Analysis of Security Attacks and Security Protocols of Wireless Sensor Network: Review

Amrita Tiwari, Rohan Varma, M.M.S Rauthan, Varun Barthwal

Abstract—Wireless Sensor Network presents technology that is emerging on the market and in upcoming "future" it will be having more diverse use in many fields. WSN is a group of sensor nodes cooperating to form a large network. The key feature of WSN is low power, low energy, and low memory. This paper studies various security concerns concerning WSN and also includes some security protocols used to achieve security in the network.

Index Terms— Keywords- WSN, routing protocols, security attacks, security

———————— ◆ ————————

1 Introduction

A distributed network containing independent small-sized nodes is known as Wireless Sensor Network (WSN) [1]. WSN is an emerging research area field in the twenty-first century [5]. Sensor nodes are generally autonomous, inexpensive, low powered and self-directed. Interaction between sensor nodes is wireless also process signals smartly and transmit data over the network.

The greatest challenges for WSN are limited size and security issues [4]. Main challenges are as follows –

- Memory
- Delay in communication
- Distant or unattended nodes

WSN used in the fields of military defense, remote control, smart sensing, neighbor node discovery and many more real-time applications [3]. Similarity and difference between WSN and MANET are shown in table 1.

TABLE 1
SIMILARITY AND COMPARISON BETWEEN WSN AND MANET

WSN	MANET	Similarity
Focus on communication with surroundings	focus on facilities like laptop, PDAs, etc.	Both are distributed wireless network
For WSN entirely new Quality of Service requires which also takes energy explicitly into account	Quality of Service in a MANET traditionally dictated by conventional application	use of multihop routing
Symmetry key cryptography	Public key cryptography	Both networks use a wireless channel placed in unlicensed spectrum
WSN is smaller, powerful	Less in compare to WSN	self-management is necessary
Supports specialized traffic pattern(routing)	Use either source routing or distance vector protocol	

Sensing unit which is used to sense the surroundings, Processing unit which is used to computes confined permutation of data already sense and finally Communication unit which is used to share the processed information among neighboring sensor nodes. The building block of sensor nodes is shown in figure 1.

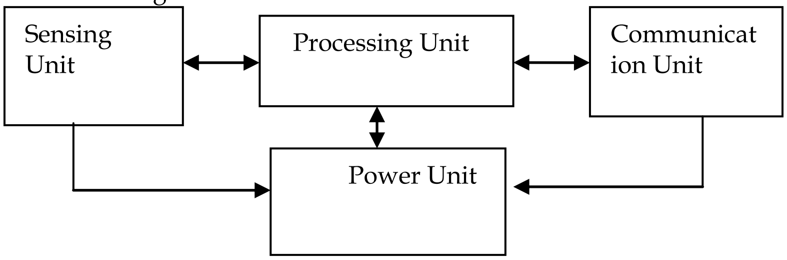

Fig.1. Sensor nodes building block

2 Wireless Sensor Networks

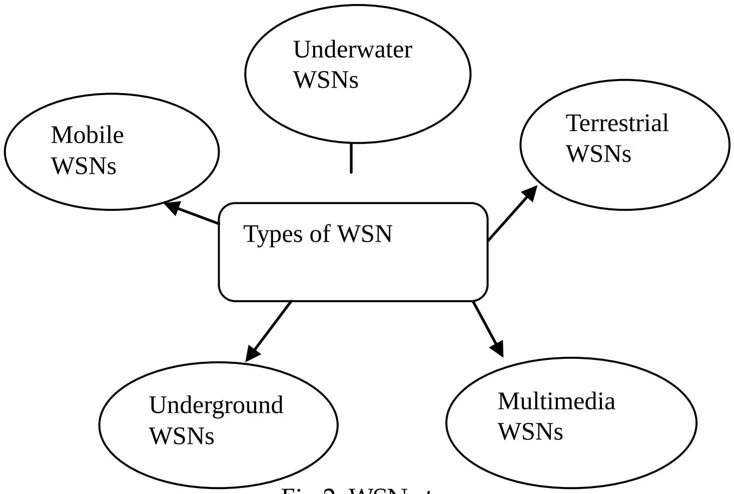

Fig.2. WSNs types

2.1 Mobile Wireless Sensor Networks (MWSNs)

Mobile Wireless Sensor Networks (MWSNs) is a combination of MANET and WSN properties. MWSNs are WSN which are more versatile than the stationary sensor networks [4][8]. The

