IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.6, Issue.10, Oct. 2018 E-ISSN: 2347-2693

Security Issues and Comparative Analysis of Security Protocols in Wireless Sensor Networks: A Review

A.K. Nuristani[1*], Jawahar Thakur[2]

[1]Dept. of Computer Science, Himachal Pradesh University, Shimla, India
[2]Dept. of Computer Science, Himachal Pradesh University, Shimla, India

[*]*Corresponding Author: nuristani4u@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 10/Oct/2018, Published: 31/Oct/2018

Abstract- Wireless sensor network (WSN) is a wireless network with large number of sensor nodes or it could be defined as a set of distributed devices which could be used to monitor sensible and natural conditions. These sensors can execute processing and sensing tasks, and additionally equipped for communicating with each other. Because of the extensive area of its applications it became one of the premier research topics recently. The main objective of wireless sensor network is regularly to gather sensing data from all sensors to particular sink nodes (base stations) and after that performing additionally operations at these sink nodes. Currently wireless sensor networks are available as a subject at advanced undergrad and graduate levels at some universities around the world. One of the challenges in WSNs is to devise and implement high security protocols with limited resources. This paper debated the security issues; challenges and protocols that are discussed and reviewed on the basis of attributes (confidentiality, availability, freshness, encryption methods, MAC authentication, key management, attacks protected and scalability) and tabulated WSNs security protocols, on the basis of (authors, protocols, advantages, disadvantages and applications) based on researches done by the researchers.

Keywords—WSNs, Attacks in WSN, Security Protocols

I. INTRODUCTION

Wireless communication technologies are experiencing fast developments. The most recent couple of years have encountered a lot development in research in the field of wireless sensor networks (WSNs) [1]. Wireless sensor networks (WSNs) are a standout amongst the most usable and significant technologies in the twenty first century. Wireless sensor networks are composed of vast number of inexpensive, low power and multi-functional sensor nodes which are used in any area which we need [2]. The generation of large-scale sensor networks interconnecting a few hundred to a couple of thousand sensor nodes opens up a few specialized difficulties and massive application opportunities. Wireless sensor networks have moved from the research space into the real world with the business accessibility of sensors with networking abilities. Organizations, for example, Crossbow (www.xbow.com) and Sensoria (www.sensoria.com) have risen as providers of the important equipment and software building blocks [3]. This paper emphasis on security issues in WSNs,

For the most part WSNs are used to gather data from different areas of physical world and furthermore they are deployed in controlled and uncontrolled locations, so wireless sensor networks are insecure by their applications and deployment nature. These networks have various limitations like node (less computational power, less memory, less energy and so on.), network (the network is acting as mobile ad-hoc network) and physical limitation (deployed in various areas like public and hostile environments) which makes them completely vulnerable against different security attacks. The main challenge which effects on security and reliability of sensor networks is the ad-hoc nature of it. Due to the restricted computational and processing compels ordinary security methods and strategies are not appropriate to look after Authentication, Availability and Integrity in WSN [4].

Wireless sensor networks (WSNs) are amazingly vulnerable and helpless to outside and inside attacks as they comprise of various devices with limitations like; less memory, related low energy and low battery power. In WSNs the nodes are communicating with wireless links. In WSNs still there are unsolved issues and security is one of the most important research issues [4]. WSN networks are deployed in hostile areas.

This paper contains four sections; first section is related to introduction to WSNs, security objectives and attacks in

wireless sensor networks. Section II contains the related works done by researchers earlier. Section III contains the performance analysis of some security protocols in WSNs based on their attributes, advantages, disadvantages and applications and section IV contains conclusion and future directions of the paper.

WSNs Security Objectives:
This part, will present the primary security objectives for WSNs which are outlined in data authentication, data integrity, data confidentiality, data availability and data refreshing.

A. Data Confidentiality
Data confidentiality refers to protection of data and messages from a passive attacker and it could be one of the most important issues in network security. It is very important to have a safe channel in a WSN. In order to have a protection shell against the traffic analysis attack sensors and public keys must be encrypted. The typical method for keeping sensitive data secure is to encrypt the information with a secret key which would be available only for the intended nodes [5].

