Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 3694- 3704
Research Article

Survey On Various Attacks And Intrusion Detection Mechanisms In Wireless Sensor Networks

J. Josephin Jinisha[1] ,Dr. S. Jerine[2]

[1]Research Scholar, Department of Computer Application, NOORUL ISLAM CENTRE FOR HIGHER EDUCATION
[2]Associate Professor, Department of Software Engineering, NOORUL ISLAM CENTRE FOR HIGHER EDUCATION

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract
The new and most advanced technologies include Wireless Sensor Network (WSN), widely used in a wide range of applications, for example, militarily and communication intelligence, environmental studies, modern logistics, medical services and equipment, agricultural applications, computers, IOT and ecosystems, etc. Due to its inherent energy resources and processing power limitations, WSN technology poses major network problems and realistic security. The threats were developed and a structured model of WSN security met the required safety objectives. We decided to provide our WSN security model with a practical theoretical analysis to meet this challenge. The distance between two adjacent moving sensors and entre leaving sensors and the moving intruders is still not extensively investigated and undetermined. Intrusion detection is one of the most critical wireless network security approaches. Different features were used to detect various malignant activities through an Intrusion Detection System (IDS). However, it is important to obtain location information for detection nodes and to plan routes to ensure that detections are avoided by advancing the electronic anti-recognition technology. It calls an "enhanced intrusion system" that creates more problems with conventional methods of intrusion detection. The most recent intrusion detection technology provides accurate information on the attack. The primary objective of intrusion detection, however, is a little aware if the protection has been breached. Furthermore, networks continue to have a significant effect on and weaken reliability and robustness. WSN theory and methods for data recovery, data consistency, network trust, network topology, and routing protocols have been previously used.

Keywords:FT – Fault Tolerance, CH – Channel Head DoS – Denial of ServiceNDAE - non-symmetric deep auto-encoder,MI – Mutual Information MLP – Multilayer Perception

Introduction

The WSN is a group of sensing nodes that communicate wirelessly so that data collection and all physical and environmental phenomena can be intelligently monitored. A WSN is a community of wireless nodes that can be set up as you wish. Due to the monitoring needs in very challenging areas, the wireless sensor systems play a major role in the military. In medicine, engineering, IT and industrial applications, WSN Technology was also found to be helpful. The protection problem is highly important, because of the violent nature of the WSN deployment scenarios. However, the general limitation in most models is that researchers are not able to track but become more vulnerable a wide range of security threats within WSN [1]. They suggest many methods for protection. Another problem is that such protections consume enormous resources to reduce the life span of a typical node. Therefore, a reliable long-term and energy-efficient WSN protocol [1] needs to be established that we understand the different types of safety attacks against WSN in detail. The intrusion detection systems based on WSN have been developed to address border controls, regional monitoring and security problems after disasters [2]. The project needs a continuous framework for controlling and tracking [3] intruders and can therefore be modeled as a coverage management concern for continued high-quality intrusion coverage.

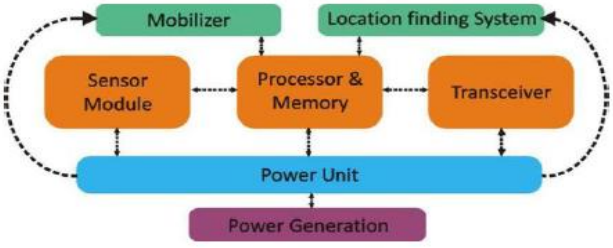

Figure 1: Block Diagram of WSN Node

Figure1 shows the transceiver transmitting a signal from the sensor node focuses on the basic operating concept and data transmission by the internal processor and sensor node or module memory. Mobile sensors can detect the same as static sensors and, after initial deployment, can adapt to the right situation to ensure an excellent coverage. The process of mobilisation is also included. Although these moving nodes increase the efficiency of coverage, no intruders can be detected and controlled. The attacker may also have sensor devices in real-world applications that collect information from detection nodes and plan trajectories with development in the field of electronic counter sensor technology for detection prevention. The smart operation which makes a sensor node

untractable and separate from naive intruders distinguishes this intruder. Consequently, it is difficult to develop a mechanism to effectively detected intruders by approved intruders[4]. If nodes are alerted to an intrusionist, the information is sent to the specific station or cluster node which, after review and processing, takes the necessary steps. The interplay between the detector nodes and the base or cluster node demands frequent activity that not only covers a high bandwidth but also increases the network transmission latency leading to delayed proceedings like an interruption or an intrusion. Therefore, the traditional central architecture, especially against strong intruders, is inappropriate for realistic scenarios. Mobile nodes must be able to record and process the trajectory in tracked intruders in realtime to obtain local computing; however, normal nodes can not do this[4].

Literature Survey

To achieve a continuous, high quality intrusion coverage issue for coverage improvement [5] the WSN intruder detection issues can be modeled. Three groups can be included: regional [6], objective [7] and obstacle [8][10], as well as a detailed optimization review of the WSN coverage. Various intrusion detection systems based on static sensor networks have been proposed. [11]. Sharmin et al., Objective coverage helps the network sensor to interpret and collect data from these targets while Barrier Coverage examines the possibility of a monitoring area detecting an item [12]. The purpose and obstacle can be covered through the detection of intrusion in WSNs [14]. The sensor node's versatility would enhance breaches of scope and boost the detection of intrusion [14].

Security in Wireless Sensor Networks (WSN)

The WSN safety specification must be stable and reliable to achieve the WSN safety objectives in Figure.2. Security hazard – a danger to safety that could affect system efficiency by infringement of security[15]. In most cases intercept, interrupt, operation, and performance are known as security risk / WSN attacks [15]. A type of attack which, without authorization, can harm privacy through a sensor node and data / key that it stored [15]. Interruption-a sort of attack which prevents legitimate communication between the parties. Disruption can damage access to the Internet [14] through message leakage, insertion of malicious code, physical node capture, etc. A challenge to the integrity of the network. The opponent can not only track, but also take advantage of, for example, the contents of data transmitted by the opponent during that attack. False data packets are introduced into an authentication of the vulnerable network by the adversaries [15]. It is not real to transmit the data.