- *Amrita Tiwari, Rohan Varma, M.M.S Rauthan, Varun Barthwal*
- *School of Engineering and Technology, H.N.B.G.U, Srinagar Garhwal*

stationary sensor has a drawback as if any of the nodes fail to work; it does not adopt any topological changes but easily can be done in a mobile sensor. Other advantages of mobile sensor are battery energy frequency, better and improved coverage.

In spite of various advantage its main concern and needed to be solved i.e., it is more vulnerable to security attacks. The threats can occur from anyway because these nodes are mobile and without any centralized infrastructure forms a temporary network [6][7]. The reason for not including any complex security mechanism or any algorithms for security is due to resource constraints.

MWSNs still had many challenges as dynamic network topology, mobility of sin, localization and many more.

2.2 Underwater Wireless Sensor Network (UWSNs

Autonomous underwater vehicles are used for gathering information in UWSNs. But most challenging is to build the underwater wireless communication due to some reasons like propagation delay, bandwidth or sensor failure [4].

For especially short-range distance optical communication is a feasible solution. It is an enormous area for research but there are several difficulties to deal with such as complex deployment environment especially in 3-D space, limited battery power available in nodes, high error rate and large propagation delay [8]..

2.3 Wireless Underground Sensor Networks (WUSNs)

WUSNs are an exceptional extension of TWSNs (Terrestrial WSN) but are expensive in terms of maintenance, deployment, and equipment cost consideration [8]. Nodes are completely underground or maybe in an open space like a cave or completely embedded in dense rock or soil. To retrieve information additional downstream nodes are located above surface level.

There are many challenges like power consumption, topology design, antenna design, environmental extremes.

2.4 Wireless Multimedia Sensor Networks (WMSNs

WMSNs contains small sensor node proposed to enabled tracking, habitation, monitoring, ecological monitoring and many more in a form of images, audios, and videos [8][10]. They can be used to sense, compute, actuate and communicate.

The challenges in WMSNs include data processing, storage and power, high energy consumption, signal detection and compressing technique. The basic features for WSNs routing protocols include the use of mini hops, maximum available power, less load of traffic and low latency [4].

2.5 Terrestrial Wireless Sensor Networks (TWSNs)

TWSNs includes hundreds to thousands of cheap WSNs are installed. The deployment can be in two ways- in a structured or unstructured network [13].

Sensor nodes established randomly from a plane into the area of target comes under unstructured network whereas four placements introduced as grid, optimal, 2-D or 3-D placement models comes under structured network [8].

Usage of battery is a challenge. Therefore battery is equipped with the solar path. Solar cells used as a secondary power medium.

3 WSNs Routing Protocols

Routing Protocols are classified into three as Data-centric protocols, Geo routing protocols and Hierarchical routing protocol [18]. Evaluation of different routing protocols is shown in table 3.

