Shireen Fatima, 2022, 10:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

A Survey on Attacks Detection in Wireless Sensor Network

M.Tech. Scholar Shireen Fatima, Dr. Shaheen Ayyub
Department of Computer Science and Engineering
Technocrats Institute of Technology,
Bhopal MP, India

Abstract- A number of solutions have been developed using Wireless Sensor Networks (WSN). The main goal of a wireless sensor network is to enable different devices to communicate with one another. As a result, this virtual network assists the client in gathering and transmitting data via the Internet. WSN is, at the end of the day, an extension of the digital world that now includes tangible objects from the real world. WSNs were widely used for detecting and observing traffic, securing country borders, and analyzing pollutants, among other things. In light of the working technique for WSNs, security is the most basic and fundamental concern in wireless frameworks. Power consumption-related attacks, bandwidth-related attacks, routing-related attacks, identity-related attacks, and privacy-related attacks are all discussed in detail in this work. Researchers in this subject offered and created research solutions, which were also addressed. Finally, numerous strategies for detecting various forms of WSN assaults were addressed, which aid in the identification of hostile nodes in wireless networks.

Keywords- Adhoc Network, Wireless Sensor Network, Communication Attacks, Virtual machines.

I. INTRODUCTION

The main goal of the WSN concept is to make various devices capable of exchanging data with one another. As a result, this virtual network assists the client in gathering and transmitting information across the Internet. WSN is, at the end of the day, an extension of the digital world that now includes tangible objects from the real world. WSN becomes a module of the more broad class of digital physical network when it is extended with sensors and actuators. Sensors help us collect more precise data about our real-world surroundings.

As a result, the incorporation of these actuators has increased control over the scenario that exists in the real world. Information management encourages us to automate a number of processes and expand our framework's knowledge base. The primary goal of the Internet of Things is to improve the quality of people's daily lives [1].

Wireless communication technologies are evolving at a rapid pace. In the last few of years, there has been a lot of progress in the field of wireless sensor networks (WSNs) [1]. WSNs (wireless sensor networks) are one of the most useful and important technologies in the twenty-first century. Wireless sensor networks are made up of a large number of low-cost, low-power, multi-functional sensor nodes that can be utilized in any application [2].

The development of large-scale sensor networks with a few hundred to a few thousand sensor nodes presents a number of specific challenges as well as a plethora of application possibilities. With the commercial availability of sensors with networking capabilities, wireless sensor networks have gone from the realm of research into the real world. Crossbow and Sensoria, for example, have risen to prominence as suppliers of critical equipment and software building blocks [3].

This study focuses on WSN security challenges. WSNs are typically employed to collect data from various parts of the physical world, and they are deployed in both controlled and uncontrolled environments, making wireless sensor networks

insecure by their uses and deployment nature. These networks have a number of limitations, including node (low computational power, memory, and energy), network (the network acts as a mobile ad-hoc network), and physical limitations (deployed in public and hostile environments), all of which make them completely vulnerable to various security attacks. The ad-hoc nature of sensor networks is the key obstacle that affects their security and reliability.

Ordinary security approaches and procedures are not adequate to look after Authentication, Availability, and Integrity in WSN [4] due to the limited computational and processing capabilities. Wireless sensor networks (WSNs) are extremely vulnerable to both external and internal attacks since they are made up of a variety of devices with limitations such as limited memory, low energy, and low battery capacity. Wireless links are used by nodes in WSNs to communicate. There are still unsolved challenges in WSNs, and security is one of the most important study topics [4]. WSN networks are used in hostile environments.

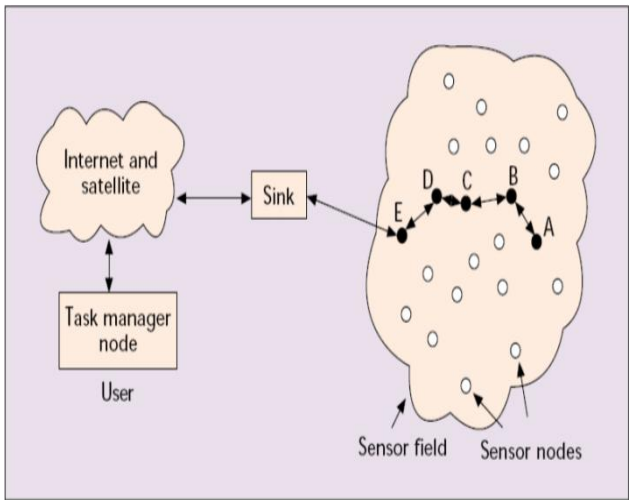

Figure1.Wireless Sensor Network.

