International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

ANALYTICAL STUDY ON SECURITY AND ATTACKS CONCERNING WORMHOLE DETECTION IN STATIC WIRELESS SENSOR NETWORKS

Jagathese G Chelladurai
Research Scholar
Department of Computer Science, Mansarovar Global University Bhopal (M.P)
Dr. Mona Dwivedi
Research Guide
Department of Computer Science, Mansarovar Global University Bhopal (M.P)

Abstract
Sensor nodes, when organized to build a WSN working below the switch of a central specialist, Improper position, are skilled of displaying fascinating applications due to their potential to be distributed widely in hostile and pervasive contexts. However, for the same reason, security is now a top concern for these networks. WSNs are susceptible to a variety of internal and external attacks due to their lack of tamper-proof packaging, limited processing power, memory capacity, and battery life. Because of their widespread use, WSNs are particularly susceptible to a variety of security risks. A denial-of-service attack is the most frequent and dangerous enemy to WSNs (DOS). Wormhole assault is another one of the several attack strategies. In order to achieve optimal network performance, a static clustering approach is suggested in this research. To assist in determining the initial energy allocation of these cluster heads and nodes, an energy model of this technique is offered. Finally, a simulation is shown to demonstrate how energy allocation is made to significantly lengthen network lifespan.

Keywords: Security, Security Requirements, WSNs, Wormhole Attack, Malicious Node Detection.

INTRODUCTION

WSNs, which be there a component of MANET, are made up of several tiny sensor nodes that are constantly monitoring environmental factors. To increase network scalability and coverage, sensor nodes carry out important responsibilities such signal meting out, computation, and network self-formation. Together, the sensors paint a more complete image of the environment

than the individual sensors could [1]. They are also in charge of information transport and environmental sensing. Usually, the transmission process is challenging since there are few sensors and a lot of data to transmit. The network is susceptible to many assaults because of the limited number of sensor devices. Due to their complexity and constrained node count, WSNs do not lend themselves to conventional security approaches. Furthermore, these precautions don't rule out the prospect of further assaults. WSNs are useful in many important industries, including the military, healthcare, security, and the environment. A WSN, for instance, keeps track on many activities during a military operation [2].

Background

A WSN is made up of these collaborating sensor nodes. Despite becoming competitive in a number of industries, WSNs have challenges such as communication, transmission, memory, and energy resource constraints, which are partly caused by their small batteries, as anticipated by WSN forecasting. Although forecasts for the near future vary, all businesses agree that there will be a greater need for WSNs in the long run (red line). These predictions show how valuable WSNs are, and we can see how technology based on WSNs may have a big impact on our world. WSNs are a part of MANET and are made up of several small sensor nodes that continually track environmental factors. In order to promote network autonomy, signal processing, computation, and other critical tasks are carried out by sensor nodes. [5]. Greater detail is offered by the sensors' global environment scenario than by individual sensors operating in isolation. They are also responsible for gathering and disseminating data pertaining to the climate [6].

A wireless network is one that connects network nodes via wireless data links. we fewer Ad-hoc networks and infrastructure-based networks are the two categories into which networks fall. Every user must utilize access points or base stations to communicate in an infrastructure-based network, but in an ad-hoc network, nodes establish and maintain intercommunication connections on their own, independent of any pre-existing infrastructure. Because the network's infrastructure is lacking in Laci, there are no central organizations. Ad hoc network security is challenging due to unpredictable network structure and unstable connectivity between nodes. Wireless networks are more vulnerable to intrusion and interference assaults,

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

as well as eavesdropping. A huge number of small sensor nodes make up the WSN, which is a component of MANET and continually analyzes the surroundings. The network's self-configuration, signal processing, and other operations that sensor nodes carry out assist to increase network coverage and boost scalability. Tens to thousands of Sensor Nodes dispersed over a large region make up a WSN. Each Sensor Node (SN) is made up of four fundamental components: a detecting unit, a processor unit, a transceiver unit, and a power unit. These small sensors can perceive, process data, and communicate with one another using radio frequency channels. They also feature other, optional, application-specific parts like a mobilize, a power generator, and a location-finding system. Sensors and Analog Digital Converters are the two components that make up the Sensing unit (ADCs). With the aid of the ADC, analog signals are transformed into digital signals before entering the processing unit. The processing unit controls the operation that enables the SN to cooperate with one another to do the specified **task, and it is connected to a tiny storage unit tasks.**