B. Data Integrity
Data confidentiality refers to security (protection) of data and information from harmful nodes; though, it can't prevent data from being changed by illegal people. Data integrity guarantees that the message won't be changed through communication. A harmful node can make the system doesn't work properly by disrupting the message. Besides that the messages may also be disrupted in the absence of harmful node during the transmission of it [6].

C. Data Authentication
As WSNs use public wireless environment, they require authentication methods to get out messages and deceptive packets which are coming from malicious nodes. With authentication methods the nodes which are in contact with each other would confirm their identity very easily. Now suppose that there would be no authentication, and then a harmful node would carry on as it was an alternate node and might get some delicate information and furthermore disrupt appropriate activity of other nodes. If there are only two nodes are in contact, authentication can be accomplished by symmetric key cryptography. Sender and receiver can process the verification code of the considerable number of messages sent by a typical hidden key [6].

D. Data Availability
Data availability is the significant factor for keeping active an operational network. It is the capability of a node to use the resources and the system is accessible for the message to move onward [5].

E. Data Freshness
Though the confidentiality and the integrity of the data are guaranteed, message refreshment is also required because it guarantees that information contents are update and there is no replay of any old content. This option is particularly necessary when there are shared-key strategies utilized in the design and should be changed after some time [5].

F. Self-Organization
WSN is usually an ad-hoc network, which needs that each sensor node should be autonomous and sufficiently adaptable to be self-organizing and self-healing in any satiations. There is no fixed framework available for the network administration, so nodes should adjust themselves for the organization strategy [5].

Types of Security Attacks in WSNs:
Attacks in WSNs can be divided based on the following properties: goals, performance, and layer wise and are showed in figures 1.1, 1.2 and 1.3.

A. Attacks Based on Goal of Attackers
This kind of attack is divided into active and passive attacks.

- **Active Attacks:**

The attacker won't be passive in active attacks; however he will take active operations to gain access over the network. Some of the active attacks are DoS, Hello flood, black hole, replay, sinkhole, jamming, node subversion, man-in-middle attack, selective forwarding and false node [7].

- **Passive Attacks:**

Passive attacks are basically against data privacy. An attacker will monitor the decoded traffic and searches for sensitive data that can be utilized as a part of different kind of attacks. Within the passive attacks attacker will monitor communications, analyze of traffic, decoding of weakly encoded traffic and catching authentication data.

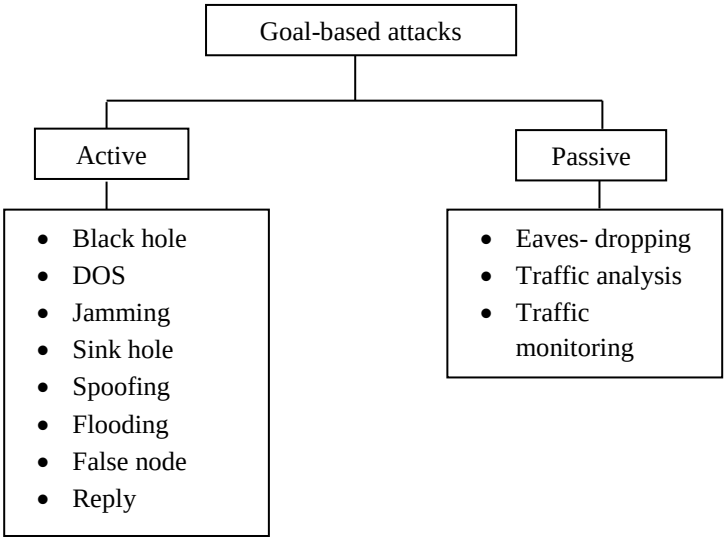

Figure1. Goal-based attacks

B. Attacks Based on Attacker's Location

Here WSNs attacks which can be either external or internal attacks would be discussed.

