www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 4 April 2017, Page No. 21070-21080
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i4.46

Security Analysis with respect to Wireless Sensor Network – Review

K.Sethu Selvam[1], Dr.S.P.Rajagopalan[2]

[1]Research Scholar, Vels University,
Pallavaram, Chennai, India
sedu.devi@gmail.com
[2]Professor, G.K.M College of Engineering and Technology,
Perungalathur, Chennai, India

Abstract: ***Security or Privacy is the most important challenges in network. These challenges and issues are mostly affected in Wireless than Wired network because medium is open and less limited resources. Sensor is a tiny and low cost device. Wireless Sensor Network (WSN) is operated remotely and can be used in various fields like military surveillance, environmental monitoring, traffic monitoring, health monitoring and etc. In this paper, analysis of various security attacks and security techniques of WSN was done.***

Keywords: Wireless Sensor Network, Security, Attacks, Security Techniques, Sensor**.**

1. Introduction

Wireless sensor networks (WSN) are collection of nodes where each node has its own sensor, processor, transmitter and receiver. Sensor is a Tiny and low cost device that performs a specific type of sensing task. It deployed densely throughout the area to monitor specific event. It mostly operates in public and uncontrolled area.

Wireless Sensor Architecture: WSN contains the following network components [22]

- **Field devices** are used to route the packets. It controls process or process equipment.
- **Gateway** is used to communicate between Host application and field devices.
- **Network manager** is used to configure the entire network which includes scheduling communication between devices, management of the routing tables and monitoring and reporting the health of the network.
- **Security manager** is used to generate, store and management of keys.

Wireless Sensor Characteristics

✓Ability to work in harsh environment.
✓Manage when node is failure
✓Heterogeneity of nodes
✓Ease of use
✓Cross-layer design
✓Low cost
✓Power consumption constraints using batteries.

WSN Application: Some of the applications harshly used in WSN are as follows [22]

- Nuclear reactor control
- Traffic monitoring
- Fire detection
- Contaminant Transport.
- Environmental/Habitat monitoring.
- Acoustic detection.
- Military surveillance
- Medical monitoring.
- Disaster Management.

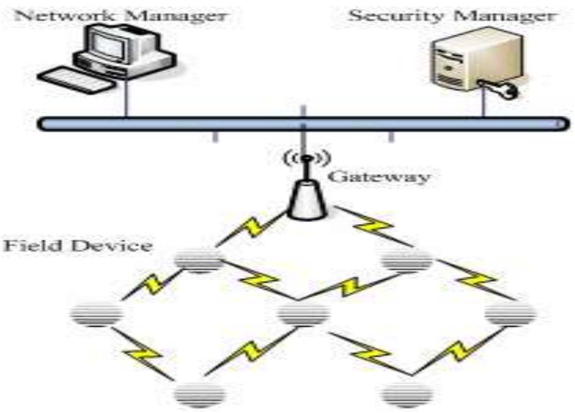


Figure 1 WSN Architecture

Security Limitation in WSN [22]

a. Wireless Medium
b. Limited Storage space and Memory
c. Power Limitation
d. Exposure to physical attack
e. Managed Remotely
f. No Central Management point

Security Goals

Data Integrity: The message has not been altered during transmission.

Data Freshness: The message is recent, and it make sure that no old messages have been replayed.

Data Availability: checks whether a node has able to use resources/to communicate with network or not.

Data Confidentiality: ensures that receiver only can understand the message not by attacker.

Self Organization: It specifies that every node be independent and flexible enough to be self-organizing and self-healing according to different situations.

Authentication: make sure that communication between nodes is trusted.

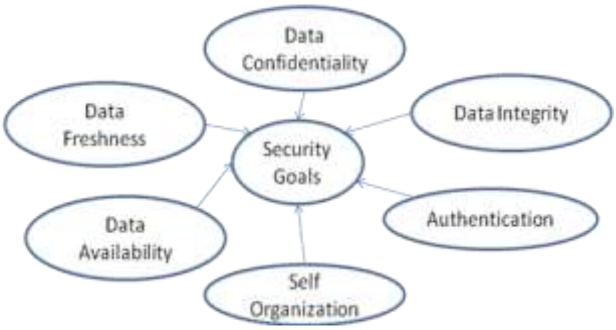
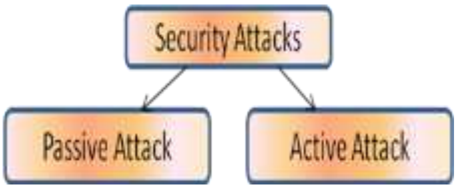