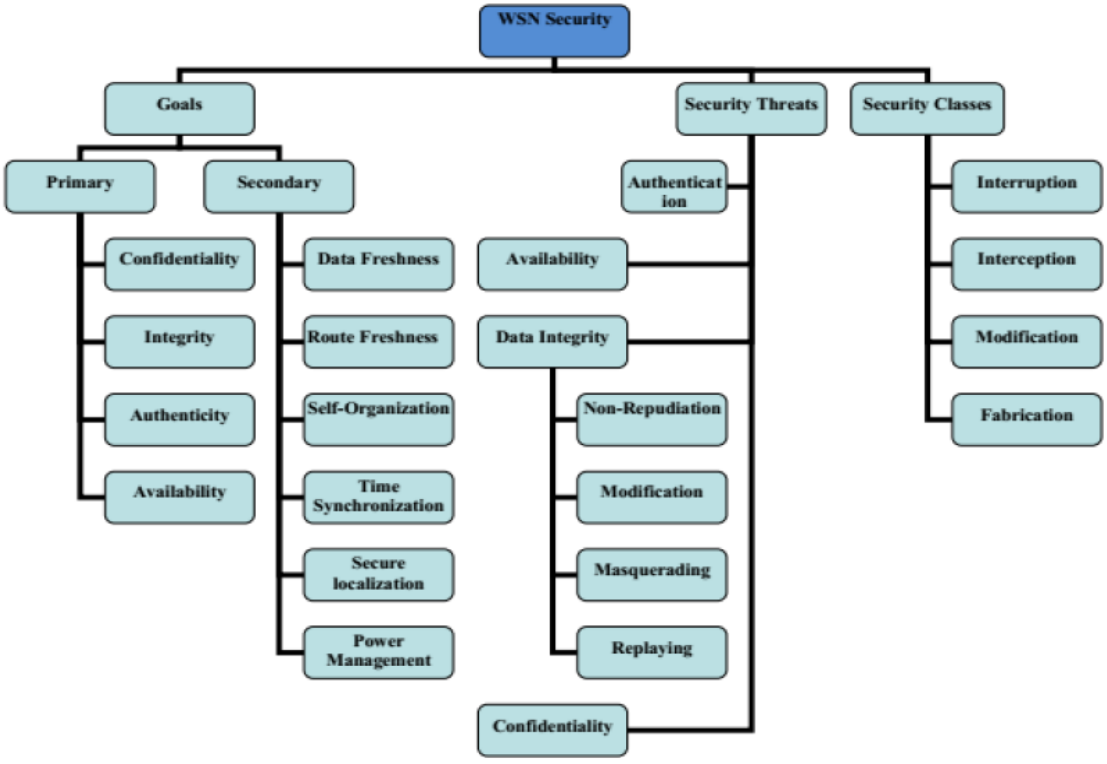

Figure 2:Classification of security issues in WSN.

ATTACKS ON DIFFERENT LAYERS OF WSN

Active Attacker

Efficient attacks to change and/or destroy network data trigger normal network activity [17] when the attacker begins. Simplifications [17] Changes in the data packet [20] unauthorized access control, eavesdropping, and modifications to data streams and resources if attacks are conducted by an in-house or internal adversary.

Passive Attacker

A passive intruder can message between nodes be disrupted in the regular network layout. The integrity of the data is not harmed during a passive attack, but the confidentiality of the data is breached. Therefore, detecting a passive attack is exceedingly difficult. The passive attacker can perform the following functions [21]: a standard node that gathers data from allocated attackers and enemies of communication channels through wireless networks, wipes, and surveillance.

Physical Layer Attacks

Jamming Attack – An attachment may trigger a jamming attack externally and internally. A powerful transmitter is used to perform a jamming attack, creating a powerful signal to interrupt legitimate wireless communication. Either an actual source can transmit a packet or reject legible packets [28]. WSN assaults in aggressive and remote areas in the majority of instances. The fractured and unforeseen deployment of WSN leaves these surroundings vulnerable to physical attacks. The attacker is able to physically break the node, block associated circuits, erase, modify sensor coding or replace robber sensor codes [29]. These physical attacks are often destructive of the sensor nodes, causing permanent losses [28]. The physical attack node Subversion-Instruments, like cryptopic keys, within the network may be exposed if an attacker physically or electronically captures a network. [30]. Passive Data Collection – A raiser can collect important information from the network of wireless sensors, if it is unencrypted in high-powered wireless sensor networks [28]. The data stream can easily be infiltrated by a hacker with an integrated antenna and a powerful receiver [17]. They can intercept and delete messages including the physical position of the sensor node [31]. In addition to the node sensor location, system drumming attacks [31] will also be analysed with messages IDs, timelines and other area of problem [31]. Nodes should be authenticated and signed for control messages from a discovered node target [16]. For example, the discovery of the track impedes the creation of a routing loop as no node can generate and mark a data packet for a node which has been generated or spoofed [16].