Motivation

The transmission role is often significant since data and sensors are typically scarce. The network is susceptible to a number of assaults because of the small sensor devices. WSNs' typically enormous size and small node count preclude the adoption of conventional security techniques. Usually, such remedies do not entirely exclude the possibility of further assaults. WSNs are critical in many important fields, including, among others, industry, the military, healthcare, and defence. A WSN, for instance, keeps an eye on various military operations. These sensor nodes communicate with other nodes to convey information to the base station (referred to as the sink) whenever an event is noticed [7]. To gather information from WSNs, basic positions are frequently utilized. They often have more possessions than conventional sensor nodes, which have comparable limitations (such as processing power and energy). Aggregation points aggregate the data they receive from adjacent sensor nodes, distribute it to base stations for additional processing, or send it to a processing center [8]. This makes it possible for WSNs to store energy, hence prolonging the life of the network. Safekeeping is one of the key aspects of WSN systems that deserves careful attention given the variety of

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

potential applications. This article provides a comprehensive summary of current methods for identifying network layer wormhole attacks while taking security constraints into account.

Sensors that track and document the physical aspects of their surroundings and transmit information to a central location are referred to as WSNs. WSNs may keep an eye on environmental factors including humidity, wind, and noise levels as well as temperature [9]. Wireless sensor data transmission relies on wireless networking and ad hoc network development, much as wireless ad hoc networks. WSNs keep track of physical or environmental variables like pressure, sound, and temperature. Modern networks collect data and regulate sensor activity in both directions. These networks were developed in response to military uses like battle surveillance. Such networks are used for consumer and commercial applications, including machinery health monitoring and control as well as process monitoring and management [10].

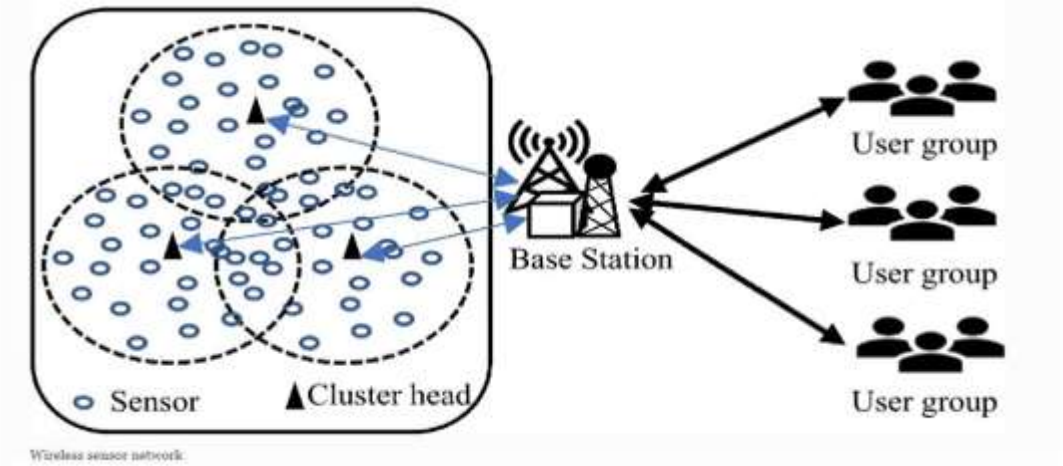

Figure 1.1 A comprehensive study on key management, authentication and trust management techniques in WSNs

A WSN is made up of "nodes" that can number anywhere from a few to thousands and are each connected to additional sensors. Each node normally consists of a variety of parts, such as a radio transceiver with an internal antenna, an external antenna link, a microprocessor, an electrical circuit, a power source, a battery, or a built-in energy collection device [11]. Shoebox-sized sensor nodes are possible, although minute measurements must still be taken. The cost of the sensor node varies from a few to one hundred dollars depending on how

