Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6– No.10, April 2017 – www.caeaccess.org

A Survey of Wireless Sensor Network Attacks

Ahmed S. Elqusy
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

Salah E. Essa
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

Ayman EL-Sayed
Computer Science & Eng. Dept.,
Faculty of Electronic Eng.,
Menoufia University, Menouf
32952, Egypt

ABSTRACT
There are a lot of application using wireless sensor network, including using in enemy environment. One of the most valuable issues in any WSN is security. The purpose of this paper is to study the security attacks and the defense mechanism over WSN. Trust Management will be clarified and its importance in security.

Keywords
Wireless Sensor Networks, Security Defense mechanisms, attack's types.

1. INTRODUCTION
A wireless sensor network (WSN) is a self-configuring network of tiny sensor nodes communicating with each other using radio frequency, and used in quantity to sense, monitor and understand the physical world. Sensor are outfitted with processor in different modes (sleep, idle, active), source of power (AA or coin batteries, sunlight based boards), memory which is utilized for storing program code and memory buffering, the data is sent using radio frequency to be stored in specific site and finally sensors with specific function like humidity, light , temperature, and so forth. WSNs give an extension between the physical and virtual universes and permit the capacity to watch the beforehand inconspicuous at an accurate resolution over vast spatiotemporal ranges. They have an extensive variety of applications.

As in [71], WSNs can be utilized as a part of taking after circumstances *Environmental applications*: Forest fire discovery, Seismic Monitoring, Flood location, computerized agribusiness, and Ecological living space observing. *Military applications:* Monitoring hardware, Battlefield reconnaissance, Nuclear, natural and compound assault identification, Target following, and Monitoring adversary powers. *Health applications*: Remote checking of physiological, and information Disease counteractive action. *Home applications*: Home security, Home automation, and Fire detection. *Commercial applications*: the control of environmental in up to date and office structures, and office buildings, commercial and industrial sensing over network. Traffic flow surveillance, and Vehicle following.

There are many reasons that make individuals like wireless sensor network that are rundowns as take after [50]: Network arrangement can be done without settled framework, Suitable for the non-reachable places, for example, over the ocean, mountains, rustic zones or profound woods, Flexible if there is irregular circumstance when extra workstation is required, Implementation estimating is modest, It dodges a lot of wiring, It may oblige new gadgets whenever, It's adaptable to experience physical parcels, and It can be gotten to by utilizing a concentrated monitor.

As indicated by the significance utilization of WSN particularly in the military fields, security ought to be given to guarantee the accompanying administrations, for example, *Data Confidentiality* which implies the capacity to disguise messages from a latent aggressor so that any message conveyed through the sensor arrange stays classified [24,59], *Data Integrity* which guarantee the collector that the got information is not modified in travel by a foe, *Data Freshness* which infers that the information is later, and it guarantees that an enemy has not replayed old messages, *Availability* figures out if a node can utilize the assets and whether the network is accessible for the messages to impart, *Self-Organization* which implies that the nodes in a WSN self-organize out among themselves for multi-hop directing as well as to carryout scratch administration and creating trust relations [34]. Most sensor system applications depend on some type of time synchronization. Besides, sensors may wish to register the end-to-end defer of a packet as it goes between two sensors which are pair-wised [73]. *Secure Localization* frequently, a sensor network intended to find errors so it will require precise area data to pinpoint the area of an error, *Authentication* which guarantees the unwavering quality of the message by distinguishing its root and confirms the character of the senders and collectors, *Non-repudiation* must be given as it keeps an element from denying past responsibilities or activities [12].

This paper is arranged as follow: The taxonomy of WSNs security attacks, and the protection mechanism opposite to each type of attacks are proposed in section 2. In section 3, the trust management concept for WSN have been discuss. After that, in Section 4 the open points in the field of WSN security. Finally, the conclusion of the works presented in section 5.

2. TAXONOMY OF SECURITY ATTACKS IN WSN
Attacks in Wireless sensor networks can be classified into the following categories and shown in Fig 1.

2.1 Attacks against privacy
The importance of maintaining the privacy of the data WSN is a matter of very difficult [10]. Moreover, the enemy of the data that seem simple to extract sensitive information if he knows how to collect data from multiple nodes Assembly may collect sensor. Here are some common attacks on Sensor Data Privacy:

Eavesdropping and passive monitoring: In this attack, the detection of the attacker from the contents of the communication by listening / trying to hide data by intercepting which means the exploitation of WSNs nature of wireless transmission medium, or by using a powerful and resources of powerful hardware, such as well-designed

antennas and robust receiver. Which leads to serious consequences, such as launching other attacks (the hole, the black hole), and extract sensitive information WSN, delete and protect privacy and limit data confidentiality [11].

Secondly *Traffic analysis:* The pernicious node could make network traffic analysis to determine the node which have high activity in the network. Once the sensor nodes are discovered that it is very active, the malignant nodes could cause damage to the sensor nodes [7].

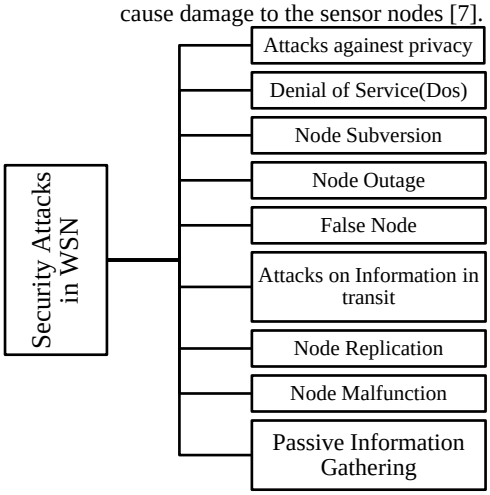

Fig 1: Classification of Security Attacks in WSN

At last, *Camouflage Adversaries:* Malicious nodes could be hidden in the network of sensors that masquerading as a regular sensor nodes. Therefore, they fool the sensors and other groups to attract packets of data from them. After Packet receiving, the malicious node could do two folded actions which are misroute the packet or drop the packets of data at the end. [7].

Defenses- *Eavesdropping* is a passive behavior, thus it is rarely detected. However, using the disclosure of misconduct can be disclosed techniques. Defenses key steps against eavesdropping is to add access control mechanism to the network, reducing the sensor data details, using distributed processing, adding restrict access, and utilize of robust encryption techniques.