MAC Layer Attacks

Selfish node transmission — A selfish node normally prevents the transmission of packets, or actively drops packets to protect its property and resources [30]. It is not possible to relay packets. Malicious nodes – These attacks aim primarily at interrupting normal network activity, such as network resources and performance, thereby preventing other legitimate users from communicating [30]. Most of the attacks in these cases are Service Denial (DoS). Return Interval-If the sender wants to cause a service denial, the sender will be able to choose smaller intervals [30]. The vulnerabilities of Protocols 802.11[32] have been misused. Jelly Fish Attacks — The nasty node meets the Jelly Fish Assault protocol but secretly interrupts, delays and lowers packages [35]. An attack of this kind is hard to detect, since node functions take a long time, and so the confidentiality of such nodes cannot be overcome by a monitoring system [33]. Smart-Cheater attacks [34]-These attacks are like the Jelly Fish attacks [30] where nodes are almost always strong and sometimes weak [34]. The attacks are very difficult. It's too hard to hit. Due to smart and sophisticated nodes that sustain the confidence rate below the cap, the potential for harm to these threats cannot be discovered [34]. Jamming Connection Layer An grippes — this attack is designed to interrupt the usual functioning of the Jammer sensor nodes [36]. Many of the protocols take advantage of the link layer weakness [37]. In particular packages, such as accreditation (AC K) messages, collisions-collisions can intentionally occur in the enemies or adversarial node [36]. This means that a number of MAC protocols [36] are costly for exponential back-up.

Network Layer Attacks

This is a WSN attack [36] that is among the worst and most complex known as Wormhole Attack. An elevator maintains packet logs on one network location and constructs the tunnel through this tunnel at a separate network node [39]. In both of these collusive attack directions, this tunneling is referred to as a wormhole[40]. The colluding raids make the tunneling process a wormhole. When the two ends of a wormhole are rapidly shifting, rushing assault packages which have tunneled through a wormhole are spreading faster than any normal multi-hop path. This kind of hurried attack[41] is stated. Connect spoofing attack-Other nodes are distributed by malicious bugs other than neighbouring nodes to disrupt operations such as routing[42]. Byzantine attack — An intermediate node infected by the byzantine attack or a group of affected nodes is running, and attacks, including the transmission of packets through unoptimized pathways leading to routing loops, lead to routine degradation

and/or operational disruption. Many raiders are in favour of dropping and/or changing the packet(s) to avoid routing in their wireless device sensor network during such an attack. Colluding attacks unacceptable. The use of traditional or modern methods can not define such an attack[43]. Replay Attack — The topology of the WSN network also shifts with the movement of the sensor node, which means the current network topology will not last long. True control messages from another node are captured and transmitted in a sensing node like this[44]. Other sensor nodes must then record their routing tables[30]. Quick tracking collects information on the attack site position or location on the target node network structure. In order to prepare attack scenarios he collects node details like a roadmap. IP Spoofing Attack – The fresh node of a random address selected (call Y) is transmitted to a conflict allocation network and a packet (controversy detection) is transmitted. Any denial of the node would prevent such an address from being used. If the target node is a partner with the same IP address, then the attack is known as IP Spoofing as below[16]. This attack is not known. Next Attack: The intermediate node for the packet contains its ID until it is transmitted in the next node after it is received. If a raider transfers only the packet without indicating his identity, the nodes are adjacent even though they are not within contact. Routing messages are stopped directly by use of packet dropping attacks[16]. An attacker can work together in traditional attacks of this kind and also initiate packet drop attacks, which are regarded as the normal intermediate node. The concept behind the assault is to repeatedly question node-provided services. Sleep Default Attack Deprivation of Sleep Assault Torment So the node gets into inexhaustible state control or defence. The main objective of the assailant is to prevent him from sleeping in an attack in Sinkhole by drawing the full traffic from a compromised knot in a field. A sinkhole attack[45] is the method of receiving traffic. Sybil Attack-A malicious sensing node has numerous IDs for other nodes that are network components. This attack helps disperse networks that accept faults such as many paths[45]. False Node A fake sensation node increases the adversary 's sensing node and starts injecting malicious data. The intruder can be inserted with a network node that injects false or blocks the right channel[46]. A malicious code could enter all the nodes in the network and could theoretically kill or seize the network of the enemy[46]. The attacking node recognizes over hearted packets to provide fake data for neighbouring nodes[47]. Attack Spoofing Recognition True or false recognition will reassure the node that it is alive or solid. Selective forwarding attacks thus set target nodes by means of strong false links when sending information. The raider sends HELLO packets with more power from one node to another. In a network of wireless sensor systems for flood sensors, the attack uses HELLO packets as "loops"[17]. High power and communication are being used by the raider and HELLO packets are transmitted to different node sensors inaccessible in wireless sensor networks[47]. These sensors warn you that the raider is your neighbour. The hit-nodes then try, as their neighbours know, to move the raider to the base station and eventually talk[45]. When an attack happens, the raider tries to build roads to nodes that do not exist. This initiative's main objective is to establish the required means of preventing new roads and thus resolve the implementation of the Protocol[17]. Table overflow routing assault The compromised network node(s) modify the true direction of the routing attack table, or forward the wrong routing changes to other node(s) called the poisoning attack on the router table. Routing table attacks This routing table infection causes or may lead to sub-optimized routing in parts or parts of the network[17]. Replication Package Attack — Compressed node uses the extra bandwidth and battery power node for replicating antique packets to generate accidental confusion during packet routing. Attack-Any node has a route cache with information on itineraries recognized in recent years for reactive routing protocols like AODV. In order to achieve similar goals, a raider can also damage the traffic cache, such as route toxicity[17]. The raider spoke about the node IP address and then listed the appropriate number of sequences the node had expected and attacked in Denial of Service[17] during this form of assault.

Application Layer Attack

Misrepresented code intent is to target the kernel as well as user applications like worms, malware, Trojan horse and spyws[48]. Typically malicious programmers damage computers and networks or slow them down[48]. False filtration Attack — Wireless sensor network data are also used to merge in-network data [47]. End-to - end encryption is not feasible due to data collection specifications[56]. An assembly point attack allows an intrusionist to modify or manipulate the sensor implementations, the entire amount of data collected from downstream nodes and the network station agglomeration effect[47]. The Attack-Time synchronization network is a building block[50]. The sleep cycle can be disrupted during synchronization[50]. During the whole time interchange, the raider node sends the wrong syncing message to its neighbouring nodes and constructs more nodes to evaluate the wrong step and offset skew[47]. The essence of a mixture of networks is revealed to fictional data. False Injection Attack By sending false data to your data packets, an attacker may begin an external attack. It can also be launched if the internal nodes are first affected, and then misinformation into the network[47].

