ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

Security Techniques in Wireless Sensor Networks : A Survey

Chanchal Yadav[1], Raksha K[2], Supriya S. Hegde[3], Anjana N.C[4], Sandeep Kumar E[5]

Student, Telecommunication, Jawaharlal Nehru National College of Engg, Shivamogga, India [1,2,3,4]

Assistant Professor, Telecommunication, Jawaharlal Nehru National College of Engg, Shivamogga, India[5]

Abstract: Wireless Sensor Network (WSN) is a special kind of ad-hoc network. WSNs are useful in many critical applications like military and surveillance, habitat monitoring, etc. Security has been a major concern in these networks due to restrictions of resources in the sensor nodes and less human intervention during its operation. This paper outlines the security requirements, threats and vulnerabilities in WSN operations and the associated existing works towards defending against malicious attacks..

Keywords: security threats, WSN , ad- hoc networks ,security requirements ,sensor nodes.

I. INTRODUCTION

The technology takes the growing curve in the modern world the networking, become more essential. Network is a set of devices connected by communication links. Wired networks also called Ethernet network are the most common types of local area network (LAN) technology. The types of wired network are PAN, LAN, mesh, MAN, WAN and the cellular network. Wireless network is any type of computer network that uses wireless data connection for connecting network nodes. Peer to peer/ Ad-hoc and infrastructure (Wi-Fi) are the main two types of wireless networking. As both of the networks have their own advantages and disadvantages, the wireless network is more advantageous than wired network because it allows easy connectivity between computers, cost effective [1].

As the wireless technology advances, there is a rapid growth in wireless sensor network research. This is a network, which includes distributed sensors to monitor the physical or environmental conditions like temperature, sound, vibration, pressure and humidity. Sensor node has radio transceiver, microcontroller and a battery. Resources like energy, memory, speed, bandwidth, is varied according to the size of the node [2].

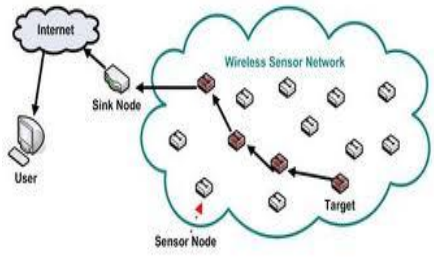

Fig. 1: Wireless Sensor Network

[*COURTESY*- enroute filtering.blogspot.com"]
As the wireless sensor node consumes less power, and due to the ease of distribution multifunctionality of the sensor nodes, these networks has been used for various applications such as healthcare, target tracking, environmental monitoring, etc. [3].

In this paper we discuss the Security requirements, attacks, security threads and vulnerability and threats defend techniques in WSN. The organization of the paper is: section II deals with security requirements and goals of WSN, section III deals with attacks in WSN, section IV deals with security threads and vulnerability, section V deals with techniques to defend threats in WSN section VI with the concluding remarks and finally the paper ends with few references.

II. SECURITY REQUIREMENTS AND GOALS OF WSN

WSNs are special kind of ad-hoc network. Security services in WSNs are required to protect the information and resources from attacks and misbehaviour [4]. The security goals are classified as primary and secondary. The primary goals are known as standard security goals such as confidentiality, integrity, authentication and availability (CIAA). The secondary goals are Data freshness, Self-organization, Time-synchronization and Secure Localization [5].The detailed description is given below:

A. Data Confidentiality : Confidentiality is the ability to conceal messages from a passive attacker so that any message communicated via the sensor network remains confidential [5]. It ensures that a given message cannot be understood by anyone other than the desired recipients [4]. This is the most important issue in network security [5]. For secure communication, encryption is used. Data is encrypted with a secret key that only authorized users have. Public sensor information should also be encrypted to some degree to protect against traffic analysis attacks [6].