To defend against *traffic analysis* attack in WSN, Deng, Han and Mishra proposed a mechanism in [15]. Two categories of attacks identified traffic analysis in WSNs: rate monitoring attack, and time correlation attack. Finally, to protect the network of *camouflage* several mechanisms has been presented. It discusses some of which are as follows: the mechanisms of anonymity are the mechanisms accurate information to enable accurate identification of the user. This poses a serious threat to privacy. One way to deal with this problem is to make the data anonymous source. Mechanism of anonymity depersonalizes data before they are released from the source. The second mechanism is based on the defense of the mechanisms and political decision-making and access control and authentication methods based on a defined set of privacy policies. Molnar and Wagner showed the concept of private documents in the application of radio frequency identification (RFID) domain [13]. Others suggested that the mechanism based on a policy for the protection of information of sensors, can be relied upon the privacy of the computer within the car which represent as a trusted agent for the location secrecy [14]. A different standards for access control that enables policies that have been identified in the mobile network framework has been proposed by Snekkenes in [62].

2.2 Dos Attacks.

Denial of service (DoS) [26] happens when hinder or disrupt the event or eliminates the network ordinary activities. Indeed, any type of efforts from the enemy to disrupt , destroy, or sabotage the network or its ability to do its ordinary activity which is expected and fulfill the desired level of performance, and which can be named a denial of service attack [16]. And the types of DoS attacks will be discussed below as shown in Figure 2

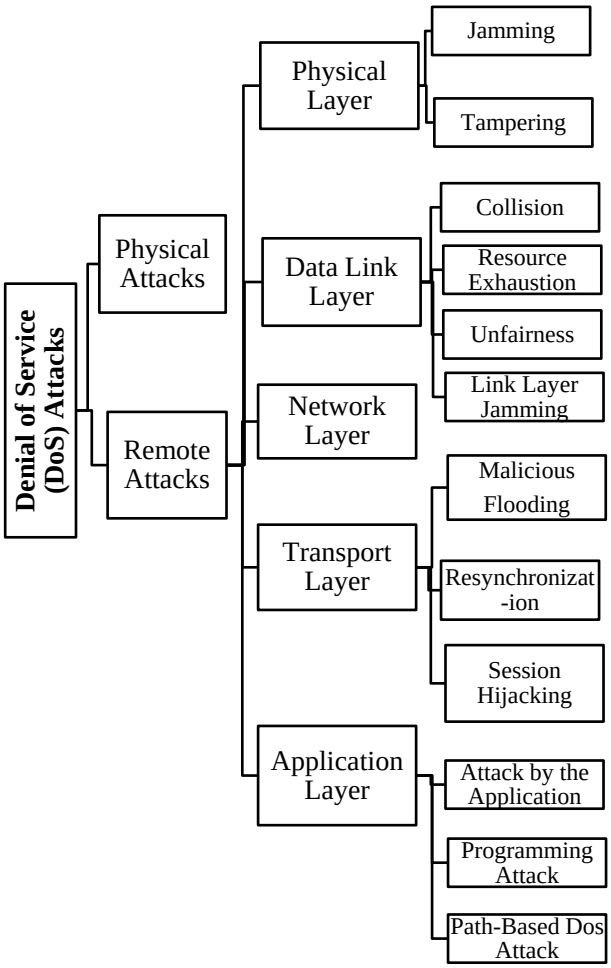

Fig 2: Classification of DoS Attacks

2.2.1Physical Attack

In this kind of attack, it is likely to achieve full dominance of the sensor node by direct access in physical way. This attack could destroy a node physically by changing the content of its memory. Other result of this, the attacker could then have unrestricted access to the network.

Defenses- For protecting from physical assault as possible, the sensor could be supported with extended device [17]. Many researchers suggested mechanisms that focus on building hardware tamper proof so that, the contents of memory chip on a sensor cannot be accessed from outside [18, 19, and 20]. It can also deploy special software and

hardware for the purposes of the node outside the sensor to detect physical tampering.

Hardware way: self-destruction of a node is an effective mechanism to hold possible theft of data in the case of a physical assault. The main idea for this situation is that when a sensor node senses there is an attack it destroy itself and eliminate all data and keys stored in its memory. Sastre has proposed a new technique which is called ECHO protocol in order to make location verification of the nodes in Wireless sensor network secure and more reliable [21]. In [22], the mechanism of defense against physical attacks, as proposed by the authors include two phases. In the first stage, the sensor nodes detect the attacker and transmit a messages in WSN to notify that there is an attack. In the second phase, the sensors that receive notification messages activate the switch off mode in order to protect themselves.

Software way: Deng and others present a mechanisms to protect the various sensors through the equipped of the proposed elements of the outside [23].

2.2.2 Remote Attacks

2.2.2.1 Attacks at Physical Layer

Jamming: WSNs is based on radio transmission media shared among network nodes. Jamming or radio interference considered as a common threat. It is easy to be implemented as the attacker needs only to capture the frequency used in the wireless network [26].

Tampering: Sensor networks regularly work in outside conditions. Because of unattended and circulated nature, the nodes in a WSN are exceedingly helpless to physical assaults [28]. The enemy can separate cryptographic keys from the caught node, alter its hardware, change the program codes or even supplant it with a malignant sensor [22].

Defenses- A few systems are projected for making certain against electronic jamming, as an example, *Spread Spectrum*:

FHSS is responsible of transmission radio signals by exchanging a transporter quickly among varied repeat channels with a pseudo-random grouping noted to each transmitter and recipient. In DSSS completely different bits are used to talk to distinctive signal with spreading code, *Mode Change*: If sensing element nodes utilize remote or infrared correspondence modes, they'll amendment the communication ‘s tactic, *Priority Messages*: At the moment of discontinuous jamming, it's transmit by the node to the base station for asserting the assault event, *Lower Duty Cycle*: sensing element nodes amendment to low power mode and moderate the maximum amount of power as possible, *Region Mapping*: The jamming areas evaluated and gatherings are created with jamming nodes by jammed region mapping strategy. On the off probability that sensing element nodes determine solid jamming signals within the running channel, the working channel will be changed with them [4]. The discovery of Tamper Attack conceivable through disconnection of sensor node, node devastation and notice misconduct of the node in network. The protective mechanism is enhancing and utilizing crypto-processors and deploying standard precautionary measures in network. Encourage the physical security of node and vindictive node identification strategies are shielding the network from these assaults. Additionally, Tamper Proofing - vaporize memory substance to forestall data spillage, and Hiding node which hide the sensor nodes into some different items can be utilized as resistance way [4].

2.2.2.2 Attacks at Data Link Layer

Collisions: It happens when two nodes endeavor to send on a similar recurrence at the same time [17]. At the point when packet impact, they are disposed of and need to re-transmit. An enemy may deliberately bring about impacts in particular packet, for example, ACK control messages. Rehashed crashes can likewise be utilized by an assailant to bring about exhaustion of resources [17].