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

sophisticated the node is. The resources capacity, memory, processing speed, and bandwidth are constrained by size and cost considerations. The design of a WSN might be anything from a complex multi-hop wireless mesh network to a simple star network. Routing or flooding can be used for propagation. There are several kinds of sensor networks available for use in medicine, including implantable, wearable, and integrated sensor networks. Medical implants are placed inside the human body. Wearable technology is used on or close to a person [12]. Environmental sensors are used by systems that incorporate the environment. In this type of network processing, the base station is supposed to be secure and to have unlimited energy whereas the sensor nodes are assumed to be insecure and to have limited energy. The current security issues for WSNs are complicated by aggregation, which calls for the creation of novel, scenario-specific security methods. The first few papers addressing approaches for secure data aggregation in wireless sensor networks offered data aggregation protection [13].

1.2 Experiments of Sensor Networks

A WSN is a specialized system with a few restrictions as compared to a standard computer network. WSN security has attracted a lot of attention recently. Computer security is more challenging to implement due to the bulk of these systems' resource constraints. The several challenges are discussed below.

1.2.1 Wireless nature of communication

Wireless networks are exposed to a variety of malicious attacks because of the inherent [14] lack of security in these systems. These assaults may be passive or violent. Active attacks, in which the attacker modifies and injects packets into the network, aim to steal information and eavesdrop on network traffic. In order to avoid negatively affecting the system's performance, this factor should be taken into account.

1.2.2 Ad-Hoc Placement

Sensor nodes that are dispersed randomly lack a preset design. It is not possible to create a regular structure in sensor networks because of their ad hoc nature. The great mobility of network nodes makes it likely that the topology will constantly change. As a result, security solutions need to be flexible to accommodate this dynamic environment [15].

1.2.3 Hostile Environment

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

An further challenge is the hostile environment where sensor nodes are deployed. Because the transmission channel is broadcast, WSNs are prone to a wide range of security flaws. Nodes are also placed in hazardous or unsafe conditions where they are not physically protected. Attackers have the ability to take control of a node, physically alter it, and extract crucial data from it. For security researchers, the hostile environment presents a difficult obstacle.

1.2.4 Resource Limitation

For their implementation, all security strategies need a significant amount of resources. contains power for the sensor's functioning, memory, and bandwidth. The existing very constrained availability of these resources in a tiny wireless sensor, however, creates substantial obstacles for resource-intensive security solutions.

1.2.5 Imperfect Memory and Storage Volume

A sensor node is a small computer with very little memory and storage space for programs. The amount of the source code for the algorithm must be kept to a minimum in order to provide an effective security system.

1.2.6 Power Restriction

As the use of WSNs grows, this has turned into the biggest limitation and most important need since each node's activities depend on energy. The system can go offline if one node fails. Thus, it is essential to develop techniques that save energy resources.

1.2.7 Scalability

Scales in WSNs range from a few nodes to perhaps several dozens. Additionally, the deployment density may be altered appropriately. The node density may get so high during the high- resolution data collection procedure that each node has a large number of neighbors within its transmission range. The protocols used in SNs should be scalable to such levels and capable of successfully maintaining and preserving performance.

1.2.8 Unreliable Communication

Unreliability in the communication channel is undoubtedly another challenge for sensor security. A specific protocol, which is dependent on communication in turn, is the main factor affecting the security of the network.

1.2.9 Unreliable Transmission

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

Typically, the sensor network's packet-based routing is connectionless and hence intrinsically unstable. Due to channel failures or being lost at nodes that are extremely busy, packets may suffer damage. A loose retract or missing packets are the result [2]. Damaged packets are another effect of the faulty wireless communication link. The software developer must allocate more resources to error handling due to a greater channel error rate. More crucially, it is possible to lose crucial security packets if the protocol does not handle takeover errors.

1.2.10 Conflicts

The communication may be unreliable even when the channel is reliable because of data packet congestion. This is true because WSNs are broadcast systems. Even though the route is honourable and the communication is via the market, it might still be unstable.