Data Link Layer Attack

Tracking and eavesdropping – eavesdroppers for example can easily detect messages by data snooping via information from the traffic control network wireless sensors[17]. Eavesdroppers can collect more information

than can be collected from the server. Traffic analysis-Transmission of encrypted messages[17] remains possible to be analyzed for WSN traffic trends. In order to damage the opponent, sensor communication should reveal necessary information inside the sensor network. Camouflage Enemies-The attacker can jeopardize or cover the number of nodes required on the wireless sensor network. The nodes imitate packets and misunderstand the data protection[17]. They 're a default node. Trace Packet — The immediate source for an overheard packet[51] is alerted by an equipped attacker in the tracking packet attack. The attacker will track the original hop-by data source[47]. The explanation also looks at the way the database is private.

S.No	Attack	Security Class	Attack Threat	Threat ModelActive/ Passive
1	Jamming Attack	Modification	Availability/ Integrity	Active
2	Physical Attack	Modification	Integrity/ Availability	Active
3	Node Subversion	Modification	Integrity/ Availability	Active
4	Passive Information Gathering	Modification/ Interception	Confidentiality/ Integrity/ Availability	Active
5	Device Tampering Attack	Modification/ Fabrication	Confidentiality/ Integrity/ Availability	Active
6	Selfish Nodes' Refusalto forwarding Packets	Interruption	Availability	Active
7	Nodes Malicious Behaviour	Interruption	Availability	Active
8	Back-off Interval Manipulation	Interruption	Availability	Active
9	Jellyfish Attack	Interruption	Availability	Active
10	Intelligent Cheater Attack	Interruption	Availability	Active
11	Link Layer JammingAttack	Modification	Integrity/ Availability	Active
12	Collisions	Interruption	Availability	Active
13	Wormhole Attack	Fabrication/Inte rception	Confidentiality/ Authenticity	Active
14	Rushing Attack	Interruption/ Interception	Availability/ Authenticity	Active
15	Link Spoofing Attack	Interruption	Confidentiality/ Availability	Active
16	Byzantine Attack	Interruption	Availability	Active
17	Colluding MisrelayAttack	Modification/ Interception/ Interruption	Confidentiality/ Integrity/ Availability	Active
18	Replay Attack	Interruption/ Interception	Confidentiality/ Availability	Active
19	Location Disclosure Attack	Modification/ Interception/ Interruption	Integrity/ Confidentiality	Active
20	IP Spoofing Attack	Fabrication	Authenticity	Active
21	Neighbor Attack	Fabrication	Authenticity	Active
22	Packet Dropping Attack	Interruption	Availability	Active
23	Sleep Deprivation Torture	Interruption	Availability	Active
24	Sinkhole Attack	Modification/ Fabrication	Confidentiality/ Integrity/ Availability	Active
25		Interruption/	Availability/	Active

	Sybil Attack	Fabrication	Authenticity	
26	False Node Attack	Interruption/ Interception	Availability/ Confidentiality	Active
27	Acknowledgement Spoofing Attack	Interruption/ Interception	Authenticity/Availability	Active
28	Hello Flood Attack	Interruption	Authenticity/Availability	Active
29	Routing Table Overflow Attack	Fabrication/ Interruption	Availability	Active
30	Routing Table Poisoning Attack	Fabrication/ Interruption	Availability	Active
31	Packet Replication Attack	Interruption	Integrity/ Availability	Active
32	Route Cache Poisoning Attack	Fabrication/ Interruption	Availability	Active
33	Session Hijacking Attack	Interruption/ Interception	Availability	Active
34	Malicious Code Attack	Interruption	Availability	Active
35	False Data Filtering Attack	Interruption/ Modification	Integrity/ Availability	Active
36	Clock Synchronization Attack	Interruption	Availability	Active
37	False Data Injection Attack	Interruption/ Fabrication	Authenticity/Availability	Active
38	Monitoring & Eavesdropping	Interception	Confidentiality	Passive
39	Traffic Analysis	Interception	Confidentiality	Passive
40	Camouflaged Adversaries	Interception/ Fabrication	Confidentiality/ Availability	Passive
41	Packet Tracking	Fabrication	Confidentiality	Passive

Table 1: List of Attacks on Different Layers

EXISTING INTRUSION DETECTION STUDY IN WSN

Trust Management

The goal is to determine and approximate targets' performance[52]. Management of the confidence in computer science. To protect suspicious processes and nodes, WSN-distributed systems and networks may use faith-oriented security mechanisms. IDMTM was introduced by Wang et al.[54], an innovative intruding sensing system. Their methodology assessed and developed a malicious node using two measurement measures: the Proof Chain (EC) and Trust Fluctuation (TF), with the result that the false alarm rate could be substantially reduced by efficient use of information collected from neighbouring and local nodes. Probst and Kasera[55] have determined the identification and minimization of dependency between sensor nodes on malicious sensors. It suggested a way to test statistical trust values and an interval of trust based on the sensor node behaviour. The Bayes rule helps to update the likelihood estimates[56] of the hypothesis with this Bayesian procedure. This model can be used to measure the trust values of an IDS object. This model can be used to assess the legitimacy of the nodes in a clustered WSN traffic information sensor. — Node may have two important roles in a WSN hierarchical: sensing and retransmission. Sensor nodes collect and send data collected directly to or through the cluster head. Sensor nodes can transmit or transmit information over a short distance through radio communication. It should be noted that within its cluster, all Nodes sensors can be managed and accessed. Data for analysis and estimation of trust data are then collected from various sensor nodes. Finally, CHs will pass the information to the base station. The trust of a CH should be determined by the base station in this hierarchical system [57] for more information.