*Resource exhaustion**:*** Repeated impacts rises weariness of resources since sender node will continue resending packet that crashed with each other. In the event that these pointless transmissions can't be ceased, the energy of the transmitting node and the nodes along the way to the collector will diminish at a disturbing rate.

Unfairness: The assailant may fall back on the previously mentioned link layer assaults haphazardly in a way with the end goal that nodes may miss deadline of transmission. An aggressor dependably tries to debase the execution of the network that may at last at some point prompt to violation. [26]

Link layer jamming: As indicated by results in link-layer jamming [28] [29], brilliant jammers can exploit the data link layer to accomplish energy efficient jamming. In the prior work [28], it was demonstrated that S-MAC can be jammed energy productively through jamming the control period of the listen term alone [28].

Defenses- A regular guard against *Collision Attack* is the utilization of error amending codes [17]. It amends some error bits amid at time of transmission [4]. Most codes work best with low levels of crashes, for example, those created by ecological or probabilistic mistakes. It is sensible to expect that an assailant will dependably have the capacity to damage more than what can be fixed. For *Energy Exhaustion Attack*, a conceivable technique is to apply a rate constraining MAC confirmation control. It disregards unreasonable demands and avert seepage of energy of rehashed transmission [4]. Another procedure is to utilize time division multiplexing where every node is distributed a schedule opening in which it can transmit [17]. To ensure against *Unfairness*, MAC protocols at link layer regulate the communication in networks by compelling seniority techniques for consistent relationship. It is conceivable to utilize these protocols consequently influencing the priority techniques, which eventually brings about services diminishing [27]. In [17] the author provides a method called Small frames, which make any node involve the channel for a little time length. For *Link Layer Jamming Attack*, there are a few guards, for example, Jam-Buster [30] proposed the accompanying Functions: Multi-bloc payloads Randomization of wake-up times, utilizing level with size packets to avert Schedule expectation assault, SAD-SJ [9] proposed a few approaches to relieve transmitting noxious signals amid spaces of the super frame. That are Random stage of times slot, and Network dynamicity management, and SMAC [32] displayed Schedule exchanging, and Data disclosing which ensure against Data packet jamming , CTRL interval jamming , and finally Listen interval jamming.

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 6– No.10, April 2017 – www.caeaccess.org

2.2.2.3 Attacks at Network Layer

There are many sorts of network layer assaults that are presented in figure 3. Brief clarify of every one as takes after:

Attacking Routing Information: Routing information is the most vital segment of routing in any network. If the routing information is disregarded, an assault might be executed specifically in the network layer. Such assaults would hinder stream of movement in the network. Interruption in typical stream might be brought about by different means like spoofing, adjusting or notwithstanding replaying routing data [31]. Disturbances may bring about routing loops, changing routes, and parceling of the network and an expansion in passivity.

Replayed Information Attack: It is an assault exist in WSN for the packet stream recording. This helping in the reuse of the packet all together access critical data of the network. The encryption systems additionally can't keep this sort of assaults as it can record and play the packet on the fly. This is the reason this assault permit illicit access to critical information [5].

Sinkhole Attack: The principle point of this assault is to persuade all the activity from a unique network by unmasking a node and making a puncture at the base station [35]. This unmasking hole appreciates routing techniques in which this assault can act. Because the data gave by the node contain hardness. This sort of assault is difficult to be counted.

Figure 2: Network Layer Attacks

Wormhole Attack: In this assault the aggressor answer over a system in which faint latency association between two sections contain messages which are a wormhole [42]. Coordinate node acknowledges this sorts of connection and direct the messages between two non-neighboring nodes which are contiguous each other, or by a couple of nodes which are in various groups in a network so they can speak with each other. Both sinkhole and wormhole assault have alike capacities.

Sybil Attack: This sort of assault characterizes a condition in which a personality of the network shows higher. This kind of attack effectively goes under the impact of the fault-tolerant arrangements, storage allocation and topology of network which are conventions and calculations [45]. One of the illustrations is an arrangement of conveyed storage. There are three classes which are an imitation of this sort of information developed. It consist of three nodes in which unmasked node is one of the two nodes can undoubtedly limit the repetition.

Hello Flood Attack: An assailant sends or replays a steering convention's HELLO packets starting with one node then onto the next with more vitality. This assault utilizes HELLO packets as a weapon to persuade the sensors in WSN. The sensors are affected that the foe is their neighbor. Thus, while sending the data to the base station, the casualty nodes attempt to experience the assailant as they realize that it is their neighbor and are at last caricature by the aggressor. [51]

Selective Packet Forwarding Attack: A malevolent node can specifically drop just certain packet. Particularly compelling if joined with an assault that assembles much movement by means of the node. In sensor network, it is expected that nodes reliably forward got messages. Yet, some unmasked node may decline to forward packets, however neighbors may begin utilizing different route. [51]

Acknowledgement Spoofing Attack: several routing algorithm for wireless sensor network need send of affirmation packets. An assaulting node may catch packet sends from its neighboring nodes and farce the affirmations consequently giving false data to the nodes [35]. Along these lines, the assailant can spread wrong data about the status of the nodes.

Looping (Vampire Attack): A few routes shape loops or reroutes. These assaults are refined kinds of DoS assaults. Bringing about loops is not more proficient than simply dropping or disposing of packets; creating makeshift routes is a wasteful method for squandering the sensor nodes' vitality. There are two sorts of looping [58]: Carousel assault, and Stretch assault.

Misdirection Attack: Misrouting the got packets or movement streams in one heading to a remote node. It occurs by Generating incorrectly messages, trip data alteration, manufacture, replication, or dispose of. Which prompts to Packets confusion, flooding its system connection, and wrong routing tables (false routing data). [11]

Rushing Attack: In this kind of assault a fast communicate the bogus advertisings of route demand through the WSN [64]. An aggressor abuses copy concealment in communicates to smother real packet by rapidly sending its own packets. This happen through sending route asks for more rapidly than any ordinary nodes [64].

Homing Attack: In this assault the aggressor do Regular movement checking and breaking down the messages exchanged, correspondence examples and sensor nodes exercises which recognizing and find basic assets that give basic/indispensable administrations to the WSN this prompts to dispatch the dynamic assault. This assault has the accompanying impacts, Identifying, find and crush basic resources, removing the touchy system data, propelling dynamic assaults (wormhole, blackhole, sinkhole) [11], and debilitate information classification and security.

Neglect and greed attack: Noxious node drop approaching packets, haphazardly or discretionary (careless node). Vindictive node gives undue need to its own messages

(insatiable node). Which prompts to reliably debase or square Traffic, Packet drop/misfortunes, Influencing/constraining the WSN Traffic, and Low dependability. [11]

Blackhole Attack: A black hole is a vindictive node that draws in all the activity in the network by promoting that it has the briefest way in the network [38]. Along these lines, it makes an allegorical black hole with the pernicious node or the foe at the middle. This black hole drops every one of the packets it gets from alternate nodes.