- **External Attacks**

External attacks can cause passive eavesdropping on transmission of information, and additionally can extend insertion of fake information into the network to make busy network resources and raise Denial of Service attacks. Sensors could be protected from external attacker by using cryptographic schemas, like encryption and digital signature [5].

- **Internal Attacks**

Internal attackers can harm the network quietly also they can get off the authentication and permissions since they are legal nodes of the local network and have full access to network data, and it is difficult to understand their attack designs. Internal attackers can take off different types of attacks, for example, misrouting, modification, eavesdropping or packet drop. The last one is trickery to counter, because when a specific packet drops, system can't differentiate whether it is a result of collision or is fall down by an attacker. There are a few kinds of packet drop attacks, for example, gray hole, black hole and on-off attacks [5]. This could be a big risk for some applications, for example, military surveillance system which monitors the battlefield zone and other basic areas.

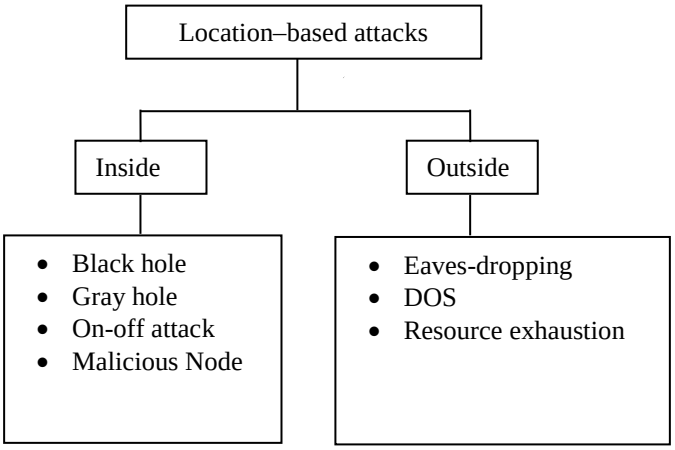

Figure2. Location—based attacks

C. Attacks Based on Layers of Network

Wireless sensor networks are designed in layered form. The layered design makes these networks risky against different types of attacks.

- **Application Layer Attacks**

This layer may contain different types of attacks, for example, data corruption, and malicious code and overwhelm. In overwhelm attack; the attacker may overwhelm network nodes, making network sending huge volumes of data to a base station. Overwhelm attack wastes network bandwidth and consumes nodes energy [5].

- **Transport Layer Attacks**

In this layer attacks an attacker would request for a new connection till the resources required by every link are getting exhausted, or reach the highest limit. Session hijacking, desynchronization and flooding are some of the attacks in this layer.

- **Network Layer Attacks**

The network layer of wireless sensor networks is defenseless against the various kinds of attacks, and their aim is to disrupt the path from sensors to the sink nodes, they use the routing protocol used by the network to lure traffic to the malicious node or drop packets. For example a sinkhole attack tries to lure all the activity toward the malicious node. Additionally if an attacker catches a single node, he would be able to gain access to the whole network. Malicious nodes can reject to route certain messages and drop them. Some of the attacks which are using network layer are as follows, wormhole, sink hole, black hole, node capture and flooding.

- **Data Link Layer Attacks**

Link layer protocol is used to arrange neighboring nodes to access shared wireless channels. WSNs are vulnerable against data link layer attacks. So we should use some methods to keep safe data accuracy. Attackers can interrupt WSNs activity by interfering with link layer services like modifying MAC protocol, tampering in communication channels and duplicating/replacing data frames. Collision, exhaustion, unfairness are some common types of link layer attacks.

- **Physical Layer Attacks**

In WSNs physical attacks could be ranged from capturing of nodes up to the jamming of the radio channel. On wireless sensor networks availability physical attacks could be very hard to prevent than software attacks, due to absence of physical control on every single node. At physical layer jamming is one of the dangerous attacks, aims to interfere with simple operations. The attacker will transfer radio signals continually on a wireless channel to disrupt communications by decreasing the signal to noise ratio. This can prompt Denial-of-Service attacks at this layer [6].