Fault Tolerance

Various defect tolerance mechanisms in WSNs were suggested in order to ensure reliability, energy savings and a longer life cycle. One of the most effective strategies was node redundancy[58]. For node-based cover and networking, Korbi et al.[60] published the new FT protocol. Mukhopadhi et al[61] proposed Markov's reliability

analysis patterns and provided a reliability comparison with hot-standby redundant nodes of several defective node replacements. Bein et al[62] have discussed the coverage problem for WSNs of loss tolerance. The report's strategy was positive since it sought to restore the node "until collapse" before it was lost.

Denial of Service

Fragkiadakis et al. have Denial-Of - Service Detection IDS (DoS) in order to improve the signal-to - noise ratio and track them. [64] Value is based on various cumulative-value nodes, one threshold and two local algorithms. The device produces BPAs based on the information gathered by a linear process. The BPA discusses the principle of D-S. We combine several metrics in the layer stack. The first of three main algorithms is for the identification and avoidance of the exposure of the DoS attacks and the third for the minimization of the impact of the MAC attack on a safe source and the recognition of the MAC as part of the DoS attacks, disapproval and detection. The first is the detection address of the Mac-layer DoS. This approach consists of three large algorithms with thresholds. This device demonstrates the quality, recovery time and resending rate of packets. Only simulated network traffic has however been analysed and no actual network traffic assessment has been performed. The proposed work [66] offers IDs for networking mode 802.11 for open-source IEEE. This is ideal for wireless installation because not all network nodes are needed for installation. In addition, there are two types of attacks: de-authentication and poor twin attacks. These two attacks are identified by a variety of network traffic metrics. Since this device achieves 90% protection for malicious decompression and double assaults.

Knowledge-based IDS

This figure offers a brief overview of the intravenous system based on methods of detection [67]. 3. An anomaly and a signature-based detection technique are the detection techniques used in this study. A network profile is generated by an abnormal identification. Statistical modeling was used to construct standard Network interface statistical models and to compare them to actual test network parameters. It scans for the frequency of anomaly and does not strike if the defect reaches the threshold. In a number of test cases, the identification of information is based on the profile of the network, which it uses to detect intrusion. Machine learning is the third type of anomaly detection. This approach generally illustrates the current status and compares it with the previous network states' present network state. Examples such as Fuzzy learning, Neural Networks, Bayesian Networks and Master Language Methods Models are. Unregulated learning, unregulated learning and half-controlled and enhanced training are the forms of machine methods employed.

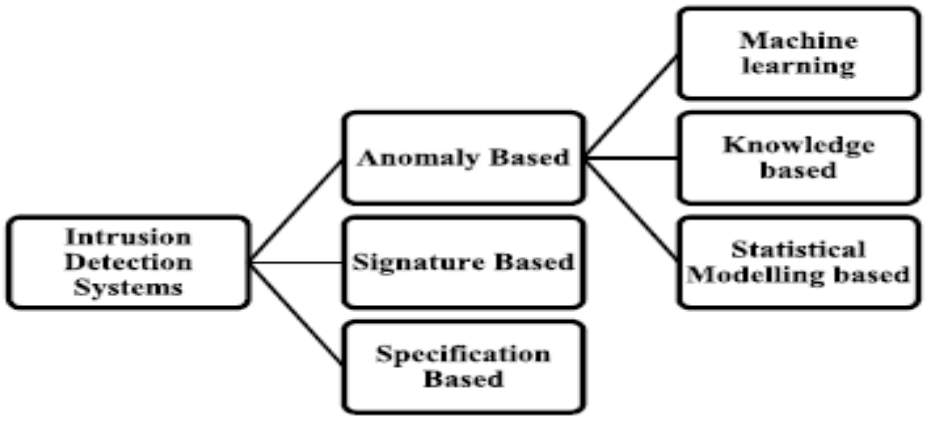

Figure 3: IDS Based Methods

Signature-based identification of a number of anomalous profiles is compared to a test network. It is understood that this system produces very few false positives and can detect previously recorded detector attacks. The intrusion detection based on requirements is focused on the set of user instructions or requirements.

A Deep Learning Method and Filter

Studies[68] have shown that a deep learning intrusion detection device for the learning of feats and the recognition of stacked NDAE's was the NDAE (Non-Symmetric Deep Auto-Encoder). An NDAE is a car encoder with several non-symmetric, hidden layers. It's a profound neural network with several non-symmetrical hidden layers. A multi-target algorithm MOMI is published by scientists[69]. It focuses on common knowledge (MI) concerning the precision and validity of the functional assessment and selection process. Tests were

conducted with the WEKA tool using three individual datasets[70] for testing MOMI performance. The classifications Naive Bayes (NB) and SVM were used. The results of this study show that only the functions needed to enhance efficiency can be selected by MOMI. The multi-layer perception (MLP) algorithm with controlled redundancy (CoR) was introduced into Chakraborty and Pal[71]. FSMLP-CoR is the way forward. MLP is a network neural input, a number of laying outputs and hidden layers (72). Typically this is used to approach, describe, extract and forecast a variety of domains[73][74]. The functions that are not difficult to overcome were defined and discarded by an MLP.

Feature Selection Method

Study suggested in [75] that a heuristic search tool and logistical regression (LR) assessment be the wrapper-based intrusion detection algorithm. GA is a heuristic and functional tool for intrusion detection. The whole system is called GA-LR. GA is a method of natural selection known as evolutionary algorithms[76]. Initial population, fitness function, genetic operator (variation, crossover and selection) and end criteria include: the following components. Wang et al.[65] used the FA algorithm instead of the feature reduction algorithm for unique purposes in terms of functional engineering methodology. The logarithm-marginal density ratio transformation was described as the SVM and FA algorithms in this research. The aim was to implement new technologies which would eventually result in greater precision of detection. In [78] this proposal uses an extensive approach to the intrusion detection of wireless network detections by IEEE 802.11 auto encoders stacked (SAE). SAE is a neural network with multi-layer sparse auto encoder. The studies conducted in this study were done using the Egeon (AWID) Wireless Intrusion Dataset, which consists of 155 ultimate class characteristics that can use the following values: injections, fluids, impersonations and frequencies.