Grayhole Attack: A grayhole assault is a variety of black hole assault in which the nodes specifically drops packets [61]. There are two routes in which a node could drop packets which are leave all UDP packets while send all TCP packets, and not receive half of the packets or can drop them with probabilistic dissemination.

Defenses- a way to protect the network from *routing information Attack* is to attach a message authentication code (MAC) to the end of the message. After attaching a MAC to the message, the recipients can confirm whether the messages have been ridiculed or changed [33].A counters or time-stamps might be bestowed in the messages to protect against *Replayed Information threat* [24]. A conceivable barrier against *Selective Forwarding* Attack is utilizing numerous path to send information [35]. Another protection is to distinguish the pernicious node or accept it has fizzled and look for an elective route. One type of protocols impervious to *Sinkhole Attack* is geographic routing protocol. Geographic protocol develop a topology on request utilizing just limited collaborations and data and without start from the base station [3]. To defend against *Wormhole Attack* the approach of Packet Leashes is utilized. A Leash is an additional snippet of data that is added to a packet to limit its most extreme travel separate. There are two sorts of leashes: geographical leashes and temporal leashes. A geographical leash [43] guarantees that the beneficiary of the packet is inside a specific separation from the transmitter [43]. In *True Line approach*, True Link is a defense which ensures against *wormhole assault* utilizing the blend of two stages: meet stage and confirmation stage. True link considers two nodes i and j. In the meet stage, i and j trade haphazardly produced numbers known as a nonce [44]. A guard method against *Sybil Attack* is Trusted confirmation strategy accept that there is a unique put stock in outsider or focal specialist, which can check the legitimacy of every member, and further issues a certification mechanism for the fair one [46]. Such testimony can be a unique equipment gadget [47] or a digital number [48]. Take note of that basically both are a progression of digits present on various Medias. Prior to a member joins a peer-to-peer network to give votes or to acquire its services, this identity should first be confirmed [49]. For *Hello Flood Attack*, Multi-way multi-base station information sending procedure is presented in [52], in which a sensor node keeps up number of various keys in a numerous tree. In [53] author proposes that *Hello flood attack* can be neutralized by utilizing "identity check convention". Considering the shortage of energy resources of sensor nodes, the author have presented in [54] a probabilistic based approach, that strengths few haphazardly chose nodes to answer to base station about Hello demands. In [55] a cryptographic method is utilized to keep the Hello Flood assault. Any two sensors have a similar key. Each new encryption key is produced on fly amid the correspondence. Yet, the fundamental disadvantage of this approach is that any aggressor can parody its identity and after that create assaults. To avoid attack like *Selective Packet Forwarding Attack*, multipath routing can be utilized. data directed through path whose nodes are totally disjoint are totally secured against selective forwarding attack including at most traded off Allowing nodes to progressively pick a packet's next hop probabilistically from an arrangement of conceivable applicants can additionally decrease the odds of a foe increasing complete control of an information stream [56].*Acknowledgement Spoofing Attack* can be forestalled by utilizing good encryption strategies and appropriate confirmation for correspondence [57]. To protect from *Looping Attack* the author in [2] presented a way amid rout disclosure stage the limit idea is used for trusted nodes evaluate. In *Misdirection Attack*, there are a few location procedures which are misbehavior detection techniques, various leveled steering system, tree-way directing Protocols, and utilizing a jump tally restrain. To keep this assault there are likewise barriers ways which are utilizing hierarchical routing, Authorization [60], Monitoring [60], Central endorsement expert, Pair-wise confirmation, Network layer validation, Adopt approval strategies, Acknowledgment check. There are two sorts of location against *Rushing Attack* which are assessing the Route Discovery [64], And Misbehavior recognition strategies. Likewise, there are a few safeguards ways like expelling postponements, an arrangement of nonexclusive systems that together protect against the *Rushing Attack*, are [64] Secure Neighbor Detection, and Secure Route, Randomized sending of Route Request, and Delegation. Bad conduct discovery methods is utilized to recognize *Homing Attack*. To resistance against it get to control, Reduction in detected information subtle elements, Distributed preparing, Strong encryption systems, And Hiding utilization of shared cryptographic keys are utilized [11]. To ensure the system against *Neglect and Greed assault* researcher ought to utilizing Multi-path routing, sending excess messages, testing, repetition [60] and customary checking. Utilizing other conceivable courses, powerfully and probabilistic pick packet's next jump, utilizing combinational techniques, or Adopt multi-bounce steering and bidirectional connection confirmation [11]. There are two kind of protection component against *blackhole assault* which are: REWARD is a directing strategy where a wireless sensor network is sorted out as a dispersed information base to distinguish black hole assault. The disseminated data base keeps up a record for suspicious nodes and territories. This routing calculation comprises of two sorts of communicate messages, MISS (material for intersection of suspicious sets) and SAMBA (suspicious area, mark a black-hole attack) [40]. Another system is Path based Detection Algorithm. In this approach, a node observes just the following jump neighbor in the present route path instead of watching each node in the neighbor [41]. To execute the algorithm, each node keeps up an FwdPktBuffer (packet digest buffer). To secure against *Grayhole Attack* there is a strategy called CHEMAS (Checkpoint-based Multi-Hop Acknowledgment Scheme): This technique utilizes three sorts of packets: event packet, ACK packets and alert packets [63]. This plan depends on checkpoint-by-checkpoint affirmation rather than hop-by-hop affirmation. The fundamental thought of this scheme depends on checkpoint nodes which are chosen from the piece of moderate nodes. The path is partitioned into a few sections which comprise of sending way between two checkpoint nodes. At the point when the source node identifies an

exceptional occasion, it creates an event packet. The packet crosses hop-by-hop towards the base station and each middle of the road node spares the event packet in its memory before sending it downstream. At the point when the checkpoint nodes get the event packet it produces an ACK packet and sends it to upstream neighbor. The ACK packet cross the same but switched way upstream. It crosses no less than two fragments before being dropped by an upstream checkpoint. Consequently, all the middle nodes in these two checkpoints realize that past event has securely landed in the downstream checkpoint. In the event that the ACK packet is not gotten from downstream by every one of the nodes in these two portions, then the following downstream neighboring node is cleared as suspicious and the alert packet is created.

2.2.2.4 Attacks at Transport Layer

Malicious Flooding Attack: When a protocol is needed to keep up state at either end of a connection, it gets to be distinctly helpless against memory exhaustion by flooding [17]. An assailant may over and over make new connection ask for until the assets required by every connection are depleted or achieve a most extreme breaking point. In either case, additionally genuine requests will be overlooked.