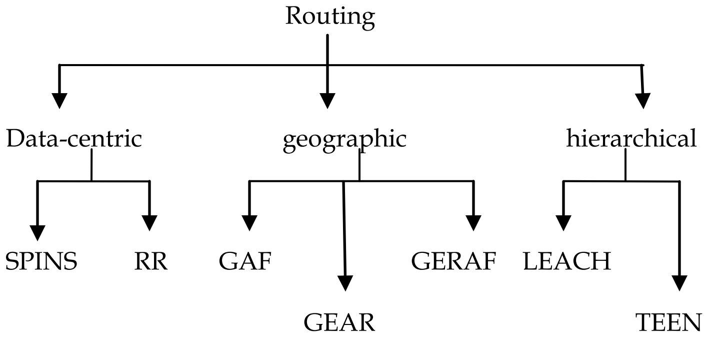

Fig.3. Classification of Routing Protocols

***Table 2** comparison among different routing protocol*

	Classification	**Extensibility**	**Mobility**	**Real-time**	**Lifetime**	**Multipath**	**robustness**
SPINS	Data-centric	General	Possible	No	Long	Yes	general
RR	Data-centric	Good	Very limited	No	Long	No	good
GAF	Geographical	Good	Limited	No	Longer	No	general
GEAR	Geographical	Good	Limited	No	Longer	No	general
GERAF	Geographical	Good	Limited	No	Longer	No	general
LEACH	Hierarchical	Good	Fixed BS	No	Longer	No	good
TEEN	Hierarchical	Good	Fixed BS	Yes	Long	No	good

4 WSNS SECURITY REQUIREMENTS

Basic security goals for WSN can be classified into two-primary goals and secondary goals [19]. Data confidentiality, data availability, data authentication, data integrity are the primary goals and freshness, self-organization, and time Synchronization are secondary goals.

1. Confidentiality- it refers to protect data or hide data from any unknown attacker node. It should be understandable only to desired recipients [9]. To provide data confidentiality we can adapt two encryption schemes-symmetric encryption or asymmetric encryption [1]. However, there is no single mechanism that provides better security due to the size of the key and computational effort [1][5].
2. Data authentication- it ensures that two-way communication should be valid and done by trusted nodes [1].
3. Data integrity- it ensures the message could not be changed tampered or altered during communication [9]. In WSNs, an attacker node can change message due to unreliable communication channels [11]. Data integrity is not efficient for wireless communication.
4. Data availability- it ensures data is available and accessible whenever needed. It works against for Denial of Service (DoS) attacks [11].
5. Data freshness- data sent received should be new and latest it ensures. It helps in preventing replay attacks [1].
6. Self-organization-it ensures sensor nodes are capable of Adding or removing nodes themselves as nodes are densely deployed and ad-hoc network [9]. They should sufficient enough to self-organize and self-heal in any circumstances [5][9].

5 TYPES OF SECURITY ATTACKS

Security attacks in WSN are roughly categorized into three as follows [5]:

1. The goal of the attacker
2. Attacker's location
3. Protocol layer based

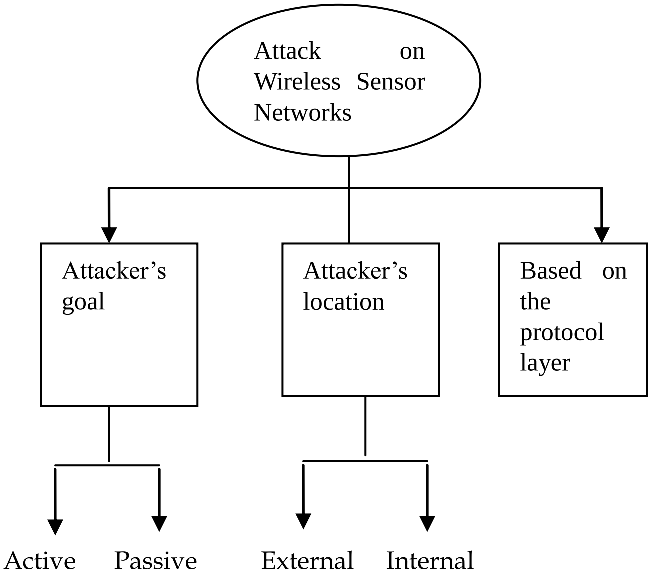

***Fig.4.** Security Attacks*

1. Goal of attackers
   - Active attacks vs. passive attacks

Active attacks include black hole, DoS, jamming, sinkhole, spoofing, flooding, replay and false node attacks whereas passive attacks include eavesdropping, monitoring, analysis attacks [5].

2. Attacker's location
   - External attacks vs. internal attacks

External attacks include eavesdropping, DoS, resource exhaustion and eavesdropping. It can be prevented by using encryption or digital signature [12] whereas internal attacks harm to network silently and hard to detect as they are internal nodes only. It includes attacks such as black hole, gray hole and malicious node [5].