Figure.2 Security Goals in WSN

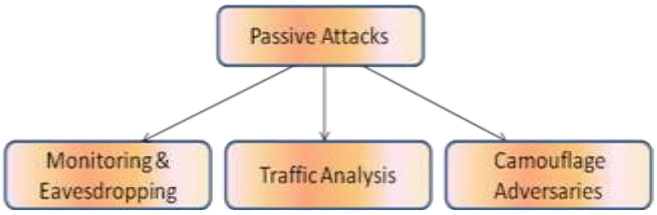
II. SECURITY ATTACKS IN WSN

Security attacks are categorized in two types. These are [5]



Passive Attack

An adversary is monitoring and listening of the communication channel. This attack is also known as Attacks against Privacy.



- **Monitor and Eavesdropping:** An unauthorized person can easily find out information while transmissions.
- **Traffic Analysis:** while transmission information is in encrypted means it may be damaged.
- **Camouflage Adversaries:** A node which is inserted by Intruder acts as normal node in the network to attract the packets.

Active Attack During data transmission, Intruders senses packet and modify message is known as active attacks. The attacks may be given as below.

1. **Routing attacks:** The attacks which acts on the network layer are called routing attacks. The following are the attacks that happen while routing the messages[22]

- ***Spoofed, Altered, or Replayed Routing Information:*** In order to disturb traffic, an attacker may spoof, alter or replay routing information in the network.
- ***Selective Forwarding:*** A node should forward only certain messages and simply drop others.
- ***Sybil Attacks:*** The fault tolerant schemes like multipath routing, topology maintenance and distributed storage are affected in this attack.
- ***Wormholes Attacks:*** An attacker collect packet of information at one particular place in the network, transfers them to some other location, and then resend them into the network.
- ***HELLO flood attacks:*** A malicious node sends or re-plays HELLO packets from one node to another with more power.
- ***Sinkhole Attack:*** When the whole traffic is attracted at a specific node then it is called as sinkhole attack.
- ***Black-hole Attack:*** When path finding process, malicious node suggests the incorrect paths as good paths to the destination node.
- ***Acknowledgement Spoofing:*** An attacker can spoof the acknowledgements of overheard packets destined for particular nodes for providing false information to the neighboring nodes[5].
- **Misdirection***:* A malicious node sends the packets in wrong direction where the destination is unreachable.
- ***Internet Smurf Attack:*** The attacker may fake the network and the address of victim and broadcasts multiple messages in the network to flood a victim with hundreds of responses for every request.
- ***Homing:*** An attacker targets cluster head nodes and key manager nodes to accomplish DoS by destroying these keys.

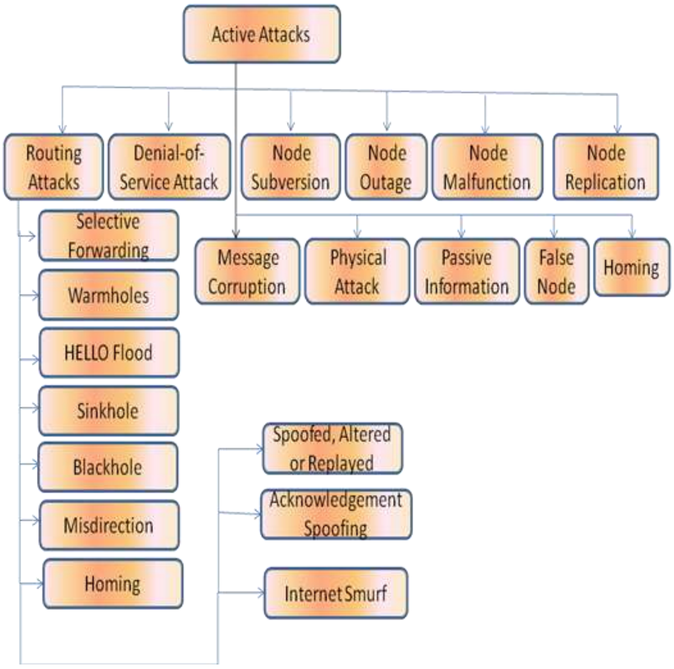
2. **Denial of service attacks**: Sudden failure of the nodes in the sensor networks.
3. **Node Subversion:** An attacker node can capture normal node and it may disclose its important security information and affects the entire security mechanism of the WSN.
4. **Node Outage**: When node stopped function, WSN protocols must be to manage this node outage problem by using some other route

5. **Physical Attacks:** WSN works in an open or harsh environment, it is risk of physical attack.