B. Data Authentication : Authentication ensures the reliability of the message by identifying its origin. Attacks in sensor networks do not just involve the alteration of packets; adversaries can also inject additional false packets

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

[5]. It ensures that a malicious node cannot masquerade as a trusted network node [4]. Informally, data authentication allows a receiver to verify that the data really sent by the claimed sender. In the case of two-party communication, data authentication can be achieved through a purely symmetric mechanism: the sender and the receiver share a secret key to compute the Message Authentication Code (MAC) of all communicated data [7].

C. Data integrity : Data integrity in sensor networks is needed to ensure the reliability of the data and refers to the availability who confirm that a message has not been tempered with, altered or changed [5]. With the implementation of confidentiality, an adversary may be unable to steal information. However, this does not mean the data is safe. The adversary can change the data, so as to send the sensor network into disarray [7]. The integrity of the network will be in trouble when:

- A malicious node present in the network injects false data.
- Unstable conditions due to wireless channel cause damage or loss data. [5]

D. Data Availability : Availability determines whether a node has the ability to use the resources and whether the network is available for the messages to communicate [5]. It ensures that the desired network services are available even in the presence of denial-of-service attacks require configuring the initial duty cycle carefully [4].

The Secondary goals are:

a) Data Freshness : Freshness implies that the data is recent and ensures that no adversary can replay old messages [4]. Data freshness is classified in two types based on the message ordering: weak and strong freshness. Weak freshness provides only partial message ordering but gives no information related to the delay and latency of the message. Strong freshness on the other hand , gives complete request-response pair and allows the delay estimation. Sensor requirements require weak freshness, while strong freshness is needed for time synchronization within the network [6]. To make sure that no old message required a timestamp can be added to the packet [4].

b) Self –Organization : A wireless sensor network is a typically an Ad-hoc network, which requires every sensor node be independent and flexible enough to b self-organizing and self- healing according to different situation [5]. There is no fixed infrastructure available for the purpose of network management in a sensor network. This inherent feature blinks a great challenge WSN security as well [7]. The dynamic nature of a WSN makes it sometimes impossible to deploy any preinstalled shared key mechanism among the nodes and the base station [8].

c) Time-Synchronization : Most sensor network applications relay on some form of time-synchronization. Furthermore, sensors may wish to compute the end-to-end delay of a packet as it travels between two pair wise sensors. A more collaborative sensor network may require group synchronization for tracking applications [4, 5, and 9].

d) Secure Localization : In WSN each sensor node is required to locate itself in the network accurately and automatically to identify the location of the fault [4].

III. ATTACKS IN WIRELESS SENSOR NETWORKS

Wireless sensor network are power constraint networks, having limited computational and energy resources. This makes them exposed enough to be attacked by any attacker deploying more resources than any individual node or base station, which may not be a difficult job for the attacker [6]. WSN are vulnerable to security attacks due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in hostile or dangerous environment where they are not physically protected [5]. Various WSN attacks on different layers are discussed below:

Physical layer:

Attacks at the physical layer include jamming and tampering. These two attacks are discussed in the sub sections.

1) Jamming:

Jamming is a type of attack which interferes with the radio frequencies that a network's nodes are using. An attacker sends some radio waves at the same frequency that it is used by WSNs [4, 8, 10]. Jamming can be of two types-constant jamming and intermittent jamming. Constant jamming affects the complete obstruct of the whole network whereas in intermittent jamming nodes are capable of communicating data periodically but not continuously [6]. A jamming source may either be powerful enough to disrupt the entire network or less powerful and only able to disrupt a smaller portion of the network [4].

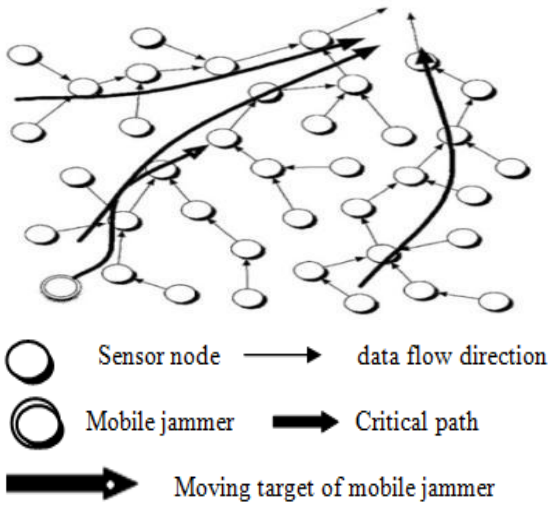

Fig2: Radio Jamming in WSN
[www.google.com/patents/us7907888]

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

2) Tampering:
Another physical layer attack is tampering [11]. Given physical access to a node, an attacker can extract sensitive information such as cryptographic keys or other data on the node. The node may also be altered or replaced to create a compromised node which the attacker controls [4].