3. Protocol layer-based- attacks in different layers and their defense mechanism in table 4 [23].

- Physical layer- In this layer attacker tends to jam the radio signals and changes the entire working of a network [5]. Attacks like jamming, DoS, tampering attacks.
- Data link layer- In this layer attacker interrupt like modifying MAC protocol, duplicate or replace data frames. Attacks like collision, exhausting happens [5].
- Network layer- In this layer attacker's motive is to disrupt the path from sensor nodes to sink nodes. Attackers generally attack routing protocols of WSNs. Attacks like a sinkhole, wormhole, hello flooding, etc. include.
- Transport layer- attacker request for new link till resources they want gets exhausted or reaches to their highest limit. Attacks like flooding, de-synchronization is common.
- Application layer- it affects the size and capacity of the network like by sending huge of no use data to base station hence wasting bandwidth and consumes nodes energy [5]. Attacks like data corruption, Overwhelm, malicious code are common [14].

TABLE 3
LAYER-WISE ATTACKS

Layer	Threats	Defense mechanism	Protocols
Physical layer	▪ Jamming ▪ Tampering	Key-management method, tamperproof	Frequency hopping
Data-link layer	▪ Collision ▪ Exhausting	▪ error correcting code ▪ rate limitation	TinySec, LMAC
Network layer	▪ Sybil ▪ Selective forwarding ▪ Sinkhole ▪ Hello flood ▪ Wormhole	▪ authentication ▪ Redundancy probing ▪ Authentication monitoring ▪ Two-way authentication ▪ Flexible routing	LEACH
Transport layer	Flooding, De-synchronization	Limited connection number	DSR protocols
Application layer	Sniffing, Clone attack	Unique pair wise key	LEAP

6 Common WSN attacks

□ Sinkhole attacks- the malicious node attracts the traffic by faking routing information in a network [15][16]. Most of the nodes get attracted as every node want to choose the shortest possible path towards base stations.
Prevention- it can be prevented by using geographical routing protocols.

- Selective forwarding- it makes believe all nodes are reliable and trustworthy to forward messages in a network [9]. If there is a certain dropping of the message instead of forwarding all it is a selective forwarding whereas dropping all messages it is known as black hole [15].
  Prevention- such type of attacks can be prohibited by using multipath routing.
- Sybil attack- multiple identities of a single node present in a different location of a network [9]. This leads to confusing the other neighboring nodes. It affects the fault tolerance schemes of the sensor network.
  Prevention- It can be prohibited by using efficient protocols for gateway or base station.
- Hello flood attack- a lot of "HELLO" message is flooded over a network to waste energy and also leads to network congestion.
  Prevention- detected by examining the average signal strength of all nodes located in a network.
- Wormhole attack- in this one or two malicious node is present in a network in a different location [9]. A valid node (sender) broadcast its information to one of this malicious node assuming as a valid neighboring node. This node tunnels the information to its partner node situated at another location then further send to neighboring nodes [9][15]. If the combination of the wormhole and selective forwarding is done with Sybil it is hard to detect [17].
  Prevention- it can be detected and prevented using geographic and temporal information by packet leashes method.

7 Wireless Sensor Networks Security Protocols

The different Security protocols for WSN [18][19] are proposed by different researchers are:

7.1 Secure Protocol for Sensor Networks (SPINS)

SPINS is proposed by Adrian Perrig et al.; 2002. Two secure constructive blocks of SPINS- SNEP (Secure Network Encryption Protocol) and µTesla [20].Working of SPINS can be summarized in three simple steps firstly a sender advertises the metadata. The interested received node then sends REQ packet and finally, the sender node responds by sending data packet [21][22]. Secure Network Encryption Protocol (SNEP) basically supports base to node communication [23]. It works in two ways [23][24]. First is using counter mode. The sender increases counter value every time after sending each message and receiver on another hand verifies received messages have an increasing counter value. It is not a good approach. The second approach is sender creates 64-bit random number and broadcast request message and use that random no in the computation of MAC field. If MAC of response message verified, the sender will get to know about the reply of the receiver node. Therefore SNEP updates the counter value on both sides of communication [23]. SNEP has various advantages- low communication overhead, use of counter which is common among sender and receiver, semantic security which helps in preventing eavesdropping and data authentication using MAC.
SNEP Packet format:

Preamble	DeS	ScR	Am	LeN	Data	MAC
6	2	2	1	1	29	4

We have µTesla for big reasons over a pure Tesla as [24][26][27]:

- to authenticate initial packet pure tesla uses a digital signature which is quiet expensive whereas only symmetric methods used by µtesla.
- One-way key chain in the sensor node is expensive so some authenticated sender is restricted in µtesla.

In simple language, we can explain the working of µTesla where base stations and nodes in a network to be time-synchronized [24]. Base station computes a MAC and a secret key together. When a node in a network gets a packet they put them in temporary storage until the base station did not discloses the secret key. Once secret key disclosed, they authenticate packet which is sent by the respective base station. One major drawback in this process is some initial information must be told to nodes before beginning an authentication process [9].

7.2 LISP

A Light Security Protocol for WSN (LISP) is proposed by the park and shin et at.; 2004. It works on a well-organized rekeying mechanism system and keeps a balance between the usage of resources and the need for security [1][25]. It helps to prevent attacks like active attacks, passive attacks, DoS such as jamming, collision, etc. [25]. LISP's key hierarchy is shown below in figure 5.

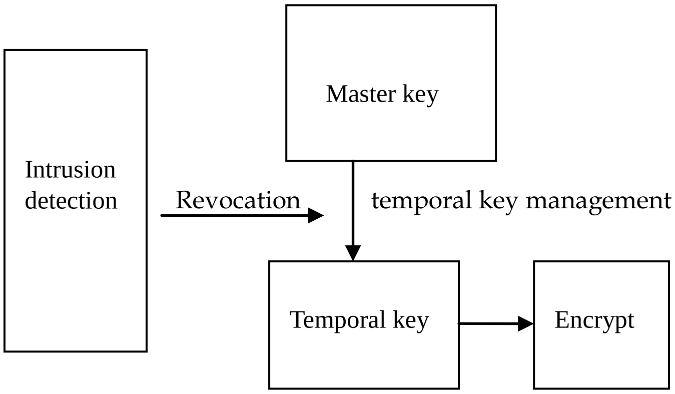

Fig.5. the key hierarchy for LISP

It renews the shared key time to time which helps in solving the problem of reusing of key stream and gradually also increases scalability. Recovery algorithm and authentication are combined for rekeying. Key server broadcast new key before encryption and decryption [1][23]. Key received is authenticated by client node and hence recovers all missing keys. The entire network divides into groups and every group has one group head (GH) which acts as KS which control the security of group [25]. That's why it is suitable for large systems. LISP's is advance in providing high-level security and maximizing energy efficiency.

Packet for LISP:

SC	PB	C1	C2	C3	-----	CL	MAC

SC- sequence counter
PB- position bit

7.3 LLSP

Link-Layer Security Protocol (LLSP) for WSN is power efficient protocol proposed by Lightfoot et at.; 2009. The goal is to the designed protocol which is more efficient than TinySec [1]. It provides three basic security services- message authentication, confidentiality, and replay protection. The best mode of operation for encryption implemented is AES-CBC as it provides semantic security [28].

A packet of TinySec and LLSP has the same concept. The only difference is in the size of the counter value (ctr) [11] [28]. The counter is removed in LLSP as both sender and receiver maintain a synchronous counter and value of counter not needed to be transmitted [28]. It is examined that after using LLSP the energy consumption and latency reduction is improved in comparison to TinySec. It is not applicable to a large network.

The packet format for LLSP:

preamble	DeS	ScR	Am	Len	Data	MAC
6	2	2	1	1	29	4

7.4 LEAP

Localize Encryption and Authentication Protocol (LEAP) for WSN proposed by Sencun Zhu et al.; 2003. It supports multiple keying mechanisms [2][30]also known as key management protocol. LEAP introduces four types of symmetric key mechanism [29].