II. RELATED WORK

LEACH [2] is a fantastic bunching-based method. Sensor nodes are sorted into a bunch in LEACH. There are bunch heads and element nodes in each group. LEACH uses neighborhood handling to reduce the amount of data sent to the BS, lowering energy consumption and increasing system lifetime. Each group's bunch heads are chosen using computational methods. The primary hurdle to LEACH is that if a sensor node with lower outstanding energy is chosen as bunch head, it will bite to shorten life quickly, eventually causing the entire group to become unusable.

The researcher presents an energy harvesting aware (EHA) computation based on a game hypothesis in [3], which talks to sensor activities as a sport (game). In this strategy, the high harvesting energy sensor nodes assist the low harvesting energy sensor nodes in maintaining the sensor arrangement's availability. In order to perform the Directed Local Spanning Sub graph (DLSS) computation, the suggested algorithm first creates a starting topology. This effort examines the energy consumption and collection rates of each sensor node at various times. At that moment, each sensor node tries to communicate with an adjacent node, which spreads up the sensor node's remote neighbour by adjusting the communication control step by step.

In this research [4], Audit Misbehavior Detection (AMD) can create ways with extremely confided in nodes that are subject to a desirable way length constraint. When paths contain mischievously acting nodes, a social assessment process successfully positions these nodes. AMD separates various dropping techniques by allowing the source to coordinate with any desired special dropping examples. When end-to-end activity is jumbled, this is extremely important. Only the source and goal approach the substance of the data units in the last circumstance, and they can identify specific dropping.

In this study [5], the source node verifies the legitimacy of the node that initiates RREP by identifying more than one path to the target. The source node waits for RREP data units to arrive from more than two nodes. The repeating paths in most typically feature some common hops or nodes in carefully designed systems. If courses to target shared hops, source node can perceive the protected course to goal when it receives RREPs. Regardless, this strategy may cause a routing delay. Because a node must wait for the RREP data unit to touch base from more than two nodes, it must be patient. In this case, a strategy that keeps the assault going while reducing routing overhead and deferring routing is necessary.

A wormhole identification protocol based on neighborhood and connection information was proposed by Manish Patel and Dr. Akshai Aggarwal

[6]. The proposed approach can effectively detect wormhole attacks while using less store space, according to a performance investigation. In wireless sensor networks, the proposed approach may successfully identify wormhole attacks. It has a low storage cost and can be used in resource restricted wireless sensor networks, according to a performance investigation.

Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack in WSN was proposed by Mosmi Tiwari et al., [7]. This research treats this issue as a serious one and attempts to provide a system for detecting and preventing wormhole nodes in mobile ad-hoc networks. The goal of this research is to investigate various methods for wormhole creation and develop approaches for detecting and preventing wormhole nodes using the AODV routing protocol.

The authors of [8] paper suggest a message analyzer method for WSNs. The approach can detect compromised SNs that are horizontal to DDoS attacks. Furthermore, it is capable of detecting any compromised communications sent to the base station via the sender nodes by the attackers.

III. CLASSIFICATION OF ENERGY EFFICIENT TECHNIQUES

1. Layer-by-layer attacks:

Multiplexing of data streams, data frame detection, medium access control, and error correction is all handled by the link layer. At this layer, malicious collisions, resource exhaustion, and unjust allocation are all possible attacks. When two nodes try to communicate on the same frequency at the same time, a collision occurs [11]. Colliding packets are rejected and must be re-transmitted. Collisions in specific packets, such as ACK control messages, might be strategically caused by an attacker.