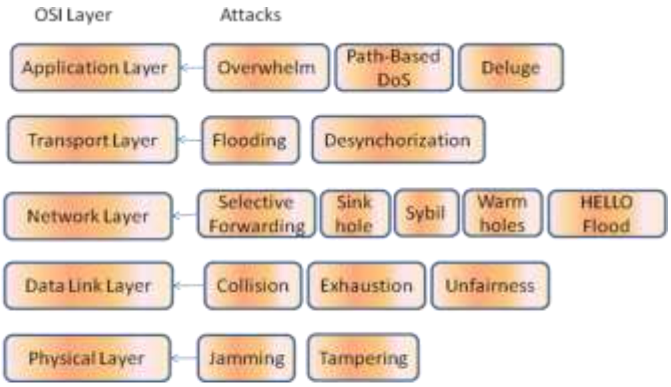
6. **Node Replication Attacks:** An attacker inserts malicious node in the sensor network by copying the node-id of a normal sensor node.

7. **Passive Information Gathering:** An attacker can easily gather information which not encrypted during data transmission.

8. **False Node:** An attacker inserts malicious node in the network then it sends malicious data in the network.



Attacks in OSI Layer



1. Physical Layer: This defines on the transmission media between sending and receiving nodes, the data rate, signal strength, frequency types are also addressed in this layer [5].

1.1 Jamming: This disrupts the accessibility of transmission media.

1.2 Tampering: The simplest way to attack is to damage or modify sensors physically and stop their services. The attack is also to capture sensors and extract sensitive information from them.

2. **Data Link Layer :** This layer is responsible for the data frame detection, medium access and multiplexing of data and includes collions, exhaustion and unfairness attacks [5].
2.1 **Collions:** An attacker may cause collision of packets transmitted on the same frequency and the packets will then be discarded[5].

2.2 **Exhausion:** Repeated collison of attacks can cause resource exhaustion which will deplete the energy of surrounding nodes and transmitting nodes[5].

2.3 **Unfairness:** This is considered as the weak form of a DoS attack. Repeated application of these exhaustion or collision based MAC layer attacks can lead into unfairness[5].

3. Network and Routing Layer : The attacks occurred in the network layer they are referred as routing attacks. There are various attacks occurred at the network layer - Spoofed, altered and replayed routing information, Sinkhole attack, Black-hole attack, Wormholes etc. All these attacks are explained above under routing attacks [5].

5. Transport Layer : This layer is used for external networks and to manage the end to end connections. It includes two attacks flooding and desynchronization [5].

1. **Flooding:** An attacker may repeatedly make new connection requests until the resources required by each connection are exhausted or reach the maximum limit[5].
2. **Desynchronization:** An attacker may repeatedly spoof messages to an end host, causing disruption of an existing connection and missed frames[5].

6. **Application Layer :** This layer is responsible for data collection, management and processing of the data by using the application software to obtain trustworthy consequences[5].

1. **Overwhelm attack:** This attack consumes network bandwidth and drains node energy by overwhelming the nodes causing the network to forward large traffic to the base station[5].

2. **Path-Based DoS attack:** This attack can starve the network of legitimate traffic, because it consumes resources on the path to the base station, thus preventing other nodes from sending data to the base station[5].

3. **Deluge (Reprogram) attack:** If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network[5].

III. Related Work:

Various security methods are applied in WSN.
In this paper, we classified widely used security techniques.
They may be

1. Cryptographic Algorithm
   a. Key Management
   b. Authentication
   c. Key Agreement and Authentication
2. Non –Cryptographic Algorithm
   a. Signal Strength Based
   b. Genetic Algorithm
   c. Firefly Algorithm
   d. Evolution game theory
   e. Stochastic Geometric

Woo Kwon Koo et al.[30] implemented cryptographic algorithm name as HIGHT which recommended for TinySec. This algorithm provided better security solution than Skipjack and RC5.
Virendra Pal Singh et al. [29] implemented Signal strength based system which to detect and prevent Hello Flood attack. Based on signal strength, this method detect whether a node is friend node or stranger.

A.M.Riad et al. [21] implemented Artificial Intelligence (AI) based routing protocol. It reduced communication overhead by removing data redundancy from the network. Energy consumption is achieved by this method.

Sung Jin Choi et al.[27] proposed an Energy-Efficient Key Predistribution Scheme using Eigenvector. Values are used in this vector as Generated pool of random key.