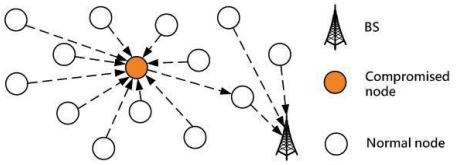

Fig.3: Tampering attack [4]

Data Link Layer
Attacks at the link layer include the following:
3) Collisions:
A collision results when two nodes trying to send data on same frequency. When packets collide, a change will likely occur in the data portion, causing a checksum mismatch at the receiving end. The packet will then be discarded as invalid [4, 8]. An attacker may cause collisions in particular packets such as ACK control messages. The effected packets are transmitted again, increasing the energy and time cost for transmission. Such an attack reduces the network perfection [6].

4) Exhaustion:
Repeated collisions can also be used by an attacker to cause resource exhaustion [8, 11]. This attack dominates the power resources of the node by causing them to retransmit the message even when there is no collision or late collision [6].

5) Unfairness:
Unfairness can be considered a week form of DoS attack. An attacker may cause unfairness in a network by intermittently using the above link layer attacks [4]. MAC protocols at link layer administer the communications in networks by constraining priority schemes for seamless correlation. It is possible to use these protocols thus affecting the precedence schemes, which ultimately results in decrease in service [12].

Network layer:
The network and routine layer of sensor network is usually designed according to the following principles [4, 11]:

- Power efficiency is an important consideration.
- Sensor networks are mostly data-centric.
- An ideal sensor network has attribute-based addressing and location awareness.

The attacks in the network layer include the following:
Spoofed, Altered, or Replayed Routing Information:
The most direct attack against a routing protocol in any network is to target the routing information itself while it is being exchanged between nodes. An attacker my spoof, alter, or replay routing information in order to disrupt traffic in the network [4, 8, 11]. These disruptions include the creation of routing loops, extend or shorten service routes, generate false error messages, increase end-to-end latency [5] and partitioning the network [4].

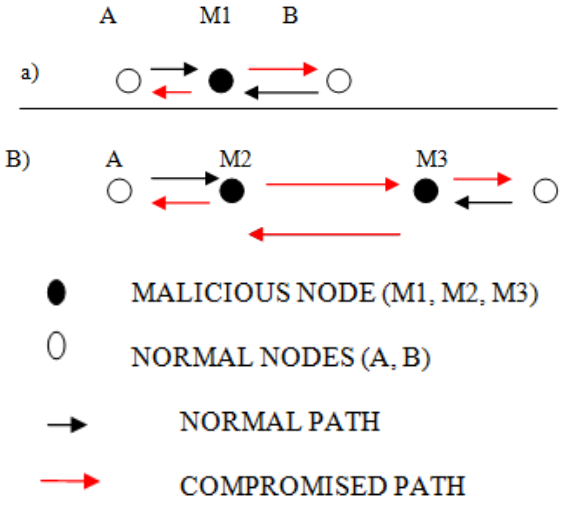

Fig.4: Replay attack

6) Selective forwarding:
An attacker may create malicious nodes which selectively forward only certain messages and simply drop others [4, 8, 11]. One form of this attack is black hole [10]. Like a black hole attack, malicious nodes refuse to forward any packets through it.

7) Sink hole:
Attracting traffic to a specific node is called Sink hole attack. In this attack the adversary's goal is to attract nearly all the traffic from a particular area to a compromised node [13]. This compromised node is chosen by the surrounding nodes for routing their data, as the end result.

