JCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Volume-5, Issue-4 E-ISSN: 2347-2693

A Survey on Security and Various Attacks in Wireless Sensor Network

P. Sengar, N. Bhardwaj

Department of CSE/IT, Madhav Institute of Technology and Science, Gwalior, India
Department of CSE/IT, Madhav Institute of Technology and Science, Gwalior, India

Corresponding Author: pspoojasengar@gmail.com

www.ijcseonline.org

Received: 21/Mar/2017, Revised: 02/Apr/2017, Accepted: 20/Apr/2017, Published: 30/Apr/2017

Abstract**—** Wireless sensor networks (WSN) have a set of algorithms and protocols with self-establishing capabilities. These sensors work with every other to sense some physical phenomenon after which the information gather is processed to get relevant outcomes. These sensor nodes can calculate, sense, and assemble particulars from the atmospheres and based on some neighborhood decision process, they are able to transmit the sensed records to the person. The battery is the main electricity supply in a sensor node and secondary power supply that harvests strength from the atmospheres together with solar panels may be added to the node depending on the appropriateness of the atmospheres where the sensor will be diffuse. Clustering is the technique which performs the grouping of similar nodes and then starts communicating into the clusters. Security can be achieved by encrypting and decrypting the data and make them unable to read that from the malicious users. Cryptography is the useful technique which contains symmetric and asymmetric methods. In this paper we study about WSN and its application or various attacks which exist in the sensor network in the middle of paper we discuss various existing technique and it's working. Various attacks are performed in this network such as passive and active attacks or insider and outsider attacks. The wirelessly network always required security in the form of data integrity, confidentiality, authenticity and etc.

Keywords— WSN; attacks; security; security issues;

I. INTRODUCTION

A WSN involves of spatial distributed self-directed sensors to atmosphere circumstances or monitor physical, e.g. sound, pressure, temperature, etc. [1]. These sensors are slight, and they are inexpensive and with limited processing and computing resources as equaled to standard sensors. These sensor nodes can measure, sense, and collect facts from the atmospheres and, based on some neighborhood decision process, they are capable to transfer the sensed records to the person. Sensor nodes are lowest power tool ready with one or greater sensors, a processor, memory, a power supply, a radio, and an actuator.

A variety of thermal, organic, optical, mechanical, and magnetic and chemical sensors can be connected to the sensor node to measure assets of the atmosphere. Since the sensor nodes have restricted memory and are usually diffuse in the difficult-to-get entry to places, a radio is carried out for wirelessly communiqué to transfer the records to a base station (BS) (e.g., a computer, a non-public handheld device, or a get right of entry to factor to a set infrastructure). Battery is the primary electricity supply in a sensor node. Secondary power supply that harvests strength from the atmospheres together with solar panels may be add to the node depending on the appropriateness of the atmospheres where the sensor will be diffuse. Depend on the usage and the kind of sensors utilized; actuators may be incorporated in the sensors [2].

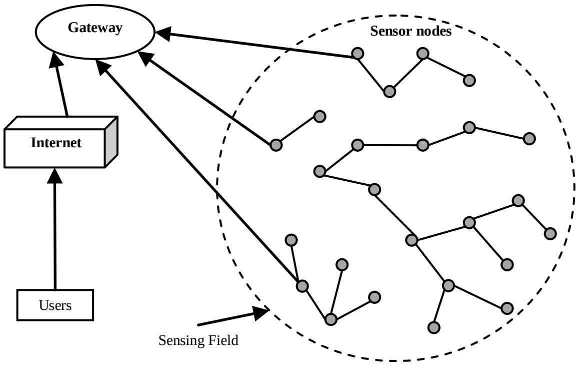

Fig. 1 WSN

II. WSN APPLICATION

We can classify the usage of WSN into defense applications, forest applications, and domestic applications.

A. Defense applications

WSNs can be an integral part of defense command, security control, data communications, computation, intelligence, targeting systems such as surveillance etc.

B. Forest applications

Certain environmentally usage of sensor networks (SN) comprise recording and detect the activities of minor birds and insects, monitoring environmental conditions, animals, earth monitoring and exploration.

C. Medical Science applications

Certain of the applications of health for SN are diagnosing the patients, tracking location and movement of patients and doctors inside hospital etc.

D. Industrial applications

Certain industrial applications of WSNs are make virtual keyboards, environmental control in office constructions, robot control, interactive toys, monitoring product quality etc.