Zhiling Tang et al. [36] proposed technique as Epidemic model based security analysis of Firefly clock Synchronization. It is implemented in MAC layer.

Mohamed Elhoseny et al. [15] proposed technique which is combination of Genetic Algorithm and new cryptography scheme based on Elliptic Curve Cryptography(ECC). In this method, first phase is related to constructing the network structure that minimizes energy exhaustion using GASONeC algorithm. Then the proposed encryption schema is applied to guarantee secure data routing from sensor nodes to the BS. It prevented passive attack and improved network performance of time.

Udaya Suriya Raj Kumar Dhamodharan et al. [28] proposed technique compare match position (CAM) verification method based on message authentication passing (MAP). CAM-PVM algorithm is used to check the node information from base station iNodeInfo table during data transmission. After verification of node details ID, timestamp and current location of node compared with initial information when the node are registered. The result of this algorithm can provide only trusted nodes in the route to ensure secured data transmission. It is used to prevent Sybil attack.

M. Rajalakshmi et al. [19] implemented Energy Efficient Cryptographic (EECA) algorithm. It provided data confidentiality, authenticity and data integrity. It reduced processing time and memory capacity than RSA, AES and DES.

Mohammad Mozumdar et al.[17] proposted Security proposed technique is Zero Knowledge Protocol (ZKP). It is an authentication technique which provided high security solution with minimal usage of resources and high throughput.

Ayaz Hassan Moona et al.[3] implemented a technique which is based Elliptical Curve Digital Signature Algorithm (ECDS). It is mutual authentication technique with the help of computationally low signature scheme.

Kashif Saleem et al. [12] implemented technique as Enhanced biology-inspired self-organized secure autonomous routing protocol (E-BIOSARP). It is based on Artificial Immune system which is used to gain knowledge for neighboring nodeIt This method is used to countermeasures against selective forwarding, spoofing, eavesdropping, replaying or altering of routing information, Hello flood attack and Sybil.

YoHan Park et al. [33] implemented technique as Bio-metric based user authentication and key agreement. It is based on ECC. It provided better functionalities of mobile services in WSN.

Shital Patil [25], author implemented a security method which is based on Bio-metric and private key. In this method, Smart phone is used to capture biometric input data (finger print).

Lavinia Mihaela Dinca et al. [14] proposed implications of spoofing biometric data for retrieving the derived key. They demonstrated that spoofed biometrics could yield the same key, which in turn will lead an attacker to obtain the private key. Smart phone is used to capture biometric input data. Fingerprint and iris is used in biometrics and the fuzzy extractor for biometric key extraction. This method defined a biometric PKI scenario and an in depth security analysis for it.

Alireza Ahadipour et al.[2] implemented a Location-based Probabilistic Key Pre-distribution Scheme (LKPK). In this method, nodes are represented same region and used graph coloring technique to efficiently assign the random keys. This method is better performance than existing random key pre-distribution schemes.

Table 1 : Comparative table for various Security Technique applied by various authors

No	Title	Year	Author	Method	Advantage
1	Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks [30]	2008	Woo Kwon Koo et al.	HIGHT	• Cryptographic algorithm • Better security solution than previous method skipjack and RC5 algorithm
2	Hello Flood Attack and its Countermeasures in Wireless Sensor Networks [29]	2010	Virendra Pal Singh et al.	Signal Strength based	• Based on signal strength , it is considered node as a friend or a stranger.
3	Efficient combined security system for wireless sensor network [6]	2012	N.S. Fayed et al.	Lightweight Kerberos and Elliptic Curve Menezes–Qu–Vanstone (ECMQV)	• Combined two protocols provides enhanced security • Enhanced energy consumption.
4	Secure Routing in Wireless sensor network: A state of the Art [21]	2013	A.M.Riad et al.	AI based routing protocol	• Reduced communication overhead by removing data redundancy from the network
5	An Energy-Efficient Key Predistribution Scheme for Secure Wireless Sensor Networks Using Eigenvector [27]	2013	Sung Jin Choi et al.	Key predistribution scheme	• It is a scheme based on Eigenvector which having matrix includes eigenvalues in generating a pool of random key.
6	A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks [10]	2014	Junghyun Nam et al.	Smart card based user authentication	• Based on elliptic curve cryptography (ECC) • Achieves both authentication key exchange and user anonymity.
7	Security Analysis and Improvements of Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Networks [8]	2014	Jiye Kim et al.	Two-factor authentication	• Used Authentication and key agreement. • Efficient because of less computation and communication cost.
8	Security Enhanced User Authentication Protocol for Wireless Sensor Networks Using Elliptic Curves Cryptography [35]	2014	Younsung Choi et al.	User authentication protocols	• It is based on ECC Mutual authentication Perfect forward secrecy Key agreement between user and sensor
9	An Efficient Identity-Based Key Management Scheme	2014	Zhongyuan Qin et al.	Identity-Based Key Management (IBKM)	• Using Bloom filter to authenticate the