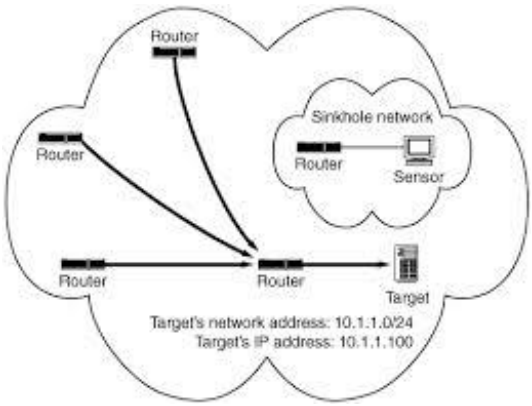

Fig.5: Attack traffic redirected to Sink hole network ["users.atw.hu/denialofservice/ch06lev1sec4.html"]

8) Sybil:
The Sybil attack is a case where one node presents more than one identity to the network [11]. Sybil attack tries to degrade the integrity of data, security and resource utilization that the distributed algorithm attempts to achieve. This Sybil attack can be performed for attacking the distributed storage, routing mechanism, data

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

aggregation, voting, fair resource allocation and misbehaviour detection. Basically, any peer-to-peer network is vulnerable to Sybil attack [11]. Authentication and encryption techniques can prevent an outsider to launch a Sybil attack on the sensor network [13].

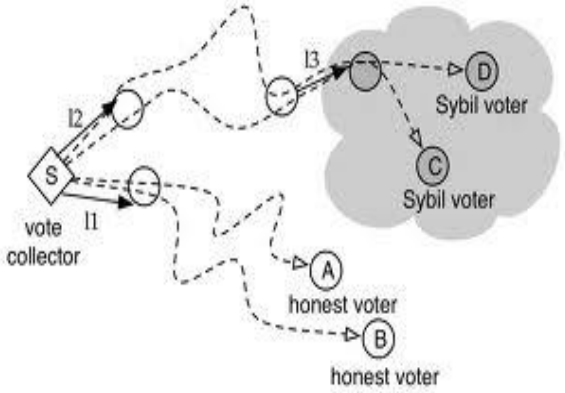

Fig.6: Sybil attack [sumsup.news.cs.nyu.edu]

9) Wormhole attack:
Wormhole attack is a critical attack in which the attacker records packets at one location in the network and tunnels those to another location. The tunnelling or retransmitting of bits could be done selectively [14]. A wormhole is a low-latency junction between two sections of network. The malicious node receives packets in one section of the network and sends them to another section of the network. These packets are then replayed locally. This creates a fake scenario that the original sender is only one or two nodes away from the remote location. This may cause congestion and retransmission of packets squandering the energy of innocent nodes [3].

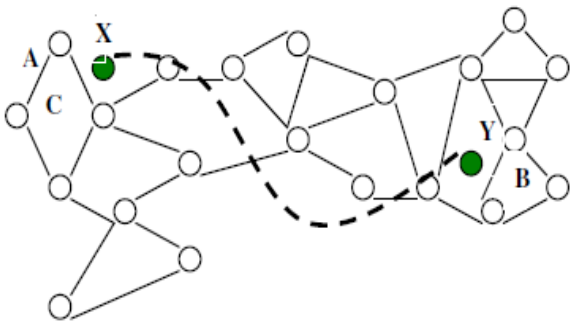

Fig.7: Wormhole attack [16]

10) Hello flood attack:
An attacker sends or replays routine protocol's HELLO packets from one node to another with more energy [1]. This attack uses HELLO packets as a weapon to convince the sensors in WSN. In this sort of attack an attacker with a high radio transmission range and processing power sends HELLO packets to a number of sensor nodes which are dispersed in a large area within a WSN. The sensors are thus persuaded that the adversary is their neighbour. As a consequence, while sending the information to the base station, the victim nodes try to go through the attacker as they know that it is their neighbour and are ultimately spoofed by the attacker [11].