1.2.11 Latency

The length of time it takes a node to watch, find, and communicate actions is known as latency. Data is gathered, processed, and sent to the base station via sensor nodes. These operations and the time it takes a sensor node to transport data in a dense or sparse network are used to calculate the latency of a network. It might be challenging to synchronize sensor nodes because to network delay caused by factors including multi-hop routing, network congestion, and node dispensation.

1.3 Outbreaks on Wireless Sensor Networks

WSNs are vulnerable to a number of security flaws since the transmission route is multi-hop in wildlife. WSNs are also vulnerable since nodes are frequently placed in risky or weak areas. The communication protocol for WSNs does not have a standardized layered architecture, but it is nevertheless required to list potential dangers and security measures in accordance with the ISO-OSI model's distinct tiers [3].

2. PROPOSED SYSTEM ARCHITECTURE

The so-called wormhole attack, which was initially described in [1], [2], and [3], is one of the most significant security dangers. With low resources, an adversary may carry out this sort of assault without jeopardizing any network sensors or getting through any cryptographic safeguards. The intrusive party sets two radio receivers in remote areas of the network,

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

connected by a high-speed, high-capacity channel, to begin the attack. Received signals are relayed through the "wormhole" by the receivers.

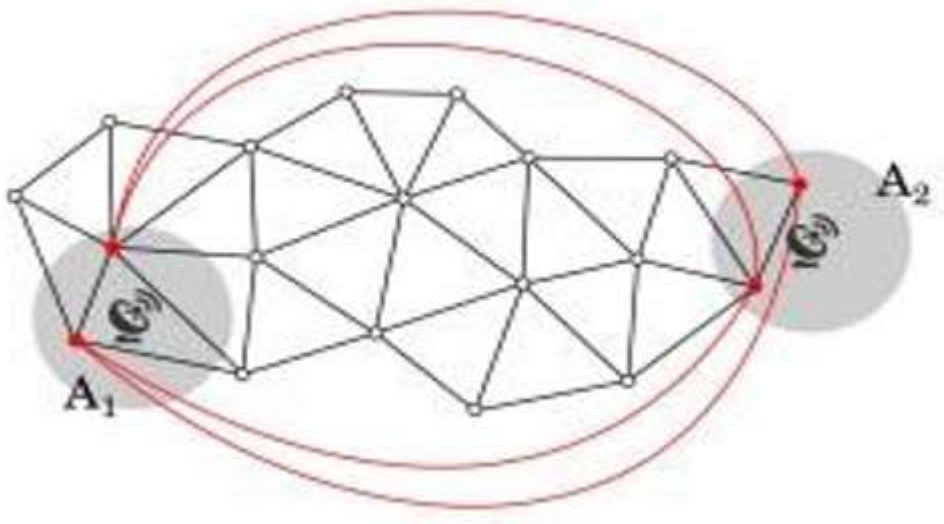

Fig.:2.1 Example of a wormhole attack. A1 and A2 are the areas directly affected by the two receivers. As a result of the attack, new connections are established between all nodes of A1 and A2 Wormhole Attack Architecture

The security of WSNs should be taken into consideration in many applications. For example, precise data collectors are essential if sensors are to detect drilling data effectively in an oil well. They must also be free from tampering, manipulation, and the insertion of phony data. In order to guarantee data privacy, confidentiality, authenticity, and accessibility as well as to survive attacks, the network must be able to. The core safety principles of WSNs are explained in this article.

2.1 Security in WSNs

1. Data Integrity: The goal of data integrity is to ensure that all the original data attributes established in the sensing node are retained on the way to the database station throughout the data life cycle.
2. Confidentiality: Information access rights must only be granted to nodes that have them.
3. Authenticity: This assures that the data is accurate and unchanged from the source node.

Because it guarantees that data is always accessible to authorized users, availability is essential.