III. TYPE OF WSN

According to formerly research paintings completed five forms of WSN are feasible relying upon wherein and how sensors are installed up to monitor info. According to these properties of sensor deployment we are able to classify WSNs into five primary sorts namely; underground WSN, Ground (terrestrial) WSN, aquatic (underwater) WSN, and mobility WSNs.

A. Ground (Terrestrial) WSNs

Usually include hundreds to thousands of cheap WSN deployed randomly in a given sensing region. Sensor nodes can be dropped from a randomly and plane located into the target region in ad hoc diffuse. In a ground (terrestrial) WSN, reliable communiqué in a dense atmosphere is very vital. Ground sensor nodes must be able to efficiently communicate info return to the BS. While battery power is constrained resource aid and it's important constraint on network performance and its able to not be rechargeable or replaceable again, ground sensor nodes however can be well-found with a secondary power source e.g battery or solar cell. So due to this it is always important for sensor nodes to conserve energy.

B. Underground WSNs

Underground WSNs are sequence of few of the sensor nodes located inside the earth crust or in a cave or in a mine and they may be utilized to monitor underground activities together with volcanic situations and many others. Extra sink or BS nodes are positioned above crust of earth to transmit info from the sensor nodes to the BS. These kind of WSN are a entire more high priced than a ground (terrestrial) WSN in phases of equipment, maintenance and deployment. Underground sensor nodes are extra high priced because vital device parts ought to be decided on to ensure reliable communiqué thru soil, water, rocks, and other contents residing internal crust. The inside circumstances atmosphere create wirelessly communiqué a challenge because of highest levels of signal losses and attenuation.

C. Aquatic (Underwater) WSNs

Aquatic WSNs comprise of few of sensor nodes and vehicles diffuse under water. As opposite to ground WSNs, aquatic sensor nodes are more high-priced and lesser sensor nodes are diffuse in sensing area. Self-directed aquatic vehicles are utilized for collecting or exploration data from sensor nodes. As in evaluation to a dense diffuse of sensor nodes in a ground WSN, a sparse diffuse of sensor nodes is located at sea level. Typical aquatic (underwater) wirelessly communications are implemented through transmission of acoustic waves.

D. Multi-media WSNs

Multi-media WSNs are mixture of a no. of lowest price sensor nodes well-appointed with microphones and cameras. These sensor nodes interconnected with every different over a wirelessly connection for data sensing, records processing, statistics correlation, and records compression. Multi-media WSNs are utilized to allow monitoring of events inside the shape of multimedia programs.

E. Mobile WSNs

Mobility WSNs are a no. of transferring sensor with their interplay with sensing atmosphere. Moving sensor nodes have the potential to compute, like non-moving nodes. Mobility WSNs are utilized in military and other industrial applications [3].

IV. ATTACKS ON WSN

A. Internal Attacks

These are mainly done because of the compromised nodes. These compromised nodes continuously seek to disrupt or parallelize the network. Based on kind of activity performed by attacker, it can be further classified as: Outside Attack- in which, an attacker can replace/introduce new malicious node from outside. Inside Attack- in which, an attacker can capture any node; reprogram it, to act as malicious node.

B. External Attacks

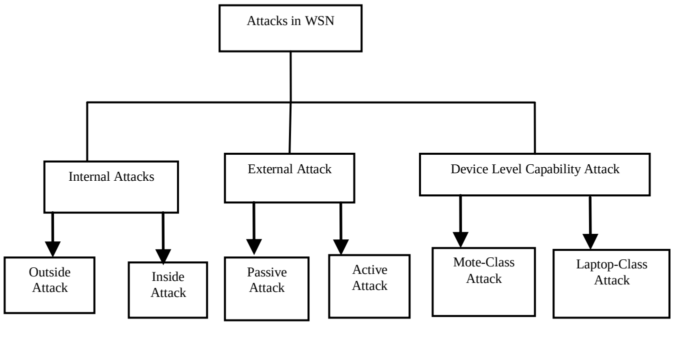

Fig. 2 Attack classifications in WSN

In these attacks, the attacker node isn't always an authorized participate of SN. Depend on the conduct of attacker node, it could be categorized as:

- Passive Attack- it comprise eavesdropping on or monitoring packets swapped within a WSN. It involves only unauthorized listening to the routing packets.

Generally, encryption is the standard solution to defend against these attacks.