Resynchronization Attack: The aggressor modify the sequence number of packets to disturb the protocol of communication. Confirmation of packets might be a conceivable solution [26].

Session Hijacking Attack: Session hijacking exploits the way that almost all communication are secured (by giving certifications) at session setup, but not from there on. In the TCP session capturing assault, the assailant parodies the casualty's IP address, decides the right sequence number that is normal by the objective, and afterward plays out a DoS assault on the casualty. Along these lines, the aggressor imitates the casualty node and proceeds with the session with the objective. Hijacking a session over UDP is just as over TCP, aside from that UDP assailants don't need to stress over the overhead of overseeing sequence numbers and other TCP systems. Since UDP is connectionless, edging into a session without being distinguished is significantly simpler than the TCP session assaults [66].

***Defenses*:** To guard against the *Attack of Malicious Flooding* at the transport layer, Aura et al have presented a technique utilizing client confuses [65]. The fundamental thought is that each interfacing client ought to show its dedication to the connection by tackling bewilder. As an assailant in most probability, does not have unbounded resource, it will be unimaginable for him to make new connection sufficiently quick to bring about resource starvation on the serving node. A conceivable barrier against *Re-synchronization Attack* is to uphold a compulsory prerequisite of validation of all packets imparted between nodes [17]. On the off chance that the verification mechanism is secure, an assailant will be not able send any mock messages to any goal node [4]. To ensure against *Session Hijacking Attack* the author in [4] utilizing session binding proxy which takes SSL/TLS session-aware confirmation and inverts proxy. In the event that a client having a session ID initially and it sends solicitations to the intermediary, then the intermediary transfers the solicitations to the server back-end application.

2.2.2.5 Attacks at Application Layer

Attack by the Application: An application may create many messages, for example, control and alarm passed on to send nodes, along these lines producing enormous activity in the network. Cutoff points might be put on the quantity of ready messages or sifting might be connected to such messages subsequent to checking a few parameters for legitimacy [26].

Programming Attack: nodes might be reconstructed in extraordinary cases. This might be finished by sending false projects to nodes. This kind of assault might be countered by checking respectability of the got program [26].

Path-based Denial of Service Attack: The path as often as possible utilized by nodes for information packets to achieve base stations might be utilized for sending expansive number of counterfeit information packets. The nodes will dependably stay occupied and some of the time deplete their assets in sending these packets, subsequently denying real packet activity [26].

***Defenses*-** The accompanying countermeasure can be used to secure the WSN programming and be shielded from being misused by malignant clients: Software verification and approval, e.g. Remote software-based attestation for sensor systems, characterizing precise trust limits for various parts and clients, utilizing a confined domain, for example, the Java Virtual Machine, dynamic run-time encryption/unscrambling for software, excluding that the code running on the gadget is scrambled, Exploiting the product, and equipment confirmation. The trusted figuring bunch stage and cutting edge secure processing base give this sort of validation. A comparable model could be utilized as a part of sensor systems [3].

2.3 Node Subversion

Catch of a node may uncover its data including exposure of cryptographic keys and along these lines trade off the entire sensor network. A specific sensor may be caught, and data (key) put away on it may be acquired by an enemy [67].

***Defenses*-** the author in [68] presented an ECC based convention is appropriate for remote sensor systems, and furthermore proposed conspire gives shared validation and a mystery session key for communication. Which increment the strength of the node against node corruption.

2.4 Node Outage

Node blackout is the circumstance that happens when a node stops its services. It is to a great degree unsafe particularly when this node is a group pioneer [67].

***Defenses*-** For the situation where a Cluster head quits working, the sensor protocol of the network ought to be sufficiently vigorous to moderate the impacts of node blackouts by giving a backup route of action.

2.5 False Node

A false node includes adding of a node by an enemy and causes the infusion of malignant information. Noxious code infused in the system could spread to all node, possibly decimating the entire network, or far and away more terrible, assuming control over the network for the benefit of a foe [69].

Defenses- The proposed scheme in [68] utilizing a protocol of asymmetric encryption which shields the system from false node risk.

2.6 Attacks on Information in transit

In a sensor network, sensors screen the progressions of particular parameters or values and answer to the sink in accordance with the necessity. During sending the report, the data in travel might be adjusted, satirize, replayed once more, or vanished. Any aggressor can screen the movement stream and get enthusiastically to interfere with, capture, alter or manufacture bundles along these lines, give wrong data to the base stations or sinks [70].

Defenses- data gathering and authentication mechanisms may counteract it [1].

2.7 Node Replication

In this attack, an aggressor endeavors to add a node to a current WSN by replication (i.e. duplicating) the node identifier of an officially existing node in the network [72]. A node repeated and participated in the system in this way can conceivably bring about extreme interruption in message communication in the WSN by ruining and sending the packets in not correct routes.

Defenses- A system for dispersed discovery of node replication assaults have presented by Parno, Perrig and Gligor in [72]. They have used two techniques which work by the aggregate activities of various nodes. The algorithm are: Randomized multicast calculation disperses area data of a node to haphazardly chose witnesses, misusing birthday conundrum to recognize reproduced nodes, and Line-selected multicast utilizes the system structure to replication distinguish.

2.8 Node Malfunction

A malfunctioning node will create off base information that could uncover the uprightness of sensor network particularly in the event that it is an information gaining node, for example, a cluster head [67].

Defenses- A double weighted trust evaluation (DWE) which has been propose in [6] that plan to recognize noxious nodes despite flaws in a various leveled sensor network, where sensor nodes report their readings to a sending node for conglomeration

2.9 Passive Information Gathering

An enemy with intense assets can gather data from the sensor network in the case that it is not scrambled. An interloper with well-designed antennas and a suitably intense receiver can without much of a stretch pick off the information stream. Block attempt of the messages containing the physical areas of sensor nodes permits an assailant to find the nodes and decimate them [74].

Defenses- To abstain from overpowering measures of movement, the detected qualities [55] must be accumulated back to the base station. As the framework may ascertain the normal the temperature of a geographic area. With the assistance of evacuating excess information, information collection [51] can incredibly lessen vitality utilization. As a rule, [8], when outlining a protected information accumulation convention, the essential goal is to devise a safe total capacity that registers the information totals safely and the auxiliary target is to guarantee that other than the sink and the sources, middle of the road nodes ought not have any learning of the collection result or the raw data.

3. TRUST MANAGEMENT

Trust is an old however essential issue in any networked environment [70]. Trust can take care of a few issues past the force of the customary cryptographic security. For instance, judging the sensor nodes nature and the nature of their administrations, and giving the equivalent access control. The trust administration is the way to assemble trusted, tried and true wireless sensor network applications. In any case, it is difficult to manufacture a decent trust display inside a sensor arrange given as far as possible. Trust administration plans are arranged into three classifications: centralized, distributed and hybrid as shown in Figure 4.