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

2.2 Wormhole using Encapsulation

Attackers that use wormhole encapsulation shred the routing data and deliver it to their cooperator through other nodes. This kind of wormhole assault requires at least two attackers, and since the tunnel is built using regular network nodes, no special tools are required. The real hop count in this kind of assault does not rise throughout traversal. Figure 6 shows an example of an encapsulation-based attack, which is particularly dangerous to routing systems that employ hop count as a path selection. Assume that, in the presence of the two malicious nodes M1 and M2, nodes S (the source) and Sink (the destination) search for the quickest route to reach each other. An RREQ is transmitted by Node S. (Route Request Message), Through the path that exists between M1 and M2, M1 receives the RREQ and wraps it in a packet with M2 as its destination (E-F-G). The packet is returned to its original condition by Node M2, who then broadcasts it once more. The data packet's encapsulation prevents the hop count from rising while RREQ moves between M1 and M2 (E-F-G). In parallel, a second instance of the RREQ moves from S to sink over the path that passes via nodes A through BC. There are currently two ways to go from S to Sink: the first is a four-hop route (S-A-B-C-Sink), while the second looks to be three-hops lengthy (S-M1-M2-Sink), but really requires six hops (M1-E-F-G-M2-Sink). The second route is chosen by the sink because it seems to be the shortest one. This wormhole attack technique is easy to launch since neither of the two sides of the wormhole need special equipment like a high-speed wire line connection or a high-power source.

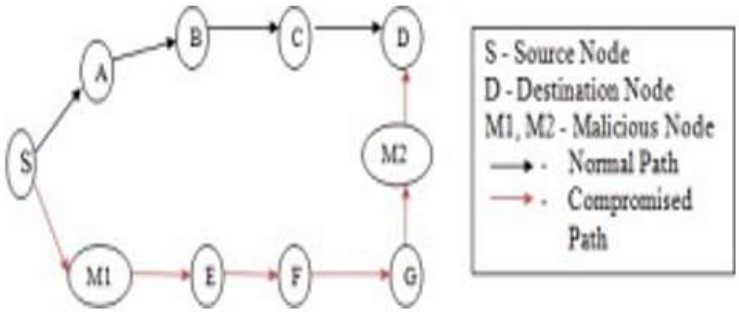

Figure 2.2 Wormhole through packet encapsulation

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

When a malicious node receives a route request in this manner, it is broadcast loudly and is therefore unavailable to other nodes on the network. The high-power broadcast must be retransmitted to the target by every node that receives it. A malicious node can increase its chances of being on the pathways connecting the source and the destination using this strategy, even in the absence of a cooperating node. An easy way to defend against this attack is feasible if every node has models of how signals travel over long distances and can compute signal strength accurately and securely. In this case, each node will decide on its own if the signal it is receiving exceeds the permitted power level. However, this approach is at best approximate and depends on the surroundings. This option is more functional when using a local monitoring method. A hostile node, which might be either an internal or external node possessing encryption keys, starts the wormhole. For instance, by compromising a legitimate node, an insider node can be created. These malicious nodes are all capable of collision and Byzantine behavior. A powerful entity with the capacity to quickly create out-of-band channels or have high transmission power capabilities might be the malicious node.

3. RESULTS & DISCUSSION

The suggested method for wormhole attack prevention and mitigation in ad hoc networks looked at two network characteristics, including throughput and packet delivery rate.

Table 4.1 Throughput

Nodes	**20**	**40**	**60**	**80**
Normal	84.62	88.32	90.32	91.20
Attack	29.35	36.74	48.90	59.43
Prevention	83.42	84.34	88.65	90.45