- Active Attack- it include few changes of the data steam or the making of a wrong stream. Also, it results in disrupting network functionalities by introducing DOS attacks, Jamming attacks & Power Exhaustion.

C. Device Level Capability Attack

This class of attacks is categorized depend on the capability of the device that is being used for attacking. An attacker may attack the WSN either using a sensor device (Sensor Level) or more powerful laptop device (Laptop Level). An adversary can highly damage the system if he/she uses Laptop Class attack having more powerful computation, storage and battery life. Beside the above mentioned classifications, an attacker may utilize one or more of the subsequent attack techniques such as.

D. Eavesdropping

In which an attacker silently listen to media for communiqué amid two parties and don't modifies the data. It's a passive technique.

E. Radio jamming

In this attack, the attacker tries to disrupt the communication by sending few radio waves at the similar frequency resulting in interference or collisions of packets over network. Jamming can be intermittent or continuous depend on the time for which network is kept jammed.

F. Message's injection

In this the attacker transmits many false messages over network in lieu of corrupting the packet data or to simply exhaust network.

G. Message's replication

In this the attackers capture and resend the same packet many times to same or different sensor and at different times in sequence to make receiver foolish.

H. Node compromise (Destruction or theft)

This includes physical capturing of a node in sequence to disrupt network by breaking the communication path or reprogramming a node so that it acts as a spy in network.

I. Denial of Service (DoS)

In this the attacker will regularly sends packet in sequence to disrupt services or battery power by using malicious nodes. This is an active type of attack.

J. HELLO Flooding

We know that HELLO message is used for discovering neighbors. In this form of attack, the attacker uses more powerful nodes to send HELLO messages to far away sensor nodes so that they trust that the malicious node is their neighbor and they will transfer future packets to it.

K. Black Hole Attack

In this attack a node tries to become receiver of packets of neighboring nodes by altering their routing table and it will never forward the packets to correct destination.

L. Selective Forwarding (Gray Hole Attack)

in this attack, the attacker will insert node of malicious in the n/w which tries to change the routing and capture data just like black hole attack but unlike it will selectively forward data (not all) and so difficult to detect.

M. Wormhole Attack

This kind of attack is done with at least two malicious nodes which have high bandwidth between them either wired or wirelessly. These malicious nodes will show other normal nodes that they provide the shorter path to the target even if they are lying far away in the network. So, the node will forward data to the malicious node that can be captured by attacker easily.

N. Sinkhole Attack

In this attack the malicious node reside near the BS and it tries to imaginary to be closest node to the BS so that other surrounding usual node will change themselves and forward info to the malicious node.

O. Sybil Attack

In this attack the adversary tries to have several individualities to different nodes and thus can be in more than one place at single time. Here it tries to be voted as the cluster head. A Sybil attacks is extensive risk to Geographic Routing Protocols.

P. Infinite Loops-

In this attack two or more malicious node tries to circulate packets infinitely in the n/w in sequence to exhaust power of the network.

Q. Message Alteration

In this attack the node of malicious will capture and modify packets on the network. It can add false data or delete data so that packet will become corrupted.

R. Sleep deprivation torture

In this attack, the malicious node will prevent a node from sleeping by sending messages to it or asks for calculation. This is complete so that the node will consume its power quickly [4].

V. SECURITY REQUIREMENTS IN WSN

A WSN is a special form of network. It shares few commonalities with a usual computer network, but also exhibitions many features that are sole to it. The services of security must be protecting the info communicated over the n/w and the resources from attacks and nodal misconduct in a WSN. The vital security necessities are listed below in WSN:

A. Data confidentiality

The security mechanism needs to make sure that no message in the n/w is understood with the aid of anybody besides supposed recipient. In a WSN, the problematic of confidentiality ought to address the next necessities.

B. Availability

This necessities make sure which the WSN services should be accessible always even in occurrence of an external or internal attacks e.g. DoS. Dissimilar methods have been defined thru investigators to accomplish this objective. While some mechanisms create exploit of additional communiqué among nodes, others propose utilize of a central access control system to make sure successful transfer of all message to its receiver.

C. Data freshness

It implies which the info is current and make sure which no adversary can replay old messages. This necessity is especially significant when the WSN nodes exploit shared-keys for message communiqué, where a potential adversary can launch a replay attack exploiting the old key as the newest key is being propagated to each the nodes in the WSN.A time-precise counter may be insert to all packet to check the cleanness of the packet.