	for Wireless Sensor networks Using the Bloom Filter [37]				communication sensor node with storage efficiency.
10	A Novel Situation Specific Network Security for Wireless Sensor Networks [16]	2015	Mohammad A-Rousan et al.	An adaptive security protocol	• It is a protocol for two layer clustered heterogeneous wireless sensor network • Better WSN lifetime longer than pair-wise key establishment
11	Key Management Mechanism for Authentication Security in Wireless Sensor Network [32]	2015	Ying Wang et al.	Identity-based multi-user broadcasting protocol	• It is used for signature ad authentication on broadcasting packet to acquire scalability and low power consumption • The scheme has lowered the power consumption at least 40% without sacrifice in safety and efficiency.
12	Epidemic model based security analysis of Firefly clock Synchronization in Wireless Sensor Networks [36]	2015	Zhiling Tang et al.	Firefly Algorithm	• It is implemented in the MAC layer of WSNs • Safe because the number of nodes which are out of synchronization decrease with time.
13	A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic Encryption [15]	2015	Mohamed Elhoseny et al.	GASONeC	• It is based on Elliptic Curve Cryptography(ECC) algorithm • It prevents passive attack, CH compromised attack, and brute force attack. • Improved network performance.
14	Sensor Data Security Level Estimation Scheme for Wireless Sensor Networks [1]	2015	Alex Ramos et al.	Sensor Data Security Estimator (SDSE)	• Designed for estimating the sensor data security level based on security metrics that analyze both attack prevention and detection mechanisms.
15	Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method [28]	2015	Udaya Suriya Raj Kumar Dhamodh-aran et al.	CAM-PVM	• It is combined compare and mach position (CAM) verification method with message authentication and passing (MAP). • It is used to prevent Sybil attack.
16	Adaptive Selection of Cryptographic Protocols in Wireless Sensor Networks using Evolutionary Game Theory [26]	2015	Srishti Arora et al.	Evolutionary Stable Strategy	• It is based on Evolutionary game theory.
17	Advanced Cryptographic Algorithm to Secure the Sensor Node Data in WSN	2016	Rajalakshmi et al.	Energy Efficient Cryptographic (EECA) algorithm	• It provided confidentiality, authenticity

	[19]				and integrity. • Reduced processing time and memory capacity than RSA, AES and DES
18	Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach [31]	2016	Yansha Deng et al.	A frame work : Stochastic Geometry	• Three-tiger physical layer security • Increasing no. of sinks improves both average secrecy rate between access point and associated sink
19	Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks [13]	2016	H. Khosravi et al.	Alpha-Beta Filtering	• Intrusion detection system • High packet delivery ratio and low delay.
20	Ensuring Authentication and Security using Zero Knowledge Protocol for Wireless Sensor Network Applications [17]	2016	Mohammad Mozumdar et al.	Zero Knowledge Protocol (ZKP)	• It is used for authentication node • High security to the network with minimal overhead, minimal energy consumption, and good throughput.
21	A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities [9]	2016	Jun Wu et al.	User Control (UCON) Technology	• It is framework proposed in which Low - level attack detection with simple rule and high-level attack detection with complex rules is performed in sinks and at the base station • Better resource consumption and attack detection rate.
22	Mutual Entity Authentication Protocol Based on ECDSA for WSN [3]	2016	Ayaz Hassan Moona et al.	ECDSA (Elliptical Curve Digital Signature Algorithm)	• A mutual authentication protocol with the help of a computationally low signature scheme. • It improves the network performance
23	A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks [4]	2016	Danyang Qin et al.	Light Authentication and Key Management Scheme (AKMS)	• Provide more efficient security with less energy consumption, control overhead, and packet loss rate than other typical schemes • Provide message confidentiality and authenticity
24	An Enhanced Lightweight Anonymous Authentication Scheme for a Scalable Localization Roaming Service in Wireless Sensor Networks [34]	2016	Youngseok Chung et al.	An Enhanced Lightweight Anonymous Authentication Scheme	• To provide anonymous authentication of sensor nodes • Low-cost functions • One-way hash function