The costly exponential back-off is one conceivable outcome of such accidents. The adversary could simply break the communication protocol and send messages incessantly in an attempt to cause collisions. An attacker can also employ repeated collisions to generate resource exhaustion [11]. A naive link layer implementation, for example, may attempt to retransmit damaged packets indefinitely. The energy levels of the nodes would quickly be depleted unless these retransmissions were discovered early. Unfairness is a type of DoS attack that is relatively weak [11]. Intermittently using the above link layer assaults, an attacker can induce unfairness. In this example, the adversary degrades real-time applications operating on other nodes by interrupting frame transmissions intermittently.

2. Attacks on the network layer:

WSNs are vulnerable to a variety of attacks, including I faked routing information, (ii) selective packet forwarding, (iii) sinkhole, (iv) Sybil, (v) wormhole, (vi) hello flood, and (vii) acknowledgment spoofing, among others. The following is a quick description of these attacks: Routing information spoofing: the most direct attack on a routing protocol is to target the network's routing information. To interrupt network traffic, an attacker can fake, change, or replay routing information [12]. Routing loops are created, network traffic is attracted or repelled from certain nodes, source routes are extended or shortened, fake error messages are generated, network segmentation occurs, and end-to-end latency is increased.

2.1 Selective forwarding: In a multi-hop network like a WSN, all nodes must accurately forward messages for message communication. An attacker might hack a node and cause it to selectively forward some messages while dropping others [3].

2.2 Sinkhole: In a sinkhole attack, an attacker forges routing information to make a compromised node appear more desirable to its neighbours [13, 12, 11]. As a result, neighbouring nodes chose the compromised node as the next-hop node via which to route their data. Because all traffic from a vast area of the network would go through the hacked node, this form of attack makes selective forwarding fairly straightforward. In a network, a Sybil attack occurs when one node presents many identities. It was first described as a method of defeating the goal of redundancy mechanisms in distributed data storage systems in peer-to-peer networks [11]. This attack is described by Newsome et al from the standpoint of a WSN [13]. The Sybil attack is effective against routing algorithms, data aggregation, voting, fair resource allocation, and misbehaviour detection, in addition to distributed data storage systems. The Sybil algorithm performs equally regardless of the target (voting, routing, or aggregate). All of the methods entail the use of numerous identities. The

Sybil attack, for example, could use numerous identities to produce additional "votes" in a sensor network voting method. Similarly, the Sybil attack would rely on a malicious node impersonating several nodes and routing various paths through a single malicious node to disrupt the routing protocol. A wormhole is a low-latency link between two parts of a network through which an attacker can replay network messages [14]. This link can be made by a single node forwarding messages between two adjacent but otherwise unrelated nodes, or by a pair of nodes in separate areas of the network talking with one another. An attacking node near the base station can establish a one-hop link to that base station via another attacking node in a different area of the network, which is similar to a sinkhole attack.

2.3 Hello Flood- most protocols that use Hello packets make the naive assumption that receiving such a packet means the sender is within the receiver's radio range. An attacker could employ a powerful transmitter to deceive a large number of nodes into believing they are in its vicinity [12]. As a result, the attacker node broadcasts a falsely shorter route to the base station, and all nodes who got Hello packets try to transmit to the attacker node. These nodes, however, are beyond the attacker's radio range. Some routing methods for WSNs require the delivery of acknowledgment packets, which can be spoofed. An attacking node can listen in on packet broadcasts from its neighbours and spoof acknowledgements, giving the nodes incorrect information [12]. The attacker is able to transmit false information about the state of the nodes in this fashion.

3. Attacks on the physical layer:

Frequency selection, carrier frequency production, signal detection, modulation, and data encryption are all handled by the physical layer [12]. The possibility of jamming exists, as it does with every radio-based media. Furthermore, WSN nodes could be put in hostile or unsecure locations where an attacker has physical access. Jamming and tampering are two forms of assaults on the physical layer.

Jamming is an assault that interferes with the radio frequencies used by the nodes in a WSN to communicate [11]. A powerful enough jammer source might bring the entire network down. By strategically placing jamming sources, even with less powerful jamming sources, an attacker might potentially disrupt communication across the entire network. Even sporadic jamming could be harmful since message communication in a WSN can be particularly time-sensitive [11].