D. Self-organization

Every node in a WSN must be self-organizing and self-recuperation. This characteristic of a WSN additionally poses good challenges to safety. The WSN dynamic nature makes it occasionally not possible to installation any pre-installed shared key mechanism the several nodes and the BS. A no. of key pre-distribution systems have been define inside the context of symmetric encryption However, for software of public-key cryptographic techniques an efficient mechanism for key distribution could be very a great deal crucial. It's perfect that the nodes in a WSN self-establish among themselves no longer simplest for multi-hop routing however also to carryout key control and growing trust relations.

E. Secure localization

In many conditions, it will become essential to accurately and automatically discover each sensor node in a WSN. For instance, a WSN planned to locate errors would necessitate precise localities of sensor nodes recognizing the faults. A capacity adversary can without difficulty provide and manipulate fake locality info with the aid of reporting fake sign asset, replaying messages and so on. If the info statistics isn't always secured properly. The writers in have defined a way called as verifiable multilateration (VM). In multilateration, the position of a device is accurately computed from a sequence of known reference points. The authors have utilized distance bounding and authenticated ranging to make sure accurate place of a node. Due to the distance bounding usage, an attacking node can best successful its claimed distance from a situation factor. However, to make certain region consistency, the attacker would additionally need to show that its distance from every other reference factor is shorter. As it isn't always viable for the attacker to prove this, it's miles viable to come across the attacker. The system is a decentralized range self-governing localization scheme. It's supposed that the locators are trusted and can't be compromised thru any attacker. A sensor calculates its location thru listening to the beacon info sent thru all locator that comprises the locator's location info. The beacon messages are encrypted utilize a shared global symmetric key which is pre-distributed in the sensor nodes. Exploiting the info from each the beacons which a sensor node accepts, it calculates it estimated locality depend on the locators coordinates. The sensor node then calculates overlapping antennas are exploiting a majority election scheme. The last sensor node locality is determined thru computing the gravity center of the overlapping antenna area.

F. Time synchronization

The applications in SN necessitate time synchronization. Any security mechanism must additionally be time-synchronized. A collaborative WSN can also necessitate synchronization among a gathering of sensors. In define a gathering of secure synchronization protocols for multi-hop sender receiver and group synchronization.

G. Authentication

The communicating node is the one that it claims to be. An adversary can't only alteration data packets but also can modify a packet stream thru inserting fabricated packets. It's, therefore, vital for a receiver to have a mechanism to confirm which the received packets have indeed arrive from the actual sender node.

VI. SECURITY ISSUES IN WSN

A. Data Integrity

It's very vital in SN to ensure the data reliability. It ensures that data packets that are accepted thru the target are exactly the ones transfer thru the source and any one can't modify that packet in amid.

B. Data Confidentiality

Confidentiality means to protect data during communiqué in a n/w to be implicit other than intended receiver. Cryptography techniques are used to provide confidentiality. It's a most significant issue in network security.

C. Data Availability

These services are always available in the n/w even under the attack such as Dos. Availability is of primary importance to maintain an operational network. Availability ensures which a sensor node remains always active in the n/w to fulfill the functionality of the network.

D. Data Authentication

The data accepted thru target has not been modified during the transmission. It's reached via asymmetric or symmetric mechanisms in which target and source nodes share secret keys.

E. Data Freshness

The data accepted thru the target is mostly current and fresh data and no challenger can replay the old info. It's reached thru utilizing mechanisms as nonce or adding timestamp to all data packet [5].

VII. TECHNIQUES TO DEFEND THREATS IN WSN

Security is a mostly utilized term encompassing features of integrity, privacy, authentication, nonrepudiation and anti-playback. The risks of the information secure transmission over the n/w increases with increase in the dependency on the info give thru the network.

A. Encryption

That mechanism gives security against passive attacks as eavesdropping. SN typically run in wild or public region over inherently insecure wirelessly channels. It is therefore insignificant for a equipment to eavesdrop or even add messages into the n/w. The traditional key to this issue has been two espouse approach e.g. technique symmetric key encryption schemes, public key cryptography and authentication codes.

B. Symmetric encryption

It's also known as sole one key cryptography. It utilizes a single key. In this encryption procedure the target and the source has to approve upon a sole secret (shared) key. Given a message (plain text) and the key, encryptions generate one intelligible data that is regarding the similar length as the plain text was. Decryption is the encryptions reverses, and utilizes the similar key as encryption.