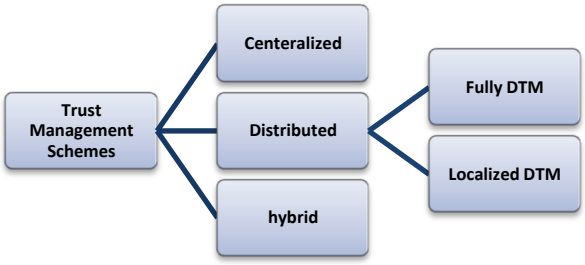

Figure 4: Trust management schemes classification.

3.1 Centralized Trust Management (CTM) Schemes

It comprises of a solitary all inclusive trusted server that decides the trust estimations of each node in the system. This gives the advantage of lesser computational overhead at the sensor node in the fact that the plurality of the trust figuring is performed at brought together trusted server that has no imperatives of computational power and memory. Also, It has the disadvantages, a solitary purpose of disappointment, which makes it minimum dependable, it smothers the hidden certainty that distinctive nodes may have diverse trust values about a given node, for extensive scale sensor networks, brought together trust plans are not appropriate, and Centralized approach presents huge correspondence overhead in the WSN.

3.2 Distributed Trust Management Schemes

There are two types of DTM schemes.

3.2.1 Fully DTM

In these technique, every sensor node keeps up its own particular trust record and that gives the advantage of less communication overhead. Additionally, it is more solid than the centralized one since it has no single purpose of disappointment. In any case, it doesn't function admirably for vast scale sensor arranges, each node locally ascertains the trust estimations of every single other node in the network that builds the computational cost, every node needs to keep up an exceptional record about the trust estimations of the whole system as a table, and the span of the table is straightforwardly corresponding to the measure of the network which brings about an expansive memory utilization.

3.2.2 Localized DTM

Which Sensor nodes just keeps up the trust an incentive about its neighboring nodes as it were. Which is reasonable to be utilized as a part of Wireless sensor network the significant downside of the confined DTM approach is that it presents deferral and reliance at whatever point any node needs to assess trust of far off nodes.

3.3 Hybrid Trust Management (HTM) schemes

Has the feature of both distributed and centralized approaches. This plan is utilized with clustering schemes, in which cluster head goes about as a focal server for the entire group. These plans reduce the cost related with trust assessment when contrasted with circulated methodologies and it is more dependable than the centralized one but less solid than the distributed one. Be that as it may, it presents more communication overhead in the network when contrasted with the disseminated one.

4. DISCUSSION

Despite the fact that research endeavors have been made on security detection and protections in WSNs, there are still a few difficulties to be tended to. Firstly, the choice of the proper security guards relies on upon the preparing capacity of sensor nodes, demonstrating that there is no compelling answer for all assaults sorts in sensor network. Rather, the security mechanisms are profoundly application-specific. Secondly, the vast majority of the present security mechanisms accept that the sensor nodes and the base station are fixed. Nevertheless, there might be circumstances, for example, battlefield environments, where the base station and perhaps the sensors should be movable. The portability of sensor nodes affects network topology and along these lines brings many issues up in the security mechanisms. Despite the fact that, WSN has many favorable circumstances and utilized as a part of numerous applications yet it is as yet having some open focuses that must be shrouded later on looks into, for example, *Memory constraints*: A sensor is a minor gadget with just a little measure of memory and storage room. There is generally insufficient space to run muddled calculations, *Unreliable Communication:* Certainly, inaccurate communication is another risk to sensor security. The security of the system depends vigorously on a characterized protocol, which thusly relies on upon communication, *Unreliable Transfer:* the packet-based routing of sensor systems depends on connectionless protocols and therefore innately capricious. The capricious wireless communication channel might prompt to harmed or ruined packets, *Conflicts*: although the channel is dependable, the communication may in any case be not true. This is because of the broadcast way of the wireless sensor network. On the off chance that packets meet amidst exchange, clashes will happen and the exchange itself will fail down, *Energy constrains*: Energy is the greatest requirement for a WSN. As a rule, vitality utilization in sensor nodes can be ordered in three sections: sensor transducer energy, energy needed for communication among nodes, and energy required for computation in the microprocessor. The computation is less cost than communication in WSNs. The additional power devoured by sensor nodes because of security is identified with the handling required for security capacities (e.g., encryption, decryption, signed information, checking marks), *Latency*: The multi-hop routing, network blockage and node preparing can prompt to more prominent inertness in the network, in this manner making it hard to accomplish synchronization among sensor nodes [37], and *Unattended Operation of Networks*: In many cases, count on the capacity of the specific sensor network, the sensor nodes might be left neglected for drawn out stretches of time. This makes security in WSNs an especially troublesome task. There are three primary provisos to neglected sensor nodes that depict underneath: Exposure to Physical Attacks, Managed Remotely, and No Central Management Point. The outline of security administrations in WSNs must fulfill these requirements.

5. CONCLUSION

In this paper, the generic idea of wireless sensor network and security in WSN have been proposed. Recent research up till now spotlight on the wireless sensor network security. There is various mechanism of security that applies in our network as our network is more prone to failure. Also so many attacks that occur in sensor network and apply to sensor node have been discussed. Additionally, the most important issue in security is Trust management is also described. In the near future, a lot of attacks will be discussed which are harm the sensor network and sensor node, and a mechanism to stop it.

6. REFERENCES

[1] Brindha, P. and Senthil, A., 2016. Security on Wireless Sensor Networks: A Survey," (IJCSIT) International Journal of Computer Science and Information Technologies, 7(6), pp.2487-2490.

[2] Singh, R., Singh, J. and Singh, R., 2016. WRHT: A Hybrid Technique for Detection of Wormhole Attack in Wireless Sensor Networks. Mobile Information Systems, 2016.

[3] Kaushal, K. and Kaur, T., 2015. A Survey on Attacks of WSN and their Security Mechanisms. International Journal of Computer Applications, 118(18).

[4] Biswas, S. and Adhikari, S., 2015. A Survey of Security Attacks, Defenses and Security Mechanisms in Wireless Sensor Network. International Journal of Computer Applications, 131(17), pp.28-35.

[5] Radha, R. and Santhosh, S.,2013, October. A Novel Security Model for Preventing Passive and Active Attacks in WSNs. In Int. J. Adv. Res. Comput. Commun.

[6] Oh, S.H., Hong, C.O. and Choi, Y.H., 2012. A malicious and malfunctioning node detection scheme for wireless sensor networks. Wireless sensor network, 4(03), p.84.