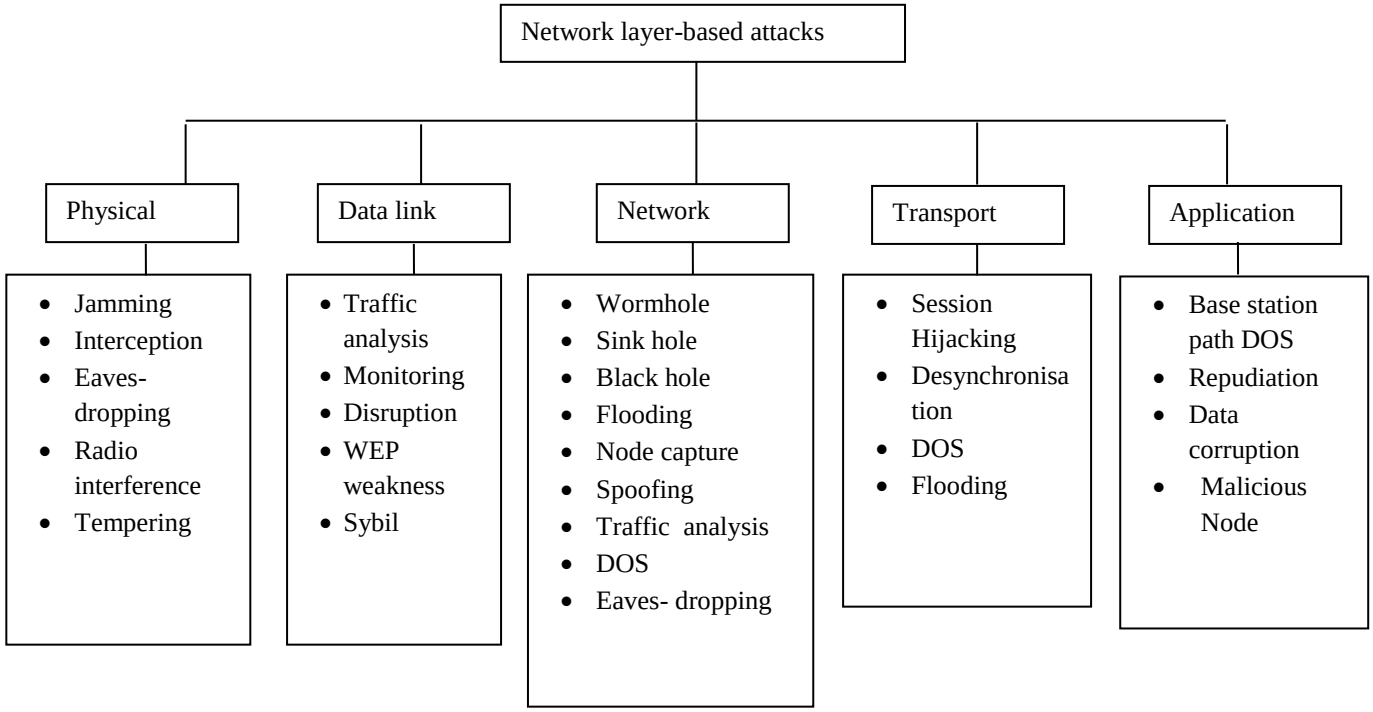

Figure3. Network layer-based attacks

II. RELATED WORK

The earlier works in security issues and comparison of security protocols in wireless sensor networks done by researchers has been summarized and presented.

C. Dhivya Devi and B. Santhi [8] had a discussion on security of WSN and various attacks in it and mostly focuses around the impact of Denial of Service (DoS) attacks, which is caused by a flood attack where there could be a combination of numerous illegal nodes, sits inside the network and can produce traffic and puts at risk the security of WSN. The paper has focused on the Hello flood attack which hangs on the network layer. The paper expressed that the future depends on the mobility of the nodes alongside the time measure to avoid the enemy from the network through the identification of the harmful nodes by signal strength comparison. The client puzzle strategy is used for every node, based on the quantity of hello messages sent and the difficulty of puzzle can be configured by applying the Dynamic approach procedure which increases the throughput of the network by considering different routing protocol at various perspectives to accomplish the proposed result from the performance of the network.