C. Asymmetric encryption

It's also known as public key cryptography. It uses two keys: public key, which known to the public, used for encryption and private key, which known only to the user of that key, used for decryption. The private and public keys are associated with extraordinary via any mathematical method. In different words, data encrypted thru a public key can be encrypted only thru its consistent private key [6].

D. Cryptography

Electing the maximum appropriate cryptographic approach is essential as all security services ensure through cryptography in WSNs. Cryptographic method utilized in WSNs have to meet the sensor nodes constraints and be evaluated thru statistics size, processing time, and code length [7].

VIII. LITERATURE SURVEY

Xiaoliang Meng et al. [2016] in the procedure of electing the multi-hop nodes in the WSN, it's significant to elect the next optimal forwarding node depend on a certain rule. Optimal electing mechanism depend on geographical location info is a protocol which exploit distances and angles, as the criteria of routing election. TBF protocol confers routing packets along a predefined disperses nodes route instead [8].

Hacène Fouchal et al. [2016] in this paper a distributed solution able to ensure authentication of nodes at any time without having any on-line access to a certificate authority. Each node will be tool with a Trusted Platform Module (TPM) which is able to store keys with security. Each node will have its own public key and private key pair in the TPM and a certificate of the public key. The certificate is issued off-line when setting-up the node. When a node communicates with another, it has to sign the message with its own private key (done securely by the TPM) and sends the message, the signature and the certificate of the public key. The evaluation of the solution has been complete using simulation and the overhead added by integrating authentication does not exceed 15% of energy consumption [9].

Gagandeep Kaur et al. [2016] Sensor nodes gather the info from the atmosphere and transmit to BS. But attackers corrupt data while transmitting therefore data security is main concern of WSN. In define protocol; we decrease the passive attack on sink node thru lessening the traffic on sink node. The simulation outcomes demonstrates the define technique can each node will compress their data before sending to cluster head. After compressing, the packet size of node will decrease. This will decrease the traffic overload. In this compression technique, they diminish the size of packet thru creating a code string of 0 and 1 [10].

Janusz Furtak et al. [2016] Ensuring security in the military usage of IoT is a biggest challenge. The main reasons for this affairs state is that the sensor nodes of the n/w are usually mobile, use wirelessly links, have a small processing power and have a little energy resources. The paper defines the solution for cryptographic protection of transmission between sensors nodes in the data link layer and for cryptographic protection of data save in the sensor node resources. The TPM was utilized. The define result makes it possible to build secure and fault tolerant SN. The following aspects were presented in the paper: the model of such a network, applied security solutions, studies of the security in the n/w and elected investigation results of such a network were presented [11].

Mauricio Tellez et al. [2016] with the fast technological progressions of sensors, WSNs have become a general technology for the IoT. They examined the WSNs security in an atmosphere monitoring usage with the goal to show the overall security. They implemented a STMS, that served as our WSN usage. Our outcomes revealed a security flaw found in the bootstrap loader (BSL) password utilized to protect MSP430 micro-controller units (MCUs). They illustrate how the BSL password can be brute pressured in a depend of days. Furthermore, we illustrate how an attacker can reverse engineer WSN applications to obtain critical security information such as encryption keys. We contribute a solution to patch the weak BSL password security flaw and better the security of MSP430 MCU chips. The Secure-BSL patch we contribute allows the randomization of the BSL password. Our result rises the brute force time to decades. The unusable brute force time accompaniments the safety of the MSP430 and averts future reverse engineering devices. Our research serves as proof that the security of WSNs and the overall IoT technology is broken if we cannot protect these everyday objects at the physical layer [12]

Pooja M.Shukre et al. [2016] Security and confidentiality of data is very much essential while deploying a WSN. Depending on the environment in which network is deployed; configuration parameters of network nodes need to be updated time to time. This can be reached exploit dissemination protocols and data discovery. DiDrip is the initial dissemination protocol and data discovery that has been designed thru taking dissimilar security vulnerabilities in think. The protocol expedites network owner to allow multiple network customers having different privileges for simultaneous and direct dissemination of data into the n/w nodes. This paper define a new technique to minimalize packet loss during data dissemination using DiDrip protocol and provide high security to WSN. RSA and Diffie Hellman key exchange algorithm are used as methods of encryption [13].