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

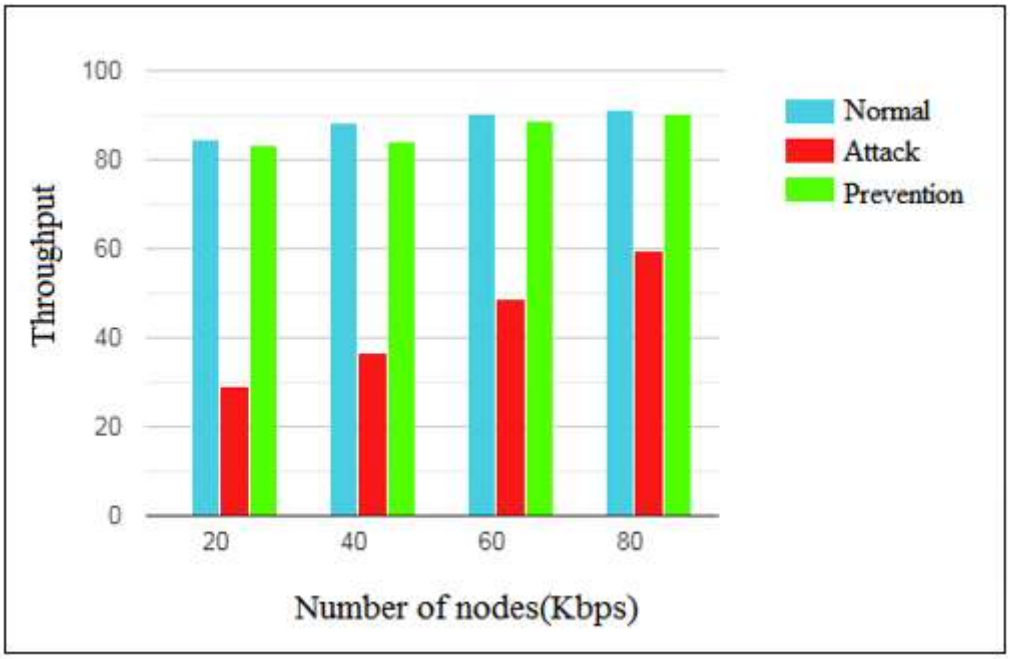

Figure 4.1 Throughput vs Number of Nodes (Kbps)

Kbps packets are shown as the Y-axis in Table 2 and Figure 4.2, and the X-axis is supplied for the number of nodes examined. Comparing the suggested technique to natural, attacked, and averted cases, throughput has risen.

Table 4.2 Packet Delivery Rate (PDR)

Nodes	**20**	**40**	**60**	**80**
Normal	95.47	88.27	97.12	98.45
Attack	32.34	36.58	43.32	58.39
Prevention	95.20	86.53	96.50	97.25

International Journal of Advanced Research and Multidisciplinary Trends (IJARMT)
An International Open Access, Peer-Reviewed Refereed Journal
Impact Factor: 6.4 Website: https://ijarmt.com ISSN No.: 3048-9458