M. Revathi and Dr. B. Amutha [9] analyzed and provided comparison about the well-known WSN protocols: TinySec, LLSP, SPINS, MiniSec, μTELSA, LiSP, LEAP, SNEP, AMNI'09, and LEDS with respect to security requirements, security objectives, typical attack scenarios, and performance. Each protocol donates strong passion of security. LiSP and SPINS have helped on symmetric key shipping a protocol which confirms to sensible security. LEDS is end-to-end security protocol which bargains an outstanding degree of security in expense of computational and communication cost. LEDS is capable in end-to-end data confidentiality, encryption, and practical level of node capture attacks. The article gives a complete evaluation of these security protocols for building up a better application record. The record will be used to select security protocols.
Ritu Sharma [10] discussed main limitations, security objectives, risk models and typical attacks on sensor networks and their defense strategies or counter measures related to the sensor networks including security techniques. The most basic region vulnerable to attack is close-by the base station as the information is more aggregated, that must be kept secure using various protective methods as expressed. This is to additionally measure the capability of these protocols and characterize their more attractive features. Currently there is no solution that can be connected to an application to give the entire requirements. The future objective of this research is to build up a new authentication protocol, by adding the most attractive characteristics of what right now exists and representing some new ideas, which is ideal for usage in wireless sensor network application security.

Yones Bazband and Kamran, fahimi [11] reviewed and compared about the Delivery duration and power consumption for two protocols LLSP and TinySec in wireless sensor network to figure out which protocol is required for each network and application type. After comparing these two protocols in NS-2 simulator; the outcomes indicated that LLSP protocol would be better than TinySec protocol in network processing applications, Resource limitations situation and small sized network.

Abu Shohel Ahmed [12] compared and analyzed five main WSN protocols: TinySec, LLSP, SPINS, LiSP, and LEDS as for security requirements, attack situations, and execution. The paper introduced application frameworks for general knowledge. Every protocol gives certain levels of security. TinySec and LLSP supply link layer security with low execution overhead. LiSP and SPINS based on symmetric key distribution protocols which guarantee low overhead and sensible security. LEDS is used for location awareness end-to-end security protocol which gives high level of security in the cost of computational and communication cost. The paper gives a complete analysis of these security protocols.

III. PERFORMANCE ANALYSIS OF SECURITY PROTOCOLS IN WSN

Comparison of security protocols based on the different attributes (Confidentiality, Availability, Fresh-ness, MAC authentication, Encryption, Key management, Attacks protected and Scalability) are tabulated in table 1.

Table 1. Attributes based security protocols comparison.

S.No	Protocol	Confidentiality	Availability	Fresh-ness	MAC authentication	Encryption	Key mgmt.	Attacks protected	Scalable
1	SPINs	Yes	No	Yes	Yes	CTR-RC5	Yes	Replay, Eavesdropping	Low
2	TinySec	Yes	No	No	Yes	Skip-jack CBC-RC5	No	Replay	Partial
3	LLSP	Yes	No	Yes	Yes	AES-CBC	No	Sinkhole, directed diffusion	Low
4	LEAP	Yes	No	No	Yes	RC5	Yes	Intrusions, node capture	Low
5	LEDS	Yes	Partial	-	Yes	End-to-end, MAC	Yes	Replay	Partial
6	LiSP	Yes	Partial	No	Yes	Stream cipher	Yes	Replay	Partial
7	MiniSec	Yes	No	Yes	Yes	OCB	No	Replay	-

Performance analysis of security protocols are evaluated from table 1 is based on the attributes. It has been analyzed that all protocols have a good security principles such as confidentiality, MAC authentication and encryptions. The availability is very low in these protocols which could be the softness of these protocols. Freshness and scalability attributes are supported by some of these protocols for larger networks and regular updated data. Wireless sensor networks are almost protected from replay attacks. All the seven protocols which are shown in the table having the capability of protection from replay attacks.