• an individual node keys:
It is shared among a node and its corresponding base station. Computational overhead is negligible due to the efficiency of pseudo-random functions [29]. The equation for computation is:

$Ku= pKi(idu)$
Where
p - Pseudo-random function
Ki- initial key
idu- the identity of node u.

• a pairwise keys:
It is shared among a node and its neighboring nodes [29]. The equation for computation is:

$Kn= pKi(idn)$
$u \rightarrow *: idn, Nonceu$
$n \rightarrow *: idn, MACKn(Nonceu | idn)$
Thus,
$Kp= pKn(idu)$

• a group keys:
It is known as the global key because it is shared among all nodes in a network

• A cluster keys:
It is a unique case of group key [9][29] which is shared with

multiple neighbors of a node. Its work is to broadcast message nearby in a network securely. The equation for computation is:

$u \rightarrow ni(Kc)Kpi$

LEAP uses RC5 for encryption. For broadcast authentication based on one-way key chains, it is a better option. It has many advantages as [9][29][1]:

- The need of base station is least and is efficient in communication and energy.
- The local communication security mechanism is its priority. By this, it protects message sent from nodes.

Disadvantages are [29]:

- The only base station is risky.
- As it is four key mechanisms maintenance and cost of capacity needed to store them is a bit high.

7.5 TinySec

Designed by Karlof et al.; 2004 for overcoming the limitations of SNEP. TinySec is specially designed for link-layer security of WSNs. The only difference between SPINS and TinySec is TinySec didn't use counter.

Message integrity and authenticity can be best done using CBC-MAC [2][31]. MAC specifies of 4 bytes less than SPINS [9]. CBC-MAC is better and fast as it based on a block cipher and also many cryptographic primitives are less [23].

TinySec introduces two security formats as – for Authenticated and Encrypted message (TinySec-AE) and for Authenticated message (TinySec-Auth) [1][9].

TinySec-AE packet, size of the payload is 29 bytes with 8 bytes of a packet header. In TinySec-AE, TinySec has to encrypt both with a MAC. In TinySec-Auth packet, the size of the payload is also 29 bytes with packet header of 4 bytes [9]. In TinySec-Auth, the whole packet is authenticated with MAC except payload [9]. A key mechanism for TinySec is of three type- per-link key, single network-wide key and group key [30]. There is a gradual rise in the computational and energy costs of TinySec.

TinySec packet format:

Preamble	DeS	Am	LEN	ScR	DATA	MAC
6	2	1	1	2	29	4

7.6 ZIGBEE

ZigBee is well-known as wireless communication technology [32][33]. ZigBee is built on IEEE 802.15.4 standard. 128 bit AES based encryption mechanism works best for ZigBee [34][35].

ZigBee coordinator has three roles in ZigBee as follows [36]:

- Trust Manager- authenticate devices who want to connect with the network.
- Network Manager- require keys are maintained and distributed in a network
- Configuration Manager- it checks on the security of devices.

ZigBee operates in two ways - residential mode with low-security demands and commercial mode with high-security demands (Boyle & Newe, 2007). Security services lie and interact between Application Support Sublayer (APS) and Network layer (NWK)[37].

There are three kinds of keys for security:

- Link key- it is used by the APS layer. It can be distributed by a trust center or preconfigured or installed on devices using SKKE [37].
- Network key- it can be preconfigured or transported by a trust center. It used to protect and secure groups in a network shared by all devices [37].
- Master key- this is optional and can be preinstalled or installed by a trust center [37]. If it comes in use, it used to generate other two above keys.

Diverse security protocols are used according to their specializations and require. Comparative analysis between the securities protocols of WSN shown in table 4.