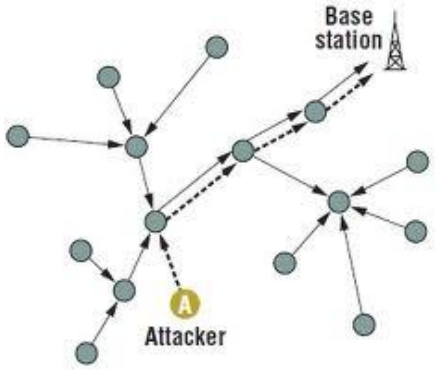

Fig.8: Hello flood attack [enroute filtering.blogspot.com]

Transport layer
Two possible attacks in this layer are discussed in the subsections:

11) Flooding:
Whenever a protocol is required to maintain state at either end of a connection it becomes vulnerable to memory exhaustion through flooding [4, 8, 11]. New connection requests can be made repeatedly by an attacker until the resources required by each connection are exhausted or reach a maximum limit.

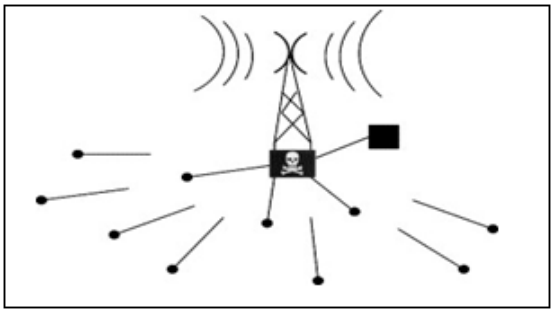

Fig.9: A flooding attack [4]

12) Desynchronization:
It refers to the disruption of an existing connection [4]. An adversary continuously swindles packets to an end host. This host then demands retransmission of dropped frames and hence energy of nodes is wasted, therefore degrading the performance of the whole network [6].

IV. SECURITY THREATS AND VULNERABILITY

WSN possess some vulnerable characteristics and security challenges which may compromise the confidentiality, data integrity, and service availability and are mentioned in this section. [15]

Wireless medium:
WSN use frequency band for wireless communication. In WSN, nodes are connected with each other, and the traffic pattern is toward the sink through the gateways, uses variable band of frequencies depending upon the nature and type of application. Jamming and scrambling are the common security threats for the wireless medium of WSN. Scrambling is periodical short term jamming in which the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

strong noise is introduces after specified interval of time, hence the communication channels of wireless medium work for some time and stop working during the period of scrambling. In wireless networks, the strategy is that to keep the location of the gateway hidden so that to prevent the physical damage and jamming kinds of attacks, as gateways are the core and most important backbone devices. However, the attackers locate the gateways [15] by first conducting a passive homing attack. In homing attack, the intruder passively monitors and observes the traffic pattern in the network.

Cooperative MAC:
WSN use cooperative MAC protocol at data link layer, which is shared among all the nodes in communication. This cooperative MAC gives rise to hidden node terminal and collision of packets.

Ready To Send/Clear To Send(RTS/CTS) mechanism was introduced to solve the problems of hidden node terminal, as first the node would send the RTS signal to the communicating node, and if receive the CTS signal, which means that no any other node is transmitting the data, hence the node can transmit the data. However, MAC with RTS/CTS still faces the problem of exposed node terminal, which needs to be resolved.

WSN are mostly dependent on the observation and captured information of the sensor node; hence the result of the received data can be seriously corrupted if the strategically important nodes in WSN become the victim of selfish MAC behaviour, and are unable to communicate
Multi-hop environment:

WSN are multi-hop wireless network. Data traffic passes in hop by hop pattern toward the destination. Multi-hop architecture is necessary for easy and rapid deployment, as well as it also reduce the deployment cost, as the nodes have the flexibility of self-healing, self-configuring and self-adjusting.