In table 2 authors, protocols, advantages, disadvantages and applications of the WSNs security protocols are tabulated based on researches done by the researchers.

Table2. Tabulated description of Security protocols

S.No	Authors	Protocol	Advantages	Disadvantages	Applications
1	Leonard E. Lighfoot et al [13].	LLSP	• Less energy consumption • Protected from replay attacks	• Low scalability • Cannot guarantee data availability	• Used in in-network processing applications • Used in small size networks
2	Jain Ren et al [14].	LLSP	• Easy to deploy • Supports local broadcast and passive participation	• Not able to compromise nodes	• _
3	Chris Karlof et al [15].	TinySec	• Guarantee message authentication, confidentiality and integrity • Energy efficient than SPINS • Less memory usage	• Vulnerable against node capture attacks and replay attacks	• Used in in-network processing and local broadcast
4	Llanos Tobarra et al [16].	TinySec	• It has a light weight design • Low power consumption	• TinySec- Auth doesn't provide any confidentiality mechanisms	• TinySec is part of the official Tiny OS
5	Ioannis Krontiris et al [17].	TinySec	• It provides two modes of operations for communications	• It relies on a single key manually programmed into the sensor nodes before deployment • It can't address messages less than 8 bytes efficiently	• _
6	Adrian Perrig et al [18].	SPINS	• Has two secure building blocks SNEP and µTesla • Low communication expense • Robust against eavesdropping and replay attacks	• Vulnerable against DoS attacks • Not suitable for environmental monitoring application	• Used in small sized networks • Communication pattern is node-to-base or vice versa

S.No	Authors	Protocol	Advantages	Disadvantages	Applications
7	Kunal M Pattani and Palak J Chauhan [19].	SPINS	• Uses metadata to avoid consuming more energy • Has the ability of data freshness and confidentiality • Avoids duplicate messages in the network	• _	• _
8	Sencun Zhu et al [20].	LEAP	• It a powerful keying mechanism which provides four types of key for every sensor node • Supports different communication pattern • Less energy consumption	• More storage space is require to store four different keys for every node • It believes that base station is never compromised	• Used in in-network processing
9	Delan Alsoufi et al [21].	LEAP	• It reduces the participation of a base station which is efficient in terms of communication and energy • It has scalability and cluster communication abilities	• Security weakness during the process of key establishment • High cost of capacity needed for storing the four different keys for each node	• _
10	Aarti Arjun Andhale and Prof. B.N. Jagdale [22].	LEAP	• It is designed as a key management protocol to provide secure communications in WSN	• _	• It is efficient for large scale sensor networks with energy efficiency capability
11	Kui Ren [23].	LEDS	• Robust against DoS attacks • Used in small and large networks • Less energy consumption	• Requires maintenance of dynamic routing and network topology, it is not applicable for battlefield applications	• It can be used in both small and large networks
12	John Gichuki Ndia [24].	LEDS	• It ensures a high level of security • It provides data confidentiality and avoids node capture attacks	• Doesn't support dynamic topology	• provides end-to-end secure authentication
13	Taejoon Park et al [25].	LiSP	• Can be used in large scale WSNs • Has the ability to sense and recover the lost keys • Robust against DoS attacks • Less energy consumption	• It is also not applicable in battlefield application • It requires IDS application to have a better security	• Used for key management of large scale and small networks

S.No	Authors	Protocol	Advantages	Disadvantages	Applications
14	Aditya Sharma et al [26].	LiSP	• Efficient key broadcast without retransmission/acknowledgement • Key refreshment without disrupting ongoing data • encryption/decryption • It has a light weight protection mechanism	• _	• Used in large as well as small networks
15	Mark Luk et al [27].	MiniSec	• Less energy consumption • It has a high security using offset codebook OCB • Its source code is distributed freely under an open source license	• Vulnerable against DoS attacks • Doesn't provide data integrity and availability	• Used in both small and large scale networks
16	Ehsan Sharifi et al [28].	MiniSec	• Protects network against replay and spoofing attacks • It is designed to protect the WSNs against Power Exhausting attack • This protocol reduces the authentication time	• It uses shared public key for all the sensors and for this reason inherits weaknesses of Tinysec	• _

