space.

There is no backtracking with PLGPa. The originator signs each communication. An attacker that can only alter packet fields that are updated while going over the route can only modify, shorten, or eliminate the path attestation field. A one-way signature chain is used to avoid truncation. PLGPa never overflows and has a low overhead while transmitting packets. It has a greater diversity of routes and a more even distribution of routing burden. Even on 8-bit processors, the cryptographic computation necessary for PLGPa is not untractable in the absence of hardware [3].

This approach defends against specific transmission phase assaults and explains PLGPa by guaranteeing that packets always go in the direction of their target destinations, hence minimising the harm caused by Vampire Attacks.

4.4 Making use of Distance Vector Protocols

Ad Hoc On Demand Distance Vector Routing Protocol. The AODV protocol is a kind of Distance Vector Routing Protocol (DV). Every node in a DV is aware of its neighbours and the costs of accessing them. Each node does have its own routing table, which maintains all of the nodes in the network, their distance from one another, and the next hops among them. If a node is unable to be reached, the distance between it and the nearest node is set to infinity. On a regular basis, each node broadcasts its whole routing table to its neighbours. As a consequence, they may assess if a feasible route to some other node that utilises this neighbour as the next hop exists. If a connection fails, a Count-To-Infinity may occur [16].

One of the most significant features of AODV is its integrated multicast routing. A multicast routing table stores the IP address of the group and sequence number. The IP address of the leader and hop count are also recorded, as is the following hop in the multicasting tree and its duration. To join a multicast group, a node must send an RREQ towards the group address with the connect flag set. An RREP can be sent by any node in the multicast tree that receives an RREQ. As a result, a recipient may receive a large number of RREPs, from which the recipient can choose the one with the smallest route to the group. A MACT (Multicast Activation Message) is delivered to the designated tree node to activate this branch.

According to one research, a homogeneous network with 10 and 20 nodes was established and tested to verify the scalability and durability of the network [9]. They sent 100, 1000, 10000, and so on packets to measure battery usage, with intervals ranging from 1 second to 100 milliseconds for each scenario. In this type of attack, a different method was used to install Vampire Attack on an inside compromised node. External Vampire Attacks are easily detected because to new node characteristics that decrease the attacking impact. To increase the effect of attacker, the adversary seeks to carry out a vampire attack by corrupting a trusted node that can be installed in line with the default routing protocol of the network. In Qualnet Simulator, a different routing protocol called VampireAODV was implemented, and the influence of interior vampire nodes on WSN was examined. After analysing the difference in battery usage by victim nodes under normal and Vampire Attack conditions, the mitigation method was incorporated in the AODV routing protocol. Following the installation of the recommended strategy, many parameters are monitored for performance monitoring under attack and mitigation.

Destination Sequenced Distance Vector. DSDV routing is one of the features of the ad-hoc network routing protocol. It is a preemptive protocol routing approach that is table-driven. Two types of routing algorithms are employed in this case: Algorithms for link-state and distance vector routing.

Link-state algorithm. Nodes in link-state protocols, such as OLSR, keep track of whether network links are up or down and send out flood routing modifications when a link goes down or a new link is activated. In this situation, every node maintains a view of the network architecture.

Distance vector routing algorithm. Distance vector protocols, such as DSDV, track the next jump to each destination, which is associated by a route cost metric, such as hop count. Under this technique, only routing updates that change the cost of a single route must be communicated.

The routing mechanism in this proposed approach mitigates the impact of Vampire Attacks by guaranteeing that packets continue to travel toward their destinations and minimising the reimbursement.

4.5 Using Elliptic Curve Diffie-Hellman Protocol

The ECDH key exchange is the elliptic curve equivalent of the standard Diffie-Hellman key exchange, and it may be used to create a shared private key between two different entities using an unprotected communication channel [6]. The ECDH method is used to authenticate and detect malicious nodes. Once the rogue node has been identified, information is sent to the target to avoid the carousel and stretch to conserve energy. The Elliptic Curve Diffie-Hellman Key Exchange Algorithm is used to accelerate the key verification procedure through sensor node cooperation. After registering and getting security certificates, a user requests broadcast services from its adjacent sensor nodes. The sensor nodes conduct mutual authentication, allowing only authenticated users to access the WSN. Before transferring the command/query to the sensor nodes, the user must sign it. A command or query is signed by the user and forwarded to the different sensor nodes.

Modified RSA Algorithm. This is a novel way for providing maximum security for data transmitted via a network. It entails encryption and decryption. A prime number is employed in a modified RSA cryptosystem to ensure network security. In this strategy, a "n" prime integer was employed that is not readily broken. n prime numbers are difficult to deconstruct. This approach increases network efficiency and dependability. To handle "n" prime integers and guarantee security, a modified RSA cryptosystem method is employed.

This approach entails creating a group key for authentication as well as connecting the network. The load of key management is decreased by employing a distributed design. Second, during data transfer, the technique employs the Modified RSA algorithm for encryption and decryption. The approach, in particular, may be extended to a hybrid design to improve scalability. As a result, the expanded method is fault tolerant as well as efficient in terms of integrity and secrecy. The simulation results demonstrate that the impact on the system was greatly decreased when the approach was implemented. The suggested approach routing protocol provably limits Vampire attack harm by ensuring that packets constantly advance toward their destinations and reduces compensation. The cryptographic primitives and key management used to provide network security against Vampire Attacks.