Sensor networks are usually used in outdoor settings, hence they are vulnerable to tampering. The nodes of a WSN are especially vulnerable to physical attacks due to their unattended and scattered nature. Physical strikes on nodes may result in irreparable damage. The attacker can acquire cryptographic keys from the seized node, tamper with its circuitry, change its programme codes, or even replace it with a hostile sensor [15]. Sensor nodes, such as MICA2 motes, have been found to be hacked in less than one minute.

4. Attacks on the transport layer:

Flooding and desynchronization attacks are two types of attacks that can be performed against the transport layer of an SN.

4.1 Flooding: A protocol becomes subject to memory fatigue when it is expected to maintain state at either end of a connection [16]. An attacker can keep requesting additional connections until the resources required by each connection are depleted or the maximum limit is reached. Further reasonable requests will be disregarded in either situation.

4.2 De-synchronization: De-synchronization refers to the breaking down of a previously established link [16]. For example, an attacker may send spoof messages to an end host frequently, prompting the host to request the retransmission of missed frames. An attacker can degrade or even prevent end hosts from effectively exchanging data if they are timed appropriately, leading them to waste energy attempting to recover from faults that never existed.

5. DoS (Distributed Denial of Service) attacks:

A DoS attack, according to Wood and Stankovic, is an event that reduces or attempts to impair a network's capacity to execute its intended function [17, 18]. Although there are various conventional strategies for dealing with some of the more prevalent denial of service attacks in the literature, the development of a general defense mechanism against DoS attacks remains an unresolved subject in a broader sense. Furthermore, most protection

systems have a substantial computational burden, making them unsuitable for WSNs with limited resources.

Because DoS assaults in WSNs can be very costly, researchers have put a lot of work into detecting different types of attacks and finding techniques to counter them. The next sections go through some of the most common types of DoS attacks in WSNs.

IV. ENERGY LOSSES AND TECHNIQUES FOR MANAGEMENT

Sensors absorb energy while detecting, handling, transmitting, or receiving information to meet the duty done by the sensor device, which is one of the reasons for energy losses in WSNs. The detecting subsystem is genetically designed to collect data. It was long known that restricting the amount of data extracted from a transducer conserved the energy of highly compelled sensors.

WSNs' inherent repetition will result in massive comparative announcing that the system is in charge of routing to the sink. The communication subsystem is a voracious source of energy scattering, according to test data. In terms of communication, there is also a tremendous amount of energy wasted in states that are useless from an application standpoint, such as [4, 19, and 20]:

1. Overloading:
When a sender sends a data unit, it is sent to all nodes in its transmission region, whether or not they are the proposed goal. When a node receives data units that are linked to distinct nodes, energy is lost in this way. One of the real energy dispersal reasons is idle listening. It occurs when a node tunes in to a sit distraction with the goal of gaining probable mobility.

2. Control packet overhead
To enable information transmissions, just a small number of control data units should be used.

3. Collision
When a node receives several data units in a short period of time, these data units collide. All data units that caused the crash must be discarded, and these data units must be retransmitted.

4. Interference:
Every node in the transmission range and the impedance area receives a data unit but is unable to decode it.

As system lifespan has become a crucial criterion for evaluating WSN, a variety of solutions for reducing energy consumption and extending system lifetime have been presented. Currently, this work provides a scientific classification of these procedures.

V. CONCLUSION

Adhoc networks and wireless networks are growing in popularity as computing services evolve. Wireless sensor networks, on the other hand, continue to raise security concerns due to their vulnerability to a variety of attacks. Wormhole identification in adhoc networks is still a difficult issue; as such assaults are carried out by two hostile nodes, causing significant damage to networks and nodes.

The solutions offered in prior research required specific hardware or algorithms to secure these wireless sensor networks from wormholes, DOS, and other threats. As a result, there is a higher requirement to keep the network in order, such as by detecting the offending node. As a result, the packet delivery ratio will improve. The trust-based technique is used to achieve this goal.

REFERENCES

[1] Satoshi Kurosawa1, Hidehisa Nakayama1, Nei Kato1, Abbas Jamalipour2, and Yoshiaki Nemoto," Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, PP.338–346, November 2007.