For security requirements, attacks and execution, every protocol gives certain levels of security. TinySec and LLSP protocols support link layer security with low execution overhead. LiSP and SPINS security protocols are based on symmetric key distributions, which guarantee low overhead and serviceable security. LEDS protocol is used for location awareness and end-to-end authentications, which gives high level of security in the cost of computational and communication cost. MiniSec Protocol provides semantic security; also it has lower energy consumption compared to TinySec. LEAP is an energy efficient communication protocol. Leap protocol provides security by multiple keys and protect WSN against intrusions and irregularities.
The decision of selecting the favorite and reliable security protocols could be done through the security attributes for the wireless sensor network. Each security protocol has its own properties with some advantages and disadvantages. So the attributes which are mentioned in the table plays an important role in selecting a right protocol for WSN.

IV. CONCLUSION AND FUTURE SCOPE

It has been observed and discussed that wireless sensor network is an important topic in recent years which is being used by many researchers and its users around the world. The main goal of this review paper is to be familiar with different security issues and challenges available in wireless sensor networks, methods and protocols used for avoidance of these issues and challenges have been studied, discussed and reviewed, It has also compared security protocols of wireless sensor networks with their confidentiality, availability, freshness, MAC authentication, encryptions and some other attributes and descriptions in table forms. In the future the comparison of some specific security protocols would be done with some simulation tools to achieve the objectives.

REFERENCES

[1] S. Misra, I. Woungang and S. C. Misra, "Guide toWireless Sensor Networks", c Springer-Verlag London Limited, pp. 1, 2009
[2] J. Zheng and A. Jamalipour, "Wireless Sensor Networks A Networking Perspective", A John Wiley & Sons, Inc., Publication, pp. xxiii-2, 2009
[3] C. S. Raghavendra, K. M. Sivalingam and T. Znati, "wireless sensor networks", Kluwer academic publishers New York, Boston, Dordrecht, London, Moscow, pp. xiv, 2004
[4] M. U. Aftab, O. Ashraf, M. Irfan, M. Majid, A. Nisar and M. A. Habib, "A Review Study of Wireless Sensor Networks and Its