TABLE 4

DIFFERENT SECURITY PROTOCOLS

Protocol	Confideentiality	Freshness	AvaIlability	AutHentication	Integrity	Encryption	Key Management
SPINS	Yes	Yes	No	No	Yes	CTR-RC5	YES
LISP	Yes	Yes	Partial	No	Yes	Stream cipher	Yes
LLSP	Yes	Yes	No	Yes	Yes	AES-CBC	No
LEAP	Yes	Yes	No	No	No	RC5	Yes
TinySec	Yes	No	No	Yes	No	Skip-jack CBC-RC5	No
ZigBee	Yes	Yes	No	Yes	Yes	AES 124-bit	Yes

CONCLUSION

This paper highlights types of WSN, security goals, security attacks, and existing different types of WSN security protocols. Providing Security is a big challenge in a WSN. WSN is a productive and only need is to choose a correct approach for getting maximum beneficial output. Some applications using WSN technology such as military and industry requires secure communication. In this paper, we also study the major security threats and prevention. To achieve security requirement various security protocols are also have been projected. All protocols are unique in their ways.

REFERENCES

[1] John GichukiNdia (2015), “A survey of Security Protocols for Wireless Sensor Networks”

[2] Jitender Grover, Shikha Sharma, and Mohit Sharma, “Optimized GAF in Wireless Sensor Network”, IEEE 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO 2014), Amity University, Noida, DOI:10.1109/ICRITO.2014.7014686, pp. 01-06, October 8-10, 2014.

[3] Sharma, K. and Ghose, M. (2010) Wireless Sensor. An Overview on Its Security Threats.IJCA, Special Issue on “Mobile Ad-hoc Networks” MANETs, 42-45.

[4] Nptel online tutorials.

[5] A.K Nuristani, Jawahar Thakur (2018) Security Issues and Comparative Analysis of Security Protocols in Wireless Sensor Networks: Review.

[6] Cho, J.-H., Swami, A. and Chen, R. (2011) A Survey on Trust Management for Mobile Ad Hoc Networks. IEEE Communication surveys &tutorials, 13, 562-583.

[7] Djenouri, D., Khelladi, L. and Badache, N. (2005) A Survey of Security Issues in Mobile Ad Hoc Networks. IEEECommunications Surveys, 7, 2-28.

[8] Muhammad Umar Aftab1,5, Omair Ashraf2, Muhammad Irfan3, Muhammad Majid4, Amna Nisar5, Muhammad Asif Habib5. (2015) A Review Study of Wireless Sensor Network and its Security. http://dx.doi.org/10.4236/cn.2015.74016

[9] Ritu Sharma, YogeshChaba, Yudhvir Singh (2010) Analysis of Security Protocols in Wireless Sensor Network

[10] Poojary, S, and pai, MM. (2010) multipath Data Transfer in Wireless Multimedia Sensor Network. 2010 International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), Fukuoka, 4-6 November 2010, 379-383

[11] KrzystofDaniluk and EwaNiewiadomska-Szynkiewiez (2012) A survey of Energy Efficient Security Architecture and Protocols for Wireless Sensor Networks.

[12] KahinaChelli, “security issues in Wireless Sensor Networks: Attacks and countermeasures" Proceedings of the World Congress on Engineering, London, U.K. (Vol. 1, 2015).

[13] Akyildiz, I.F., Su, W.L., Sankarasubramaniam, Y. and Cayirci, E. (2002) A Survey on Sensor Networks. IEEE Communications Magazine, 40, 102-114. http://dx.doi.org/10.1109/MCOM.2002.1024422

[14] David Martins and HerveGuyennet (2010), Wireless Sensor Networks Attacks and Mechanisms: A short survey.

[15] Jitender Grover and Sikha Sharma (2016), Security Issues in Wireless Sensor Network- A Review.

[16] JyotiAhlawat, MukeshChawla and Kavita Sharma (2012), Attacks and Countermeasures in Wireless Sensor Network, (IJCSCE).

[17] Banta Singh Jangra and VijetaKumawat (2012), A Survey on Security Mechanisms and Attacks in Wireless Sensor Networks, (IJEIT).