[2] Maria Sebastian and Arun Raj Kumar P, "A Novel Solution for Discriminating Wormhole Attacks in MANETs from Congested Traffic using RTT and Transitory Buffer" International Journal of Computer Network and Information Security, pp. 28-38, 2013.

[3] Imad Aad, Jean-Pierre Hubaux and Edward W. Knightl "Impact of Denial of Service Attacks on Ad Hoc Networks" IEEE/ACM Transactions on Networking, Vol. 16, No. 4, pp. 791- 802, August 2008.

[4] Yu Zhang, Loukas Lazos and William Jr. Kozma "AMD: Audit-based Misbehavior Detection in

Wireless Ad Hoc Networks" IEEE Transactions On Mobile Computing (Article in Press), 2012.

[5] M. A. Shurman, S. M. Yoo, and S. Park, "Black hole attack in wireless ad hoc networks," in ACM 42nd Southeast Conference (ACMSE'04), pp. 96-97, April 2004.

[6] Manish Patel and Dr. Akshai Aggarwal, " Detection of hidden wormhole attack in wireless sensor networks using neighborhood and connectivity information" in International Journal on Ad Hoc Networking Systems (IJANS) Vol. 6, No. 1, January 2016.

[7] Mosmi Tiwari, Deepak Sukheja, Amrita, " Modified Hop Count Analysis Algorithm (MHCAA) for Preventing Wormhole Attack in WSN" in Communications on Applied Electronics (CAE),vol.3,No.3 ,October 2016.

[8] Ademola P. Abidoye, Ibidun C. Obagbuwa. "DDoS attacks in WSNs: detection and Countermeasures" IET IEEE, January, 2018.

[9] Ms Nidhi Sharma, Mr Alok Sharma "The Black-hole node attack in MANET" 2012 Second International Conference on Advanced Computing & Communication technologies, 546-550 2012 IEEE.

[10] Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Black hole Attack in MANET", In Proceedings of IEEE 2nd International Conference on Communications, IEEE 2007.

[11] A.D. Wood and J.A. Stankovic, "Denial of service in sensor networks", IEEE Computer, Vol. 35, No. 10, pp. 54-62, 2002.

[12] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures", In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127.

[13] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses", In Proceedings of the 3rd International Symposium on Information Processing in Sensor Networks, pp. 259-268, ACM Press 2004.

[14] J. Hua, Z. Zhou and S. Zhong, "Flow Misleading: Worm-Hole Attack in Software-Defined Networking via Building In-Band Covert Channel," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1029-1043, 2021.

[15] X. Wang, W. Gu, S. Chellappan, Dong Xuan, and Ten H. Laii, "Search-based physical attacks in sensor networks: Modeling and defense, Technical report, Department of Computer Science and Engineering, Ohio State University, February 2005.

[16] Da-Zhi Sun, Zahra Ahmadian, Yue-Jiao Wang, Mahmoud Salmasizadeh, and Mohammad Reza Aref. "Analysis and Enhancement of Desynchronization Attack on an Ultra light weight RFID Authentication Protocol". eprint.iacr.org, 2015.

[17] M. A. Al-Naeem, "Prediction of Re-Occurrences of Spoofed ACK Packets Sent to Deflate a Target Wireless Sensor Network Node by DDOS," in IEEE Access, vol. 9, pp. 87070-87078, 2021.

[18] Gherbi Chirihane & Aliouat Zibouda, "Distributed energy efficient adaptive clustering protocol with data gathering for large-scale wireless sensor networks", Programming and Systems (ISPS), 12th International Conference, IEEE, 2015.

[19] T. Camilo, C. Carreto, J. S. Silva, F. Boavida, "An EnergyEfficient Ant-Based Routing Algorithm for Wireless Sensor Networks", 2006 Springer.

[20] Saneh Lata Yadav, R. L. Ujjwal, Sushil Kumar, Omprakash Kaiwartya, Manoj Kumar, Pankaj Kumar Kashyap, "Traffic and Energy Aware Optimization for Congestion Control in Next Generation Wireless Sensor Networks", Journal of Sensors, vol. 2021.