25	An Anonymous User Authentication and Key Agreement Scheme Based on a Symmetric Cryptosystem in Wireless Sensor Networks [7]	2016	Jaewook Jung et al.	Symmetric cryptosystem	• Improves the level of security, and is also more efficient relative to other related scheme • Achieves both stronger security and higher efficiency
26	Performance and Challenges of Service-Oriented Architecture for Wireless Sensor Networks [20]	2016	Remah Alshinina et al.	Service-Oriented Architecture (SOA)	• Achieve more robust and efficient network performance.
27	A Novel Secure IoT-Based Smart Home Automation System Using aWireless Sensor Network [23]	2016	Sandeep Pirbhulal et al.	Triangle Based Security Algorithm (TBSA)	• Efficient key generation procedure • Integrates low power Wi-Fi • Better performance than AES and DES
28	Cost-Effective Encryption-Based Autonomous Routing Protocol for Efficient and SecureWireless Sensor Networks [12]	2016	Kashif Saleem et al.	Enhanced biology-inspired self-organized secure autonomous routing protocol (E-BIOSARP)	• Used Artificial Immune system which is used to gain knowledge for neighboring nodes. • Is countermeasures against selective forwarding, spoofing, eavesdropping, replaying or altering of routing information, Hello flood attack and Sybil.
29	Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks [33]	2016	YoHan Park et al.	Bio-metric based user authentication and key agreentment	• Better security functionalities for mobile services in WSN. • It is based on ECC
30	Location Privacy Based Security Enhancement In Wireless Sensor Network Using LFPM And PPM [24]	2016	S. Saravanan et al.	Probilistic Packet Marking) in addition to LFPM (Local flow Packet marking)	• To trace back in to the source node location, then the source node used to another path or another server for data request and data response in the network • Better network performance
31	Early Detection of DDoS Attack in WSN [11]	2016	Kanchan Kaushal et al.	Early detection DDoS attack	• Detect the attack on early stages so that data loss can be prevented and more energy can be reserved
32	Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol [18]	2016	Parmar Amisha et al.	AOMDV (Ad hoc On demand Multipath Distance Vector)	• Used to detect and prevent Warmhole attack • Based on Round Trip Time (RTT)
33	DoS attack prevention	2016	Shital Patil	Immune System	• To prevent DoS attacks

	technique in Wireless Sensor Networks [25]		et al.		• Reduces the false alarm rate
34	User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks [14]	2017	Lavinia Mihaela et al.	bioPKI	• This model is based on Bio-metric and private key. • Smart phone is used to capture biometric input data.(Finger Print)
35	LPKP: Location-based Probabilistic Key Predistribution Scheme for Large-Scale WSN Using Graph Coloring [2]	2017	Alireza Ahadipour et al.	LPKP: Location-based	• It can randomly pre-distribute keys based on the location of the nodes

Table 2: Comparative various Security Technique with Resource Constraints

Scheme	Energy Consum-ption	Memory	Computation	Processing Time
EECA		✓		✓
GASONeC	✓	✓		
ECDSA	✓		✓	✓
AKMS	✓			
HIGHT	✓		✓	✓
Signal Strength Based	✓		✓	✓
Light Weight Kerberos & ECMQV	✓		✓	✓
User Authentication		✓	✓	
CAM-PVM	✓			✓
ZKP	✓	✓	✓	✓

IV. Conclusion

In this paper, analysis of various active and passive security attacks was done. This survey is useful for the future researchers to come up with light smarter security mechanism with less energy consumption, less memory and less computation and make safe network for wireless sensor.

References:

[1]. Alex Ramos and Raimir Holanda Filho, Sensor Data Security Level Estimation Scheme for Wireless Sensor Networks, Sensors 2015, 15, 2104-2136; doi:10.3390/s150102104.

[2]. Alireza Ahadipour , and Alireza Keshavarz-Haddad, LPKP: Location-based Probabilistic Key Pre-distribution Scheme for Large-Scale Wireless Sensor Networks Using Graph Coloring, The ISC Int'l Journal of Information Security.

[3]. Ayaz Hassan Moona, Ummer Iqbala and G. Mohiuddin Bhatb, Mutual Entity Authentication Protocol Based on ECDSA for WSN,ScienceDirect Procedia Computer Science 89 (2016) 187 – 192.