[18] Abhishek Pandey and R.C.Tripathi, "A Survey on Wireless Sensor Networks Security", International Journal of Computer Applications, Volume 3, Issue 2, pp. 43-49, June 2010.

[19] Rajat Gupta, KaushalSultania, Pallavi Singh, Archit Gupta, "Security for wireless sensor networks in military operations", Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, pp. 1-6, 2013.

[20] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J.D. Tygar (2001), SPINS: Security Protocols for Sensor Networks. {perrig, Szewczyk, culler,tygar}@cs.berkeley.edu

[21] Jitendra Grover, Sikha Sharma and Mohit Sharma (2014), Optimized GAF in Wireless Sensor Network.

[22] Jitendra Grover, Sikha Sharma and Mohit Sharma (2014), Location- Based Protocols in Wireless Sensor Network- A review.

[23] M.Revanti and Dr. B.Amutha (2017), A survey on Security Protocols in Wireless Network.

[24] Adrian Perrig, Robert Szewczyk, Victor Wen, David Culler, J.D. Tygar (2002), SPINS: Security Protocols for Sensor Networks.

[25] Taejoon Park and Kang G.Shin (2004), LiSP: A Lightweight Security Protocol for Wireless Sensor Networks.

[26] Adrian Perrig, Ran Canetti, J.D. Tygar, and Dawn Song. Efficient authentication and signing of multicast streams over lossy channels.In IEEE Symposium on Security and Privacy, May 2000.

[27] K. S. J. Pister, J. M. Kahn, and B. E. Boser. Smart dust: Wireless networks of millimeter-scale sensor nodes, 1999.

[28] JianRen, Tongtong Li and Dean Aslam, A Power-Efficient Link-Layer Security Protocol (LLSP) for Wireless Sensor Networks.MI 488824-1226.

[29] DelanAlsoufi, KhaledElleithy, Tariq abuzaghlehand Ahmad Nassar1 (2012), Security in Wireless Sensor Networks- Improving the LEAP Protocol.

[30] Jitender Grover, Shikha Sharma, and Mohit Sharma, “ReliableSPIN in Wireless Sensor Network”, IEEE 3rd InternationalConference on Reliability, Infocom Technologies andOptimization (ICRITO 2014), Amity University, Noida, DOI:10.1109/ICRITO.2014.7014694, pp. 01-06, October 8-10, 2014.

[31] Sencun Zhu, Sanjeev Setia and SushilJajodia, “LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks”, 10th ACM Conference on Computer and Communications Security (CCS 03), pp. 62-72, October 2010.

[32] Jitender Grover &Reena Rani, "Probabilistic Density-Based Adaptive Clustering Scheme to Improve Network Survivability in WSN", IEEE Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT 2014), Hefei, Anhui, China, DOI: 10.1109/ICCCNT.2014.6963132, pp. 1-7, July 11-13, 2014.

[33] Daojing He, Sammy Chan, Mohsen Guizani, Haomiao Yang, Boyang Zhou, " Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, Vol. 26, Issue: 4, pp. 1129-1139, 2014.

[34] Ritu SharmaYogeshChaba, Yudhvir Singh. Analysis of Security Protocols in Wireless Sensor Network.Int.j Advanced networking and applications,

volume:02,Issue:03, pages- 707-713,(2010).

[35] Monika Bhalla, NitinPandey, Brijesh Kumar. Security Protocols for Wireless Sensor Networks. 2015, International Conference of Green computing and Internet of Things (ICGCIoT).

[36] ZigBee Specification v1.o: ZigBee Specification (2005), San Ramon, CA, USA: ZigBee Alliance.

[37] OmojokunG.Aju (2015), A survey of ZigBee Wireless Sensor Network Technology: Topology, Applications, and Challenges. J.S. Bridle, "Probabilistic Interpretation of Feedforward Classification Network Outputs, with Relationships to Statistical Pattern Recognition," *Neurocomputing – Algorithms, Architectures and Applications,* F. Fogelman-Soulie and J. Herault, eds., NATO ASI Series F68, Berlin: Springer-Verlag, pp. 227-236, 1989. (Book style with paper title and editor)