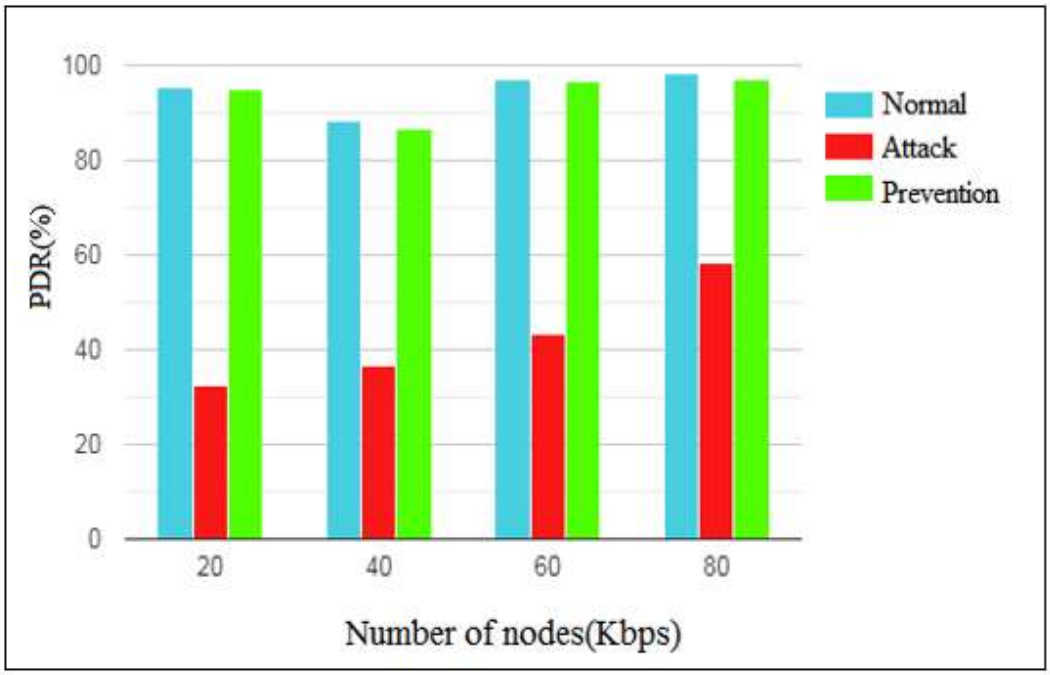

Figure 4.2 Packet Delivery Rate vs Number of Nodes

CONCLUSION

Another social event-based wormhole detection technique has been put forth. The requirement to exchange packages in the centres at remote enterprises with many skips exposes them to a variety of security issues, including the wormhole attack. Other recent research were assessed before this new approach was offered. The recommended approach, unlike some of its predecessors, does not require specialist hardware, such as instructions for locating the intrusion in addition to astonishingly accurate tickers. More evaluations are now being performed to assess the use of the advised count close to distinct attacking centres. Governments' opinions on ad hoc agreements are enhanced when the numbers change. Nevertheless, because of earth and hub physical standards, remote ad hoc systems are vulnerable to several attacks. Two parasitic hubs engaged in a wormhole attack do substantial damage to systems and hubs. Wormhole detection in ad hoc groups is still a difficult problem. Comparative investigation of several detecting variables is conducted. It was discovered that for systems with the proper values of the system characteristics, wormholes could be located

using a small number of packets, and that systems with highly mobile nodes performed far better in terms of quicker detection times.

References

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in Proceedings of 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.pp.293-301

[2] He, R., Ma, G., Wang, C., & Fang, L. (2009). Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes. World Academy of Science, Engineering and Technology.

[3] He Ronghui, Ma Guoqing, Wang Chunlei, and Fang Lan "Detecting and Locating Wormhole attacks in wireless sensor networks using Beacon Nodes" International Journal of Computer and Information Engineering Vol:3, No:7, 2009

[4] Rama Krishna Challa , Mani Arora, Divya Bansal, "Performance Evaluation of Routing Protocols Based on Wormhole Attack in Wireless Mesh Networks", IEEE Second International Conference on Computer and Network Technology, pp 102-104, 2010.

[5] Preeti Nagrath, Bhawna Gupta, "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A survey", pp 245-250, IEEE 2011

[6] Majid Meghdadi, Suat Ozdemir and Inan Guler, "A Survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", IETE TECHNICAL REVIEW, VOL 28, ISSUE 2, Mar-Apr 2011.

[7] Priya Maidamwar and Nekita Chavhan "A Survey on Security Issues to Detect Wormhole Attack in wireless sensor network, International Journal on AdHoc Networking Systems (IJANS)Vol. 2, No. 4, October 2012.

[8] Abhishek Jain, Kamal Kant, "Security Solutions for Wireless Sensor Networks", IEEE Second International Conference on Advanced Computing & Communication Technologies, pp 430433,2012.

[9] M. Bendjima and M. Feham, "Wormhole attack detection in wireless sensor networks," 2016 SAI Computing Conference (SAI), London, 2016, pp. 1319-1326.

[10] S. Bhagat and T. Panse, "A detection and prevention of wormhole attack in homogeneous Wireless Sensor Network," 2016 International Conference on ICT in Business Industry & Government (ICTBIG), Indore, 2016, pp. 1-6

[11] P. Khandare, Y. Sharma and S. R. Sakhare, "Countermeasures for selective forwarding and wormhole attack in WSN," 2017 International Conference on Inventive Systems and Control (ICISC),
Coimbatore, 2017, pp. 1-7

[12] Z. Liu, X. Deng and J. Li, "A secure localization algorithm based on reputation against wormhole attack in UWSNS," 2017 International Symposium on Intelligent Signal Processing and Communication Systems (PACS), Xiamen, 2017, pp. 695-700.

[13] Pradeep Chouksey, "Study of Routing in Ad hoc network", International Journal of Scientific Research in Network Security and Communication, Vol.5, Issue.2, pp.55-57, 2017.

[14] M. Arora, S. Sharma, "Synthesis of Cryptography and Security Attacks", International Journalof Scientific Research in Network Security and Communication, Vol.5, Issue.5, pp.1-5, 2017.