[4]. Danyang Qin, Shuang Jia, Songxiang Yang, ErfuWang, and Qun Ding, A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks, Hindawi Publishing Corporation Journal of Sensors Volume 2016, Article ID 1547963, 9 pages.

[5]. Divya Singla, Chander Diwaker, Security Issues and Challenges in Wireless Sensor Networks: A Survey, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 10, October 2015.

[6]. Fayed .N.S. , E.M. Daydamoni, A. Atwan, Efficient combined security system for wireless sensor network, Egyptian Informatics Journal (2012) 13, 185–190.

[7]. Jaewook Jung , Jiye Kim , Younsung Choi and Dongho Won, An Anonymous User Authentication and Key Agreement Scheme Based on a Symmetric Cryptosystem in Wireless Sensor Networks, Sensors 2016, 16, 1299; doi:10.3390/s16081299.

[8]. Jiye Kim , Donghoon Lee , Woongryul Jeon , Youngsook Lee and Dongho Won , A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks, Sensors 2014, 14, 21023-21044; doi:10.3390/s141121023 ISSN 1424-8220.

[9]. Jun Wu, Kaoru Ota, Mianxiong Dong, And Chunxiao Li, A Hierarchical Security Framework for Defending Against Sophisticated Attacks on Wireless Sensor Networks in Smart Cities, Digital Object Identifier 10.1109/ACCESS.2016.2517321.

[10]. Junghyun Nam, Moonseong Kim, Juryon Paik , Youngsook Lee and Dongho Won, A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks, Sensors 2014, 14, 21023-21044; doi:10.3390/s141121023 ISSN 1424-8220.

[11]. Kanchan Kaushal, Varsha Sahni, Early Detection of DDoS Attack in WSN, International Journal of Computer Applications (0975 – 8887) Volume 134 – No.13, January 2016.

[12]. Kashif Saleem , Abdelouahid Derhab, Mehmet A. Orgun, Jalal Al-Muhtadi, Joel J. P. C. Rodrigues , Mohammed Sayim Khalil and Adel Ali Ahmed, Cost-Effective Encryption-Based Autonomous Routing Protocol for Efficient and SecureWireless Sensor Networks, Sensors 2016, 16, 460; doi:10.3390/s16040460.

[13]. Khosravi .H, R. Azmi, and M. Sharghi, Adaptive Detection of Hello Flood Attack in Wireless Sensor Networks, International Journal of Future Computer and Communication, Vol. 5, No. 2, April 2016.

[14]. Lavinia Mihaela Dinca and Gerhard Hancke, User-Centric Key Entropy: Study of Biometric Key Derivation Subject to Spoofing Attacks, Entropy 2017, 19, 70; doi:10.3390/e19020070.

[15]. Mohamed Elhoseny , Hamdy Elminir , Alaa Riad, Xiaohui Yuan , A secure data routing schema for WSN using Elliptic Curve Cryptography and homomorphic Encryption, Journal of King Saud University Computer and Information Sciences (2016) 28, 262–275.

[16]. Mohammad A-Rousan,Muneer Bani Yassein, Ahmed Al-Dubai,Barraq Ghaleb, Ibrahim Mahmoud, A Novel Situation Specific Network Security for Wireless Sensor Networks , © 2015 by IFSA Publishing, S. L. Sensors & Transducers, Vol. 186, Issue 3, March 2015, pp. 33-42.

[17]. Mohammad Mozumdar , Mehrdad Aliasgari , Sudheer Matta Veera Venkata and Sai Santosh Renduchintala, Ensuring Authentication and Security using Zero Knowledge Protocol for Wireless Sensor Network Applications, International Journal of Computing and Digital Systems ISSN (2210-142X) Int. J. Com. Dig. Sys. 5, No.3 (May-2016).

DOI: 10.18535/ijecs/v6i4.46

[18]. Parmar Amisha , V.B.Vaghela,Detection and Prevention of Wormhole Attack in Wireless Sensor Network using AOMDV protocol, ScienceDirect Procedia Computer Science 79 (2016) 700 – 707.

[19]. Rajalakshmi .M, C. Parthasarathy and R.V. Indrajith, Advanced Cryptographic Algorithm to Secure the Sensor Node Data in WSN, Middle-East Journal of Scientific Research 24 (6): 1926-1931, 2016 ISSN 1990-9233 © IDOSI Publications, 2016.

[20]. Remah Alshinina and Khaled Elleithy, Performance and Challenges of Service-Oriented Architecture for Wireless Sensor Networks, Sensors 2017, 17, 536; doi:10.3390/s17030536.