DISCUSSION OF EXISTING INTRUSION DETECTION PRACTICE		
SL.NO	**VARIOUS INTRUSION DETECTION PRACTICES**	**OUTCOMES**
1.	Trust Management	Identification of Malicious Nodes
2.	Fault Tolerance	Identify coverage problem for WSNs of loss tolerance
3.	Denial of Service	Identification and avoidance of exposure of the DoS attacks
4.	Knowledge-based IDS	It scans for the frequency of anomaly and does not strike, if the defect reaches the threshold.
5.	A Deep Learning Method and Filter	The learning of feats and the recognition of stacked NDAE's
6.	Feature Selection Method	SVM and FA algorithms result in greater precision of detection in FSM

Table 2: Various intrusion detection methods

Conclusion

We stated in this paper the safety criteria and the risk of different attacks based on WSN and IoT and the sensor node implantation. This paper analysed and classified different forms of attacks in WSN as active and passive. Different IDS surveys have been closely examined, including trust, defect in tolerance, service denial, IDS-focused results, deep learning and the methods of philtering, and functional selection. Finally, some more research problems in developing intrusion detection system and other protocols for the security of WSN communications have been found.

References

[1] Muhammad NomanRiaz, AttaullahBuriro, AtharMahboob, “Classification of Attacks on Wireless Sensor Networks: A Survey”, © 2018 Published by MECS Publisher
[2] M. Mukherjee, L. Shu, L. Hu, G. P. Hancke, and C. Zhu, ``Sleep scheduling in industrial wireless sensor networks for toxic gas monitoring," IEEEWireless Commun., vol. 24, no. 4, pp. 106_112, Aug. 2017.
[3] F. Xiao, Z. Wang, N. Ye, R. Wang, and X.-Y. Li, ``One more tag enables fine-grained RFID localization and tracking," IEEE/ACM Trans. Netw., vol. 26, no. 1, pp. 161_174, Feb. 2018.
[4] WENMING WANG, et el,“Generalized Intrusion Detection Mechanism for Empowered Intruders in WirelessSensor Networks”, Digital Object Identifier 10.1109/ACCESS.2020.2970973

[5]S. Meguerdichian, F. Koushanfar, M. Potkonjak, and M. B. Srivastava, ``Coverage problems in wireless ad-hoc sensor networks," in Proc. Conf.Comput. Commun., 20th Annu. Joint Conf. IEEE Comput.Commun.Soc. (IEEE INFOCOM), vol. 3, Apr. 2001, pp. 1380_1387.
[6]Y. Zou and K. Chakrabarty, ``Sensor deployment and target localization in distributed sensor networks," Trans. Embedded Comput. Syst., vol. 3,no. 1, pp. 61_91, Feb. 2004.
[7] R. Falcon, X. Li, and A. Nayak, ``Carrier-based focused coverage formation in wireless sensor and robot networks," IEEE Trans. Autom. Control, vol. 56, no. 10, pp. 2406_2417, Oct. 2011.
[8]S. Kumar, T. H. Lai, M. E. Posner, and P. Sinha, ``Maximizing the lifetime of a barrier of wireless sensors," IEEE Trans. Mobile Comput., vol. 9, no. 8, pp. 1161_1172, Aug. 2010.
[9]C.-I. Weng, C.-Y.Chang, C.-Y.Hsiao, C.-T. Chang, and H. Chen,``On-supporting energy balanced k-barrier coverage in wireless sensor
networks," IEEE Access, vol. 6, pp. 13261_13274, 2018.
[10] H. Kim and J. Ben-Othman, ``A collision-free surveillance system using smart UAVs in multi domain IoT," IEEE Commun. Lett., vol. 22, no. 12, pp. 2587_2590, Dec. 2018.
[11] S. Sharmin, F. N. Nur, M. A. Razzaque, M. M. Rahman, A. Almogren, and M. M. Hassan, ``Tradeoff between sensing quality and network lifetime for heterogeneous target coverage using directional sensor nodes," IEEEAccess, vol. 5, pp. 15490_15504, 2017.
[12] H. Kim, J. Ben-Othman, S. Cho, and L. Mokdad, ``A framework for IoT- enabled virtual emotion detection in advanced smart cities," IEEE Netw., vol. 33, no. 5, pp. 142_148, Sep. 2019.
[13] M. Naderan, M. Dehghan, H. Pedram, and V. Hakami, ``Survey of mobile object tracking protocols in wireless sensor networks: A network-centric perspective," Int. J. Ad Hoc Ubiquitous Comput., vol. 11, no. 1, p. 34, 2012.
[14] B. Wang, H. B. Lim, and D. Ma, ``A survey of movement strategies for improving network coverage in wireless sensor networks," Comput.Commun., vol. 32, nos. 13_14, pp. 1427_1436, Aug. 2009.
[15] Mechanism for Wireless Sensor Networks", International Journal of Computer Trends and Technology- May to June Issue 2011.
[16] John Paul Walters, Zhengqiang Liang, Weisong Shi, VipinChaudhary, " Wireless Sensor Network Security : A Survey", Security in Distributed, Grid and Pervasive ComputingYang Xiao (Eds), page 3-5, 10-15, year 2006.
[17]Pradip M. Jawandhiya, Mangesh M Ghonge, Dr. M.S Ali, Prof.J.S. Deshpande," A Survey of Mobile Ad Hoc Network Attacks", International Journal of Engineering Science and Technology, Vol. 2(9), page 4063-4071, year 2010.
[18] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA, Special Issue on Mobile Ad-hoc Networks MANETs; CSE Department, SMIT, Sikkim, India; 2010.
[19] J. Yick, B. Mukherjee and D. Ghosal, "Wireless Sensor Network Survey", Elsevier's Computer Networks Journal 52 (2292-2330), Department of Computer Science, University of California, 2008.
[20] Y. Zhou, Y. Fang and Y. Zhang, "Security Wireless Sensor Networks: A Survey", IEEE Communication Surveys, 2008.
[21] Dr. ShahriarMohammadi and HosseinJadidoleslamy, "A Comparison of link layer attacks on Wireless sensor networks", International Journal on applications of graph theory in wireless adhoc and sensor networks", (GRAPH-HOC) Vol.3, No.1, March 2011.
[22] Y. Wang, G. Attebury and B. Ramamurthy," A Survey of Security Issues in Wireless Sensor Networks", IEEE Communication Surveys; 2006.
[23] K. Sharma and M. K. Ghose, "Wireless Sensor Networks: An Overview on its Security Threats", IJCA, Special Issue on "Mobile Ad-hoc Networks MANETs", CSE Department, SMIT, Sikkim, India,2010.
[24] WaltenegusDargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 8, year 2010.
[25] P. Kyasanur and N. H. Vaidya, "Selfish MAC layer misbehavior in wireless networks", IEEE Transactions on Mobile Computing, 2005, 4(5).
[26] WaltenegusDargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 11, year 2010.
[27] Pathan, A.S.K.; Hyung-Woo Lee; ChoongSeon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006
[28] Dr. G. Padmavathi, Mrs. Dr. Shanmugapriya," A survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Vol. 4, No. 1 & 2, year 2009.
[29] WaltenegusDargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 10, year 2010.
[30] WaltenegusDargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 6, year 2010.
[31] Vikrant Gokhle,S.K. Ghosh and Arobinda Gupta," Security of Self organizing Networks", chapter # 9, year 2010.