Muhammad Umar Aftab et al. [2015] this paper defines the kinds of WSNs and the probable results for tackling the listed difficulties and results of many other issues. This paper will transport the info regarding the WSN and form with literature review so that a person can get more info regarding this emerging field [14].

Biji Nair et al. [2015] the applications range depend on WSN is extensive. Security result implementation is a main problem as these networks are formed from resource constrained tiny sensor nodes which have meager computational power and network lifetime. Moreover, the applications necessitate dissimilar phase of security. A standard security solution isn’t feasible in such networks. ECC is emerging like a promising security result for WSN. Certain applications that require basic security level need not be burdened by using standard security measures which may tax on their efficiency. The correct selection of values of Elliptic Curves (EC) parameters is of paramount significance while implementing ECC for resource constrained WSN. This paper identifies the relevant parameters of EC for ECC implementation in WSN and analyses the impact in their values on the extent of protection they offer [15].

IX. CONCLUSION

WSN are networks which are comprised of sensors that are distributed in an ad hoc way. WSNs are becoming a cost-effective, practical way to go about deploying sensor networks .we use the greedy algorithm and grid-based technology. The scheme is also able to avoid the voids and obstacles in the network by its decentralized forwarding technique, thereby reducing packet drop due to network load, As against the compared approach. The results show that GBRR effectively identifies the redundant nodes and schedule them alternatively in the atmosphere with random obstacles. All these make GBRR reliable scheme that has the ability to improve the overall network quality of service for WSN.

X. REFERENCES

[1] NM. Nair, JS. Terence, "*Survey On Distributed Data Storage Schemes In Wireless Sensor Networks*", Indian Journal of Computer Science and Engineering (IJCSE), Vol.4, No.6, pp.1-6, 2014.

[2] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, “*Wireless sensor network survey*”, Science direct, Vol.52, Issue.12, pp.2292–2330, 2008.

[3] AS. Mandloi, V. Choudhary, "*An Efficient Clustering Technique for Deterministically Deployed Wireless Sensor Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.6-10, 2013.

[4] Sanchita Gupta, Pooja Saini, "*Modified Pairwise Key Pre-distribution Scheme with Deployment Knowledge in Wireless Sensor Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.21-23, 2013.

[5] N. Meenaksi, P. Rodrigues, "*Tsunami Detection and forewarning system using Wireless Sensor Network - a Survey*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.76-79, 2014.

[6] Chanchal Yadav, SS. Hegde, NC. Anjana, Sandeep Kumar, “*Security Techniques in Wireless Sensor Networks : A Survey*”, International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue.4, pp.289-295, 2015.

[7] Jaydip Sen, “*A Survey on Wireless Sensor Network Security*”, International Journal of Communication Networks and Information Security, Vol.1, No.2, pp.1-16, 2009.

[8] Xiaoliang Menga, Xiaochuan Shia, Zi Wangb, Shuang Wua, Chenglin Lia, “*A grid-based reliable routing protocol for wireless sensor networks with randomly distributed clusters*”,elsevier, Vol.51, NO.11, pp.47–61, 2016.

[9] Hacene fouchal, javier biesa, elena romero, alvaro araujo, octavio nieto taladrez, “*a security scheme for wireless sensor networks*”, 2016 IEEE Global Communications Conference (GLOBECOM), Washington, pp.1-5,2016.

[10] Gagandeep Kaur, Deepali, Rekha Kalra,“*Improvement and analys security of WSN from passive attack*”, 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, pp.420-425, 2016.

[11] Janusz Furtak, Zbigniew Zieliński, Jan Chudzikiewicz, "*Security techniques for the WSN link layer within military IoT*", 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, pp.233-238, 2016

[12] Mauricio Tellez, Samy El-Tawab, M. Hossain Heydari, "*IoT security attacks using reverse engineering methods on WSN applications*", 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, pp.182-187, 2016.

[13] pooja m. shukre, divya chirayil, "*enhancement in didrip protocol to securely disseminate data in wireless sensor network sign in or purchase*", 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, pp.1-4, 2016.

[14] MU Aftab, Omair Ashraf, Muhammad Irfan, Muhammad Majid, Amna Nisar, MA. Habib, "*A Review Study of Wireless Sensor Networks and Its Security*", Communication Network, Vol.7, No.4 , pp.172-179, 2015.

[15] Biji Nair, C. Mala,"*Analysis of ECC for application specific WSN security*", 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), *Madurai, pp.1-6, 2015.*