The main security threats due to multi-hop nature of WSN are:

- Black hole attack
- Grey hole attack, in which the malicious nodes selectively drop the network traffic.
- Wormhole attack
- False route creation attack, in which malicious nodes create false and non-existing routes between source and destination.\
- Sybil attack

Power limitation:
As WSN consist of tiny nodes which have limited or definite battery power. The sensor nodes conserve the energy by going to sleep-mode when there is no data to transmit. The energy consume when sensor node transmit the data, hence their radios are on for this purpose. So the attackers can seriously degrade the performance of WSN, if strategically important nodes are under sleep-deprivation attack [15]. In this attack, the attacker's usually forward unnecessary packets towards the target node so that to keep its radio on, hence consumes its battery power to completely drain and makes it unable to take part in the communication process.

V. TECHNIQUES TO DEFEND THREATS IN WSN

Security is a broadly used term encompassing characteristics of authentication, integrity, privacy, nonrepudiation and anti-playback [14]. The risk of the secure transmission of information over the network increases with increase in the dependency on the information provided by the network. In this section, we discuss the network security fundamentals and how the techniques are meant for wireless sensor networks:

Encryption:
That mechanism provides security against passive attacks like eavesdropping. Sensor network mostly run in public or wild area over inherently unconfident wireless channels. It is therefore insignificant for a device to eavesdrop or even add messages into the network. The traditional key to this problem has been two espouse techniques such as method authentication codes, symmetric key encryption schemes and public key cryptography [4].

Symmetric encryption:
It is also called as single l key cryptography. It uses a single key. In this encryption process the receiver and the sender has to agree upon a single secret (shared) key. Given a message (plain text) and the key, encryption produces one intelligible data, which is about the same length as the plain text was. Decryption is the reverse of encryption, and uses the same key as encryption [17].

Asymmetric encryption:
It is also called 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 public and private keys are related to each other by any mathematical means. In other words, data encrypted by one public key can be encrypted only by its corresponding private key[17].

Cryptography:
Cryptography constitutes the main theoretical concept, along with key infrastructures, underlying approaches that ensure integrity and confidentiality. Elliptic curve cryptography (ECC) has been recognized as a viable approach for WSN.ECC is a promising alternative to RSA-based algorithms, as the typical size of ECC keys is much shorter for the same level for security[18].

Artificial Intelligence:
A. Machine learning:
Machine learning in WSN helps to discover meaningful new correlations, patterns and trends, often previously unknown, by sifting through large amounts of data, using pattern recognition, statistical and mathematical

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

techniques. It can be useful not only in knowledge discovery, that is the identification of new phenomena, but also it can help in enhancing our understanding of known phenomena. In other words, machine learning techniques can help build decision-aid tools and facilitate analyzing of sensor data obtained from WSN.[19]

Applied to numerous WSN applications, machine learning algorithms provide tremendous flexibility benefits. Existing machine learning algorithms can be categorized by the intended structure of the model. Most learning algorithms fall into the categories of supervised, unsupervised and reinforcement learning. In the first category, machine learning algorithms are provided with a labeled training data set. This set is used to build the system model representing the learned relation between the input, output and system parameters. In contrast to supervised learning, unsupervised learning algorithms are not provided with labels (i.e. there is no output vector). Basically, the goal of an unsupervised learning algorithm is to classify the sample sets to different groups (i.e. clusters) by investigating this similarity between the input samples. The third category includes reinforcement learning algorithms, in which the agents learns by interacting with its environment (i.e. online learning). Finally, some machine learning algorithms do not naturally fit into this classification since they share characteristics of both supervised and unsupervised learning methods. These hybrid algorithms (often termed as semi-supervised learning) aim to inherit the strengths of these main categories, while minimizing their weaknesses. [20]

B. Computational intelligence:

Computational intelligence is the study of adaptive mechanisms that enables or facilitates intelligent behavior in complex and changing environments. These mechanisms include paradigms that exhibit an ability to learn or adapt to new situations, to generalize, abstract, discover and associate. CI is defined as the computational models and tools of intelligence capable of inputting raw numerical sensory data directly, processing them by exploiting the representational parallelism and pipelining the problem, generation reliable and timely responses and withstanding high fault tolerance. Paradigms of CI are designed to model the aspects of biological intelligence. CI encompasses paradigms such as neural networks, reinforcement learning, swarm intelligence, evolutionary algorithms, fuzzy logic and artificial immune system. CI provides adaptive mechanisms that exhibit intelligent behavior in complex and dynamic environments like WSNs. CI brings about flexibility, autonomous behavior and robustness against topology changes, communication failures and scenarios changes [21].