[32] IEEE802.11 wireless LAN media access control (MAC) and physical layer (PHY) specifications, IEEE, 1999. http://standards.ieee.org/getieee802/802.11.html.
[33] I. Aad, J. Hubaux, and E. W. Knightly, "Denial of service resilience in ad hoc networks", in Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom 2004), September 26–October 11, 2004, pp. 202–215, ACM Press, Philadelphia, PA, USA.
[34] L. Guang and C. Assi, "On the resiliency of mobile ad hoc networks to MAC layer misbehavior", in Proceedings of the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, October 10–13, 2005, Montreal, QC, Canada.
[35] R. V. Boppana and S. Desilva, "Evaluation of a statistical technique to mitigate malicious control packets in ad hoc networks", in Proceedings of the 2006 International Symposium onWorld of Wireless, Mobile and Multimedia Networks, 2006.
[36] Qinghua Wang and Tingting Zhang, "Security in RFID and Sensor Networks", chapter # 14, year 2010.
[37] Y. Law, P. Hartel, J. Hartog, and P. Havinga, "Link-layer jamming attacks on S-MAC", Technical Paper, University of Twente, the Netherlands, 2005.
[38] Y. C. Hu, A. Perrig, and D. B. Johnson, Packet leashes: "A defense against wormhole attacks in wireless networks", in Proceedings of Twenty-Second Annual Joint Conference of the IEEE Computer and Communications, March 30–April 3, 2003, Vol. 3.
[39] Y. C. Hu, A. Perrig, and D. Johnson, "Wormhole attacks in wireless networks", Selected Areas in Communications, 2006, 24(2).
[40] R. Maheshwari, J. GAO, and S. R. Das, "Detecting wormhole attacks in wireless networks using connectivity information", in Proceedings of 26th IEEE International Conference on Computer Communications, May 6–12, pp. 107–115, Anchorage, AK, USA.
[41] Y. C. Hu, A. Perrig, and D. B. Johnson, "Rushing attacks and defense in wireless ad hoc network routing protocols", in Proceedings of the 2nd ACM Workshop on Wireless Security, September 19, 2003, San Diego, CA, USA.
[42] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for Security", in 2nd OLSR Interop/Workshop, Palaiseau, France, July 28–29, 2005.
[43] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks",in Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, 2000, Boston, MA, USA.
[44] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks against OLSR: Distributed key management for Security", in Proceedings of 2nd OLSR Interop /Workshop, July 28–29, 2005, pp. 1–7, Palaiseau, France.
[45] Chris Karlof, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", Adhoc Networks (elsevier), Page: 299-302, year 2003
[46] G. Athanasiou, L. Tassiulas, and G. S. Yovanof, "Overcoming misbehavior in mobile ad hoc networks:An overview", ACM Crossroads 11.4: Mobile and Wireless Networking, 2005.
[47] Qinghua Wang and Tingting Zhang, "Security in RFID and Sensor Networks", chapter # 14, year 2010.
[48] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "DDoS defense by offense", in Proceedings of the SIGCOMM 2006, September 11–15, 2006, Pisa, Italy.
[49] Dr. ShahriarMohammadi and HosseinJadidoleslamy, "A Comparison of link layer attacks on Wireless sensor networks", International Journal on applications of graph theory in wireless adhoc and sensor networks", (GRAPH-HOC) Vol.3, No.1, March 2011.
[50] WaltenegusDargie and Christian Poellabauer, "Fundamentals of Wireless Sensor Networks: Theory and Practice", chapter # 7, year 2010.
[51] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source location privacy in sensor network routing", in Proc. 25th IEEE International Conference on Distributed Computing Systems (ICDCS), 2005.
[52] J. M. Gonzalez, M. Anwar, and J. B. D. Joshi, ``A trust-based approach against IP-spoo_ng attacks," in Proc. 9th Int. Conf. Privacy, Secur. Trust (PST), Jul. 2011, pp. 63_70.
[53]J.-H. Cho, A. Swami, and I.-R.Chen, ``A survey on trust management for mobile ad hoc networks," IEEE Commun. Surveys Tuts., vol. 13, no. 4, pp. 562_583, 4th Quart., 2011.
[54] F. Wang, C. Huang, J. Zhang, and C. Rong, ``IDMTM: A novel intrusion detection mechanism based on trust model for ad hoc networks," in Proc.22nd IEEE Int. Conf. Adv. Inf. Netw. Appl. (AINA), Mar. 2008, pp. 978_984.
[55] M. J. Probst and S. K. Kasera, ``Statistical trust establishment in wireless sensor networks," in Proc. Int. Conf. Parallel Distrib.Syst. (ICPADS), Dec. 2007, pp. 1_8.
[56] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, ``Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEEJ. Sel. Areas Commun., vol. 24, no. 2, pp. 305_317, Feb. 2006.
[57] WEIZHI MENG, et el, "Enhancing Trust Management for Wireless Intrusion Detection via Traffic Sampling
in the Era of Big Data" IEEE ACCESS, VOLUME 6, 2018,Page 7234 to 7243