[7] Virmani, D., Soni, A., Chandel, S. and Hemrajani, M., 2014. Routing attacks in wireless sensor networks: A survey. arXiv preprint arXiv:1407.3987.

[8] Jariwala, V. and Jinwala, D., 2012. A novel approach for secure data aggregation in wireless sensor networks.

[9] Tiloca, M., De Guglielmo, D., Dini, G. and Anastasi, G., 2013, September. SAD-SJ: A self-adaptive decentralized solution against Selective Jamming attack in Wireless Sensor Networks. In Emerging Technologies & Factory Automation (ETFA), 2013 IEEE 18th Conference on (pp. 1-8). IEEE.

[10] Gruteser, M., Schelle, G., Jain, A., Han, R. and

Grunwald, D., 2003, May. Privacy-Aware Location Sensor Networks. In HotOS (Vol. 3, pp. 163-168).

[11] Mohammadi, S. and Jadidoleslamy, H., 2011. A comparison of physical attacks on wireless sensor networks. International Journal of Peer to Peer Networks, 2(2), pp.24-42.

[12] Menezes, A.J., Van Oorschot, P.C. and Vanstone, S.A., 1996. Handbook of applied cryptography. CRC press.

[13] Molnar, D. and Wagner, D., 2004, October. Privacy and security in library RFID: Issues, practices, and architectures. In Proceedings of the 11th ACM conference on Computer and communications security (pp. 210-219). ACM.

[14] S. Duri, M. Gruteser, X. Liu, P. Moskowitz, R. Perez, M. Singh, and J. Tang, "Framework for security and privacy in automotive telematics", In Proceedings of the 2nd ACM International Workshop on Mobile Commerce, 2000.

[15] Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M. and Tang, J.M., 2002, September. Framework for security and privacy in automotive telematics. In Proceedings of the 2nd international workshop on Mobile commerce (pp. 25-32). ACM.

[16] Pathan, A.S.K., 2010. Denial of service in wireless sensor networks: issues and challenges. Nova Science Publishers, Inc.

[17] Wood, A.D. and Stankovic, J.A., 2002. Denial of service in sensor networks. Computer, 35(10), pp.54-62.

[18] Anderson, R. and Kuhn, M., 1996, November. Tamper resistance-a cautionary note. In Proceedings of the second Usenix workshop on electronic commerce (Vol. 2, pp. 1-11).

[19] Anderson, R. and Kuhn, M., 1997, April. Low cost attacks on tamper resistant devices. In International Workshop on Security Protocols (pp. 125-136). Springer Berlin Heidelberg.

[20] Kömmerling, O. and Kuhn, M.G., 1999. Design Principles for Tamper-Resistant Smartcard Processors. Smartcard, 99, pp.9-20.

[21] Sastry, N., Shankar, U. and Wagner, D., 2003, September. Secure verification of location claims. In Proceedings of the 2nd ACM workshop on Wireless security (pp. 1-10). ACM.

[22] Wang, X., Chellappan, S., Gu, W., Yu, W. and Xuan, D., 2005, October. Search-based physical attacks in sensor networks. In Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on (pp. 489-496). IEEE.

[23] Deng, J., Han, R. and Mishra, S., 2005. Security, privacy, and fault tolerance in wireless sensor networks. Artech House.

[24] Perrig, A., Szewczyk, R., Tygar, J.D., Wen, V. and Culler, D.E., 2002. SPINS: Security protocols for sensor networks. Wireless networks, 8(5), pp.521-534.

[25] Wang, X., Gu, W., Schosek, K., Chellappan, S. and Xuan, D., 2005. Sensor network configuration under physical attacks. In Networking and Mobile Computing (pp. 23-32). Springer Berlin Heidelberg.

[26] Mukherjee, N., Neogy, S. and Roy, S., 2015. Building Wireless Sensor Networks: Theoretical and Practical Perspectives. CRC Press.

[27] Akyildiz, I.F., Su, W., Sankarasubramaniam, Y. and Cayirci, E., 2002. A survey on sensor networks. IEEE Communications magazine, 40(8), pp.102-114.

[28] Law, Y.W., Hartel, P., den Hartog, J. and Havinga, P., 2005, January. Link-layer jamming attacks on S-MAC. In Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on (pp. 217-225). IEEE.

[29] Law, Y.W., Palaniswami, M., Hoesel, L.V., Doumen, J., Hartel, P. and Havinga, P., 2009. Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols. ACM Transactions on Sensor Networks (TOSN), 5(1), p.6.

[30] Ashraf, F., Hu, Y.C. and Kravets, R.H., 2012, October. Bankrupting the jammer in WSN. In Mobile Adhoc and Sensor Systems (MASS), 2012 IEEE 9th International Conference on (pp. 317-325). IEEE.

[31] Wang, Y., Attebury, G. and Ramamurthy, B., 2006. A survey of security issues in wireless sensor networks.

[32] Law, Y.W., Hartel, P., den Hartog, J. and Havinga, P., 2005, January. Link-layer jamming attacks on S-MAC. In Wireless Sensor Networks, 2005. Proceeedings of the Second European Workshop on (pp. 217-225). IEEE.

[33] Singh, G., 2016, April .Security Attacks and Defense Mechanisms in Wireless Sensor Network: A Survey. In IJISET - Int. J. Innov. Sci. Eng. Technol.

[34] Eschenauer, L. and Gligor, V.D., 2002, November. A key-management scheme for distributed sensor networks. In Proceedings of the 9th ACM conference on Computer and communications security (pp. 41-47). ACM.

[35] Karlof, C. and Wagner, D., 2003. Secure routing in wireless sensor networks: Attacks and countermeasures. Ad hoc networks, 1(2), pp.293-315.

[36] Malik, M., Singh, D.Y. and Arora, A., 2013. Analysis of LEACH protocol in wireless sensor networks. International Journal of Advanced Research in Computer Science and Software Engineering, 3(2).

[37] Stankovic, J.A., Abdelzaher, T.E., Lu, C., Sha, L. and Hou, J.C., 2003. Real-time communication and coordination in embedded sensor networks. Proceedings of the IEEE, 91(7), pp.1002-1022.

[38] Al-Shurman, M., Yoo, S.M. and Park, S., 2004, April. Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual southeast regional conference (pp. 96-97). ACM.

[39] Dokurer, S., 2006. Simulation of Black hole attack in wireless Ad-hoc networks. Atılım University.

[40] Karakehayov, Z., 2005. Using REWARD to detect team black-hole attacks in wireless sensor networks. Wksp. Real-World Wireless Sensor Networks, pp.20-21.

[41] Ajiwen, C.A.I., Ping, Y.I., Jialin, C.H.E.N., Zhiyang, W.A.N.G. and Ning, L.I.U., 2010.An Adaptive Approach to Detecting Black and Gray Hole Attacks in Ad Hoc Network. In 2010 24th IEEE International Conference on Advanced Information Networking and Applications.