[21]. Riad .A. M, Hamdy K. El-Minir, Mohamed El-hoseny, Secure Routing in Wireless sensor network: A state of the Art , International Journal of Computer Applications (0975 – 8887) Volume 67– No.7, April 2013.

[22]. Rudramurthy V C, Dr. R Aparna, Security Issues and Challenges in Wireless Sensor Networks: A Survey, International Journal of Innovative Research in Computer and Communication Engineering (An ISO 3297: 2007 Certified Organization) Vol. 3, Issue 10, October 2015.

[23]. Sandeep Pirbhulal , Heye Zhang , Md Eshrat E Alahi , Hemant Ghayvat ,Subhas Chandra Mukhopadhyay , Yuan-Ting Zhang and Wanqing Wu, A Novel Secure IoT-Based Smart Home Automation System Using aWireless Sensor Network, Sensors 2017, 17, 69; doi:10.3390/s17010069.

[24]. Saravanan .S, Dr. M. Prabakaran, Location Privacy Based Security Enhancement In Wireless Sensor Network Using LFPM And PPM, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 6 (2016) pp 3936-3939.

[25]. Shital Patil, Sangita Chaudhari , DoS attack prevention technique in Wireless Sensor Networks, ScienceDirect Procedia Computer Science 79 (2016) 715 – 721.

[26]. Srishti Arora, Prabhjot Singh, Dr. Ashok Ji Gupta, Adaptive Selection of Cryptographic Protocols in Wireless Sensor Networks using Evolutionary Game Theory, ScienceDirect Procedia Computer Science 78 (2016) 358 – 366 .

[27]. Sung Jin Choi, Kyung Tae Kim, and Hee Yong Youn, An Energy-Efficient Key Predistribution Scheme for Secure Wireless Sensor Networks Using Eigenvector , Hindawi Publishing Corporation International Journal of Distributed Sensor Networks Volume 2013, Article ID 216754.

[28]. Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal, Detecting and Preventing Sybil Attacks in Wireless Sensor Networks Using Message Authentication and Passing Method, Hindawi Publishing Corporation Scientific World Journal Volume 2015, Article ID 841267, 7 pages .

[29]. Virendra Pal Singh, Sweta Jain and Jyoti Singha, Hello Flood Attack and its Countermeasures in Wireless Sensor Networks, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.

[30]. Woo Kwon Koo, Hwaseong Lee, Yong Ho Kim, Dong Hoon Lee, Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable forWireless Sensor Networks, 2008 International Conference on Information Security and Assurance.

[31]. Yansha Deng, Lifeng Wang, Maged Elkashlan, Arumugam Nallanathan, Ranjan K. Mallik, Physical Layer Security in Three-Tier Wireless Sensor Networks: A Stochastic Geometry Approach , EEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 11, NO. 6, JUNE 2016.

[32]. Ying Wang, Xinguang Peng, and Jing Bian, Key Management Mechanism for Authentication Security in Wireless Sensor Network, Applied Mathematics & Information Sciences An International Journal 9, No. 2, 711-719 (2015).

[33]. YoHan Park and YoungHo Park, Three-Factor User Authentication and Key Agreement Using Elliptic Curve Cryptosystem in Wireless Sensor Networks, Sensors 2016, 16, 2123; doi:10.3390/s16122123.

[34]. Youngseok Chung , Seokjin Choi , Youngsook Lee , Namje Park and Dongho Won, An Enhanced Lightweight Anonymous Authentication Scheme for a Scalable Localization Roaming Service in wireless Sensor Networks, Sensors 2016, 16, 1653; doi:10.3390/s16101653.

[35]. Younsung Choi , Donghoon Lee , Jiye Kim , Jaewook Jung , Junghyun Nam and Dongho Won , A Provably-Secure ECC-Based Authentication Scheme for Wireless Sensor Networks, Sensors 2014, 14, 21023-21044; doi:10.3390/s141121023.

[36]. Zhiling Tang and Simin Li, Epidemic model based security analysis of Firefly clock Synchronization in Wireless Sensor Networks, International Journal of Security and Its Applications Vol. 9, No. 6 (2015), pp. 19-34 .

[37]. Zhongyuan Qin , Xinshuai Zhang , Kerong Feng , Qunfang Zhang and Jie Huang , An Efficient Identity-Based Key Management Scheme for Wireless Sensor Networks Using the Bloom Filter, Sensors 2014, 14, 17937-17951; doi:10.3390/s141017937.