C. Fuzzy logic:

Classical set theory allows elements to be either included in a set or not. This is in contrast with human reasoning, which includes a measure of imprecision, or uncertainty, which is marked by the use of linguistic variables such as most, many, frequently, seldom, etc. This approximate reasoning is modelled by fuzzy logic, which is a multi-valued logic that allows intermediate values to be defined between conventional threshold values. Fuzzy systems allow the use of fuzzy sets to draw conclusion and to make decision.

D. Swarm intelligence:

SI originated from the study of collective behaviour of Societies of biological species such as flocks of birds, shoals of fish and colonies of ants. SI is the property of a system whereby collective behaviours of unsophisticated agents interacting locally with their environment cause coherent functional global patterns to emerge. While graceful but unpredictable bird-flock choreography inspired the development of particle swarm optimization, impressive ability of a colony of ants to find shortest path to their food inspired the development of ant colony optimization. The honey bee algorithm mimics foraging behaviour of swarms of honey bees [21].

Security protocols:

A. LEAP protocol:

LEAP is also a very popular security solution in WSN and it was proposed by Zhu et al in 2004. Localized encryption and authentication protocol (LEAP) is a key management protocol used to provide security and support to sensor networks. It uses micro TESLA (timed, efficient, streaming, loss-tolerant, authentication) to provide base station broadcast authentication and one-way-hash-key to authenticate source packet. This protocol is inspired by the idea that every message broadcasted between sensor nodes is different from another and comprise of different security requirements. In order to meet the variety of security [22].

B. SPINS:

It stands for Security protocols for sensor networks. It is an economical security scheme with low overhead. SPINS consist of two components called micro□□TESLA and SNEP. Micro TESLA's purpose is to provide authenticated broadcast, since this communication mode is standard in WSN. The problem solved by it is that the authenticated broadcast requires a costly asymmetric mechanism that sensor nodes cannot afford usually. The protocol emulates asymmetry by sending encrypted messages and key information independently [18].

C. SNEP:

SNEP: sensor network encryption protocol. SNEP provides a number of following advantages.

1) It has low communication overhead as it only adds 8 bytes per message.
2) Like many cryptographic protocols it uses a counter, but avoids transmitting the counter value by keeping state at both end points.
3) SNEP achieves semantic security, which prevents eavesdroppers from inferring the message content from the encrypted message.
4) Finally, SNEP protocol offers data authentication, replay protection and weak message freshness[23].

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 4, April 2015

V. CONCLUSION

The basic idea of this paper is to provide detailed information about security issues and types of attacks WSN is exposed to some possible measure for countering such attacks. An attempt has been made to explore security mechanism. This survey provides a baseline for the future researchers to come up with smarter security mechanism and make network more secure.