4.6 Detection using EWMA

EWMA operates in two stages:

Network Configuring Phase. The goal of this phase is to discover the optimum routing path in the network from origin to destination. The main issues are optimizing the node load and limiting energy consumption for data transport [12]. The node with maximum threshold energy (attacked node) emits the ENG WEG message to all nodes in its proximity during this phase. Following the reception of the ENG WEG packets, the

neighbouring nodes send the ENG REP message, which comprises information about their geographical position and present energy level. When a node receives this, it saves it in its routing table to make future computations easier.

The node then asserts the routing path by first tracing the next node by computing the energy needed to transmit the necessary data packet that is appropriate energy node and less faraway node chosen as the next forwarding node. In this manner, it creates the route from origin to destination with suitable energy and less faraway node.

As a result, the energy used by the allocated node is proportional to the data packet transmitted from the node, and this strategy prevents data packet losing, and the packets are securely delivered to the destination by the assigned forwarding node. This algorithm prioritizes achieving load balancing in the network. As long as this node can handle it, the suitable energy node will be assigned as a forwarding node. As a result, a multi-hop minimally remote path is built to limit network damage from Vampire Attacks.

Communication Phase. The primary goal of the communication phase is to avoid the similar data packets from being forwarded over the same node many times, which quickly depletes the batteries and results to network dying due to Vampire Attacks [12].

By aggregating data transmission inside the forwarding node and properly transmitting the remainder packets to the destination, the practise of repeated packets is avoided. Data aggregation is achieved by first reproducing the information of the existing packet being delivered by the node. This duplicated data is compared to the data packet passing through the node. If the sending packet and the received packet are identical, the node stops transmitting data packets across them. As a result, redundant packets are avoided from being transmitted over the same node again, and batteries are protected from rapidly depletion. Then, reliably deliver the needed data packets to the target via the established node.

By discarding packets in the network, EWMA prevents the entire network from collapsing. The load is spread equitably based on the capacities of the nodes. As a result, a multi-hop load balanced network is created.

5 Conclusion

This paper covers a research survey of WSN security breaches caused by Vampire Attacks for various stateless and state complete routing protocols, as well as several solutions for dealing with vampire assaults. Novel security approaches are devised and implemented based on newly established techniques for modelling the effect of attack deployment and performance improvement following security scheme implementation. Furthermore, in order to explain the solution and its improved performance, the conventional routing protocol is compared to the created routing protocol. Throughput, end-to-end latency, remaining energy, and packet delivery ratio are all important considerations. To conclude, we continue to find that these proposed mitigations provide

sufficient evidence for the detection of Vampire Attacks but are insufficient for the prevention of Vampire Attacks, and this remains an unresolved issue in this area.

References

1. Riddhi, M., Priyanka, B., Mayur, C., Pritesh, R.: Vampire Attacks: Detection and Prevention. IJSDR 2(4), pp. 216-222 (2017).
2. A. S. Nisha., V. Vaishali., T. Shivaranjani., P. Subathra.: The effect of Vampire Attacks on distance vector routing protocols for wireless ad hoc sensor networks. In: 2016 Second International Conference on Science Technology Engineering and Management (ICONSTEM), pp. 587-594, doi: 10.1109/ICONSTEM.2016.7560961 (2016).
3. L. R. Deshmukh., A. D. Potgantwar.: Ensuring an early recognition and avoidance of the Vampire Attacks in WSN using routing loops. In: 2015 IEEE International Advance Computing Conference (IACC), pp. 61-66, doi: 10.1109/IADCC.2015.7154669 (2015).
4. Deepmala, V., Gajendra, S., Kailash, P.: Detection of Vampire Attack in Wireless Sensor Networks. IJCSIT 6(4), pp. 3313-3317 (2015).
5. Soni Manish., Pahadiya Bharat.: Detection and Removal of Vampire Attack in Wireless Sensor Network. International Journal of Computer Applications. 126(7), pp. 46-50. 10.5120/ijca2015906101 (2015).
6. Subha, V., Selvi, P.: Defending against Vampire Attacks in Wireless Sensor Networks. International Journal of Computer Science and Mobile Computing 3(11), pp. 668-679 (2014) .
7. Rajipriyadharshin, P., Venkatakrishnan, V., Suganya, S., Masanam, A.: Vampire Attacks Deploying Resources in Wireless Sensor Networks. International Journal of Computer Science and Information Technologies 5(3), pp. 2951-2953 (2014).
8. E. Y. Vasserman., N. Hopper.: Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks. In: IEEE Transactions on Mobile Computing 12(2), pp. 318-332, doi: 10.1109/TMC.2011.274. (2013).
9. M. K. Sharma., B. K. Joshi.: Detection & prevention of vampire attack in wireless sensor networks. In: 2017 International Conference on Information, Communication, Instrumentation and Control (ICICIC), pp. 1-5, doi: 10.1109/ICOMICON.2017.8279174 (2017).
10. A. A. Patel., S. J. Soni.: A Novel Proposal for Defending against Vampire Attack in WSN. In: 2015 Fifth International Conference on Communication Systems and Network Technologies, pp. 624-627, doi: 10.1109/CSNT.2015.94 (2015).
11. Vijayanand, G., Muralidharan, R.: Overcome Vampire Attack problem in wireless ad-hoc sensor network by using distance vector protocols. International Journal of Computer Science and Mobile Applications 2(1), pp. 115-120 (2014).
12. Umakanth, B., Damodhar, J.: Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks. International Journal of Engineering Trends and Technology 4(8), pp. 3691-3695 (2013).