[42] Yadav, S., Gupta, K. and Silakari, S., 2010. Security issues in wireless sensor networks. journal of information systems and communication, 1(2), p.1.

[43] Hu, Y.C., Perrig, A. and Johnson, D.B., 2003, April. Packet leashes: a defense against wormhole attacks in wireless networks. In INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (Vol. 3, pp. 1976-1986). IEEE.

[44] Eriksson, J., Krishnamurthy, S.V. and Faloutsos, M., 2006, November. Truelink: A practical countermeasure to the wormhole attack in wireless networks. In Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference on (pp. 75-84). IEEE.

[45] Choi, J.C. and Lee, C.W., 2006, September. Energy modeling for the cluster-based sensor networks. In Computer and Information Technology, 2006. CIT'06. The Sixth IEEE International Conference on (pp. 218-218). IEEE.

[46] Chang, W. and Wu, J., 2012. A Survey of Sybil Attacks in Networks. Sensor Networks for Sustainable Development.

[47] Newsome, J., Shi, E., Song, D. and Perrig, A., 2004, April. The sybil attack in sensor networks: analysis & defenses. In Proceedings of the 3rd international symposium on Information processing in sensor networks (pp. 259-268). ACM.

[48] Ledlie, J. and Seltzer, M., 2005, March. Distributed, secure load balancing with skew, heterogeneity and churn. In INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE (Vol. 2, pp. 1419-1430). IEEE.

[49] Douceur, J.R., 2002, March. The sybil attack. In International Workshop on Peer-to-Peer Systems (pp. 251-260). Springer Berlin Heidelberg.

[50] Bhattacharyya, D., Kim, T.H. and Pal, S., 2010. A comparative study of wireless sensor networks and their routing protocols. Sensors, 10(12), pp.10506-10523.

[51] Alzaid, H., Foo, E. and Nieto J.G., 2008, January. Secure data aggregation in wireless sensor network: a survey. In Proceedings of the sixth Australasian conference on Information Security-Volume 81 (pp. 93-105). Australian Computer Society, Inc.).

[52] Hamid, A. and Hong, C.S., 2006, February. Defense against lap-top class attacker in wireless sensor network. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 1, pp. 5-pp). IEEE.

[53] Giruka, V.C., Singhal, M., Royalty, J. and Varanasi, S., 2008. Security in wireless sensor networks. Wireless communications and mobile computing, 8(1), pp.1-24.

[54] Khozium, M.O., 2008. Hello flood countermeasure for wireless sensor networks. International Journal of Computer Science and Security, 2(3), pp.57-65.

[55] Rathod, V. and Mehta, M., 2011. Security in wireless sensor network: a survey. Ganpat University Journal of Engineering and Technology, 1(1), pp.35-44.

[56] Sharma, K. and Ghose, M.K., 2010. Wireless sensor networks: An overview on its security threats. IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs, pp.42-45.

[57] Shukla, J. and Kumari, B., 2013. Security Threats and Defense Approaches in Wireless Sensor Networks: An Overview. International Journal of Application or Innovation in Engineering & Management (IJAIEM), 2.

[58] Sharma, K., Ghose, M.K., Kumar, D., Singh, R.P.K. and Pandey, V.K., 2010. A comparative study of various security approaches used in wireless sensor networks. International journal of advanced science and technology, 17, pp.31-44.

[59] Carman, D.W., Kruus, P.S. and Matt, B.J., 2000. Constraints and approaches for distributed sensor network security (final). DARPA Project report, (Cryptographic Technologies Group, Trusted Information System, NAI Labs), 1(1).

[60] Sharma, K. and Ghose, M.K., 2010. Wireless sensor networks: An overview on its security threats. IJCA, Special Issue on "Mobile Ad-hoc Networks" MANETs, pp.42-45.

[61] Mohammadi, S. and Jadidoleslamy, H., 2011. A comparison of link layer attacks on wireless sensor networks. arXiv preprint arXiv:1103.5589.

[62] Snekkenes, E., 2001, October. Concepts for personal location privacy policies. In Proceedings of the 3rd ACM conference on Electronic Commerce (pp. 48-57). ACM.

[63] Xiao, B., Yu, B. and Gao, C., 2007. CHEMAS: Identify suspect nodes in selective forwarding attacks. Journal of Parallel and Distributed Computing, 67(11), pp.1218-1230.

[64] Hu, Y.C., Perrig, A. and Johnson, D.B., 2003, September. Rushing attacks and defense in wireless ad hoc network routing protocols. In Proceedings of the 2nd ACM workshop on Wireless security (pp. 30-40). ACM.

[65] Aura, T., Nikander, P. and Leiwo, J., 2000, April. DOS-resistant authentication with client puzzles. In International workshop on security protocols (pp. 170-177). Springer Berlin Heidelberg.

[66] Lupu, T.G., 2009, September. Main types of attacks in wireless sensor networks. In I. Rudas, M. Demiralp and N. Mastorakis eds., WSEAS International Conference. Proceedings. Recent Advances in Computer Engineering (No. 9). WSEAS.

[67] Pathan, A.S.K., Lee, H.W. and Hong, C.S., 2006, February. Security in wireless sensor networks: issues and challenges. In Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference (Vol. 2, pp. 6-pp). IEEE.

[68] Maharana, R. and Khilar, P.M., 2013. An improved authentication protocol for hierarchical wireless sensor networks using ECC. International Journal of Computer Applications, 67(22).

[69] Zia, T. and Zomaya, A., 2006, October. Security issues in wireless sensor networks. In Systems and Networks Communications, 2006. ICSNC'06. International Conference on (pp. 40-40). IEEE.

[70] Rathod, V. and Mehta, M., 2011. Security in wireless sensor network: a survey. Ganpat University Journal of Engineering and Technology, 1(1), pp.35-44.

[71] Nack, F., 2010. An Overview on Wireless Sensor Networks. Institute of Computer Science (ICS), Freie Universität Berlin.

[72] Parno, B., Perrig, A. and Gligor, V., 2005, May. Distributed detection of node replication attacks in sensor networks. In Security and Privacy, 2005 IEEE Symposium on (pp. 49-63). IEEE.

[73] Ganeriwal, S., Čapkun, S., Han, C.C. and Srivastava, M.B., 2005, September. Secure time synchronization service for sensor networks. In Proceedings of the 4th ACM workshop on Wireless security (pp. 97-106). ACM.

[74] Padmavathi, D.G. and Shanmugapriya, M., 2009. A survey of attacks, security mechanisms and challenges in wireless sensor networks. arXiv preprint arXiv:0909.0576.