Security", Communications and Network, Vol. 7, No.4, pp.172-179, 2015
[5] Kahina Chelli, "Security Issues in Wireless Sensor Networks: Attacks and Countermeasures", Proceedings of the World Congress on Engineering, London, U.K. (Vol. 1, pp. 1-3, 2015
[6] Murat Dener, "Security Analysis in Wireless Sensor Networks", Hindawi Publishing Corporation, International Journal of Distributed Sensor Networks, Vol.10, No.10, pp.303501, 2014
[7] David Martins and Herve Guyennet, "Wireless Sensor Network Attacks and Security Mechanisms: A Short Survey", pp. 313-320, 2010
[8] C. Dhivya Devi and B.Santhi, "Study on Security Protocols in Wireless Sensor Networks", International Journal of Engineering and Technology, Vol.5, No.5, pp.200-207, 2013
[9] M. Revathi and Dr. B. Amutha, "A Survey on Security Protocols in Wireless Sensor Network", International Journal of Pure and Applied Mathematics, 2017
[10] R. Sharma, Y. Chaba and Y. Singh, "Analysis of Security Protocols in Wireless Sensor Network", IJANA 2010
[11] Y. Bazband and K. Fahimi, "Performance Comparison Wireless Sensor Network Security Protocols: LLSP and TinySEC", International Journal of Engineering Sciences and Research Technology, 2014
[12] A. S. Ahmed, "An Evaluation of Security Protocols on Wireless Sensor Network", TKK –T Seminar of Internetworking, 2009
[13] L. E. Lighfoot, J. Ren and T. Li, "An Energy Efficient Link-Layer Security Protocol for Wireless Sensor Networks", IEEE EIT 2007 proceedings, pp. 233-238, 2007
[14] J. Ren, T. Li and D. Aslam, "A Power Efficient Link-Layer Security Protocol LLSP for Wireless Sensor Networks", Military Communications Conference, pp. 1002-1007, 2005
[15] C. Karlof, N. Sastry and D. Wagner, "TinySec: A Link Layer Security Architecture for Wireless Sensor Networks", Baltimore, Maryland, USA, pp. 162-175, 2004
[16] L. Tobarra, D. Cazorla, F. Cuartero, G. Diaz and E. Cambronero, "Model Checking Wireless Sensor Network Security Protocols: TinySec + LEAP", in wireless sensor and actor networks, Springer, Boston, MA, pp.95-106, 2007
[17] L. Krontiris, T. Dimitriou, H. Soroush and M. Salajegheh, "WSN Link-Layer Security Frameworks", wireless sensor network security, Athens Information Technology, Greece, pp. 142, 2008
[18] A. Perrig, R. Szewczyk, J. D. Tygar, V.Wen and D. E. Culler, "SPINS: Security Protocols for Sensor Networks", Kluwer Academic Publishers. Manufactured in Netherlands, Vol.8 No.5 pp.521-534, 2002
[19] K. M Pattani and P. J Chauhan, "SPIN Protocol for Wireless Sensor Network", International Journal of Advance Research in Engineering, Science and Technology, 2015
[20] S. Zhu, S. Setia and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks", Proceedings of the 10th ACM conference on Computer and communications security, Washington D.C., USA, Vol. 2, No.4, pp.500-528, 2003
[21] D. Alsoufi, K. Elleithy, T. Abuzaghleh and A. Nassar, "Security in Wireless Sensor Networks-Improving the LEAP Protocol", International Journal of Computer Science and Engineering Survey, 2012
[22] A. A. Andhale and Prof. B. N. Jagdale, "Light Weight Security Protocol for Wireless Sensor Networks (WSN)", International Journal of Engineering Research and Technology, 2014
[23] K. Ren, W. Lou and Y. Zhang, "LEDS: Providing Location-Aware End-to-End Data Security in Wireless Sensor Networks", IEEE Transactions on Mobile Computing, Vol. 7, No.5, pp.585-598. 2008
[24] J. G. Ndia, "A Survey of Security Protocols for Wireless Sensor Networks", International Journal of Applied Computer Science, 2017
[25] T. Park and K. G. Shin, "LiSP: A Lightweight Security Protocol for Wireless Sensor Networks", ACM Transactions on Embedded Computing Systems, Vol. 3, No.3, pp.634-660, 2004
[26] A. Sharma, G. Tripathi, M. S. Khan and K. A. Kumar, "A Survey Paper on Security Protocols of Wireless Sensor Networks", International Research Journal of Engineering and Technology, 2015
[27] M. Luk, G. Mezzour and A. Perrig, "MiniSec: A Secure Sensor Network Communication Architecture", IPSN Cambridge, Massachusetts, IEEE USA, pp. 479-488). 2007
[28] E. Sharifi, M. Khandan and M. Shamsi, "MAC Protocols Security in Wireless Sensor Networks: A Survey", International Journal of Computer and Information Technology, A survey 1, 2014

Authors Profile

Mr. A. K. Nuristani pursued Bachelor of Computer Science from Kabul Education University, Afghanistan in 2010. He worked as a Network manager in IT department of Ministry of Religious Affairs and Hajj of Government of the Islamic Republic of Afghanistan till 2016. Currently he is doing Master of Technology in Computer Science form Himachal Pradesh University of Shimla, India. His research work mainly focuses on WSN security issues.

Mr. Jawahar Thakur is a doctorate in computer science form Himachal Pradesh University of Shimla, India with specialization in Networking, Big data, Software Engineering and Data Analysis. He is currently working as Professor in Department of Computer Science Himachal Pradesh University of Shimla, India. He is a lifetime member of CSI, Indian Science Congress IEEE. He has published more than 60 research paper and articles in International/National journals and conferences.