[58] N. Jabeur, A. N. S. Moh, and M. M. Barkia, ``A bully approach for competitive redundancy in heterogeneous wireless sensor network," ProcediaComput. Sci., vol. 83, no. 10, pp. 628_635, Dec. 2016.
[59] B. Zebbane, M. Chenait, and N. Badache, ``Exploiting node redundancy for maximizing wireless sensor network lifetime," in Proc. Int. Conf. (IFIP), Nov. 2013, pp. 1_3.
[60] I. El Korbi, Y. Ghamri-Doudane, R. Jazi, and L. A. Saidane, ``Coverageconnectivity based fault tolerance procedure in wireless sensor networks," in Proc. 9th Int. Conf. Wireless Commun. Mobile. Comput.(IWCMC), Jul. 2013, pp. 1540_1545.
[61] S. Mukhopadhyay, C. Schurgers, D. Panigrahi, and S. Dey, ``Model-based techniques for data reliability in wireless sensor networks," IEEE Trans.Mobile Comput., vol. 8, no. 4, pp. 528_543, Apr. 2009.
[62] W. W. Bein, D. Bein, and S. Malladi, ``Reliability and fault tolerance of coverage models for sensor networks," Int. J. Sensor Netw., vol. 5, no. 4, pp. 199_209, Jan. 2009.
[63] A. Munir, J. Antoon, and A. Gordon-Ross, ``Modeling and analysis of fault detection and fault tolerance in wireless sensor networks," ACM Trans.Embedded Comput. Syst., vol. 14, no. 1, pp. 1_43, Jan. 2015.
[64] A. G. Fragkiadakis, V. A. Siris, and A. P. Traganitis, ``Effective and robust detection of jamming attacks," in Proc. Future Netw. Mobile Summit, 2010, pp. 1_8.
[65] L. Arockiam and B. Vani, ``Framework to detect and prevent medium access control layer denial of service attacks in wlan," Int. J. Comput.Netw.Wireless Commun., vol. 3, no. 2, pp. 152_159, 2013.
[66] Z. Afzal, J. Rossebø, B. Talha, and M. Chowdhury, ``A wireless intrusion detection system for 802.11 networks," in Proc. Int. Conf. Wireless Commun., Signal Process.Netw.(WiSPNET), 2016, pp. 828_834.
[67] I. Butun, S. D. Morgera, and R. Sankar, ``A survey of intrusion detection systems in wireless sensor networks," IEEE Commun. Surveys Tuts., vol. 16, no. 1, pp. 266_282, 1st Quart., 2013.
[68] N. Shone, T. N. Ngoc, V. D. Phai, and Q. Shi, ``A deep learning approach to network intrusion detection," IEEE Trans. Emerg.Topics Comput.Intell., vol. 2, no. 1, pp. 41_50, Feb. 2018.
[69] M. Labani, P. Moradi, M. Jalili, and X. Yu, ``An evolutionary based multiobjective _lter approach for feature selection," in Proc. World Congr.Comput.Commun.Tech. (WCCCT), Feb. 2017, pp. 1510_154.
[70] I. H.Witten, M. A. Hall, E. Frank, and C. J. Pal, ``TheWEKAworkbench," in Data Mining: Practical Machine Learning Tools and Techniques, 4th ed. Burlington, MA, USA: Appendix, 2017, pp. 553_571.
[71] R. Chakraborty and N. R. Pal, ``Feature selection using a neural framework with controlled redundancy," IEEE Trans. Neural Netw. Learn. Syst., vol. 26, no. 1, pp. 35_50, Jan. 2015.
[72] L. Vanneschi and M. Castelli, ``Multilayer perceptrons," Encyclopedia Bioinf.Comput. Biol., vol. 1, pp. 612_620, Jun. 2019.
[73] F. Murtagh, ``Multilayer perceptrons for classi_cation and regression," Neurocomputing, vol. 2, nos. 5_6, pp. 183_197, Jul. 1991.
[74] A. Mondal, A. Ghosh, and S. Ghosh, ``Scaled and oriented object tracking using ensemble of multilayer perceptrons," Appl. Soft Comput., vol. 73, pp. 1081_1094, Dec. 2018.
[75] C. Khammassi and S. Krichen, ``A GA-LR wrapper approach for feature selection in network intrusion detection," Comput.Secur., vol. 70, pp. 255_277, Sep. 2017.
[76] J. McCall, ``Genetic algorithms for modelling and optimisation," J. Com-put. Appl. Math., vol. 184, no. 1, pp. 205_222, Dec. 2005.
[77] H.Wang, J. Gu, and S.Wang, ``An effective intrusion detection framework based on SVM with feature augmentation," Knowl.-Based Syst., vol. 136, pp. 130_139, Nov. 2017.
[78] V. L. Thing, ``IEEE 802.11 network anomaly detection and attack classi_-cation: A deep learning approach," in Proc.WirelessCommun. Netw.Conf.(WCNC), May 2017, pp. 1_6.