REFERENCES

[1]. Joshua Muscatello,JoshuaMartin,"Wireless Network Security",April,2005.
[2]. NehaSingh, Prof.RajeshwarlalDua,VinitaMattur,"International Journal Of Advanced Research In Computer Science And Software Engineering",Volume 2,Issue 5,May 2012,Issn:2277128x.
[3]. MarjanRadi, BehnamDezfouli, Kamalrulnizam Abu Bakar,MalreyLee,"Multipath Routing In Wireless sensor Networks: Survey And Research Challenges",Issn:1424-8220, 9 january 2012.
[4]. C.K.Marigowda,ManjunathShingadi,"Security Vulnerability Issues In Wireless Sensor Networks:AShortSurvey",International Journal Of Advance Research In Computer And communication Engineering .Vol.2,Issue 7,July 2013.
[5]. Dr.G.Padmavathi,Mrs.D.Shanmugapriya,"A Survey Of Attacks,Security Mechanisms and Challenges in Wireless Sensor Networks"(IJCSIS) International Journal of Computer Science and Information Security,Vol.4,NO.1 & 2,2009 .
[6]. AashimaSingla, RatikaSachdeva,"Review on Security Issues and Attacks in Wireless Sensor Networks", Vol. 3, Issue 4,Aprile 2013,Issn:2277128X.
[7]. John Paul Walters ZhengqiangLiag, Weisongshi, and VipinChaudary," wireless Sensor Network Security: A Survey".
[8]. JaydeepSen, "A Survey on Wireless sensor Network Security", International Journal of Communication Networks and Information Security , vol. 1,Number 2,August 2009.
[9]. Mona Sharifnejad, MonsenSharifi, MansourehGhiasabadi and SarenBeheshti,"A survey on Wireless Sensor Networks Security", SETIT 2007,fourth international Conference: Science of Electronic Technologies of Information and telecommunication, March 05-29,2007-Tunisia.
[10]. David Martins and HerveGuyennet,"Wireless Sensor Network Attacks and Security Mechanism: A Short Survey", 2010,Tweleth International Conference on Network-Based Information Systems.
[11]. Yong Wang,GarhanAttebury,andByrav Ramamurthy," A Survey of Security Issues in Wireless Sensor Networks" 2nd quarter 2006,Vol 8,NO.2 IEEE Communication surveys.
[12]. M.Yasir Malik, "An Outline of Security in Wireless Sensor Networks: Threats, Countermeasures and Implementations", Wireless Sensor Networks and Energy Efficiency: Protocols, Routing and Management DOI:10.4018/978-1-4666-0101-7.CH024.
[13]. Chris Karlay, David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Counter Measures" Adhoc Networks(Eleseviev) Page:299-302,year 2003.
[14]. Al-Sakib Khan Pathan,Hyung-Wood Lee,ChoongSeon Hong, "Security in Wireless Sensor Networks: Issues and Challenges",Isbn:89-5519-129-4,Feb 2006.
[15]. TahirNaeem,Kok-Keongloo,"Common Security Issues and Challenges in Wireless Sensor Networks and IEEE 802.11 Wireless Mesh Networks". Wireless Sensor Networks: A survey", To Appear in IEEE Communications Survey Tutorials, Volume 13, Issuse 1,2011.
[16]. PriyaMaidamwar, NekitaChavhan,"A Survey on Sercuity Issues to Detect Worm Hole Attack in Wireless Sensor Network" , International Journel on Adhoc Networking Systems(IJANS),Vol.2,No.4,October 2012.
[17]. Jawahar Thakur, Nagesh Kumar ," Des, Aes and Blow Fish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", International Journal of Engineering Technology and Advanced Engineering , Vol.1, Issue 2, December 2011.
[18]. Eric Platon and Yuichi Sei, "Security Software Engineering in Wireless Sensor Networks", Progress in Informatics, NO.5, PP.49-64,(2008).
[19]. Aziz Nasridinov, Young_Ho Park, "A Survey on Machine Learning Techniques in Wireless Sensor Networks", Advanced Science and Technology Letters , Vol.30, (ICCA 2013).
[20]. Mohammad Abu Alsheikh, Shaowei Lin , DusitNiyato and Hwee-Pinktan, "Machine Learning in Wireless Sensor Networks: Algorithms, Strategies and Applications",18 May 2014.
[21]. Raghavendra V Kulakarni, Anna Forseter, Ganesh Kumar ,Veayagamoorthu, "Computational Intelligence in
[22]. DelanAlsoufi , KhaledElleithy , Tariq Abuzaghleh and Ahmad Nassar, "Security in Wireless Sensor Networks- Improving the Leap Protocol", International Journal of Computer Science and Engineering Survey(IJCSES) Vol.3,No.3, June 2012.
[23]. Ritu Sharma , YogeshChaba, Yudhvir Singh," Analysis of Security Protocols in Wireless Sensor Networks", Int.J.Advanced networking and Applications. Vol.2, Issues:3, Pages:707-713,2010.