ISSN No. 0976-5697

Volume 8, No. 5, May – June 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A Survey on Lightweight Block Ciphers for Wireless Sensor Network

Jasvir Kaur
M.Tech Scholar
University College of Engineering
Punjabi University, Patiala, Punjab, India

Brahmaleen Kaur Sidhu
Assistant Professor
University College of Engineering
Punjabi University, Patiala, Punjab, India

***Abstract*:** With an advancement of wireless communication technology, wireless sensor network (WSN) has emerged as one of the most powerful technologies which can be used in various applications, such as military surveillance, environment monitoring, industrial control, and medical monitoring. Wireless Sensor Network includes many devices such as smart grids, mobile phones, RFID tags, smart cards and micro-chips etc which need limited resources.. In this paper, the summary of Wireless Sensor Network has been given. After that the requirement for the WSN security and various attacks on the WSN are briefly discussed. This paper depicts the various block ciphers which helps to resolve the attacks of Wireless Sensor Network and comparison of various block ciphers had also been done.

***Keywords*:**Wireless Sensor Network, Security, Cryptography, plaintext, cipher text.

I. INTRODUCTION

A wireless sensor network (**WSN**) is a wireless organize comprising of incompletely dispensed self-deciding gadgets utilizing sensors to screen physical or environment conditions. A WSN framework joins an entryway that gives remote availability back to the wired world and dispersed hubs. Engineers have made WSN applications for regions including medicinal services, utilities, and remote checking. In social insurance, remote gadgets make less intrusive patient checking and human services conceivable. For utilities, for example, the power network, streetlights, and water municipals, remote sensors offer a lower-cost technique for gathering framework well being information to decrease vitality utilization and better oversee assets. Remote checking covers an extensive variety of uses where remote frameworks can supplement wired frameworks by lessening wiring costs and permitting new sorts of estimation Wireless Sensor Networks impart by sending and accepting parcels among each other. The WSN is confronting a wide assortment of security condition, constant preparing needs, heterogenic structure, vast number of hubs, requirement for quantifiability, portability, the heaviness of the application
ecological conditions, and cost Privacy which is the essential objective of security gives a standout among the most vital impediments to overcome so as to guarantee the uprightness and accessibility and the accomplishment of time-basic and fundamental objective. Amid touchy WSN applications, for example, the reconnaissance of adversary or outskirts, the security conventions which empower the sensors to exchange mystery information to the base station must be utilized. In any case, the low processor and radio limits of the sensors keep customary security conventions from being utilized as a part of WSN applications .Nowadays, different security conventions that consider these parts of WSNs and their hubs are being produced. The security conventions to be created ought to execute all the security issues (information privacy, information respectability, information freshness, information validation, and accessibility) additionally furnish high security with low vitality utilization. It is essential to give security in remote sensor organizes so that lone the right client gets the message. Cryptography is a vital idea which gives security in Wireless Sensor Networks.

II. REQUIREMENTS OF WSN SECURITY

As indicated by their own qualities, the remote sensor systems vary from the customary remote systems, confronting more requests particularly regarding security. Keeping in mind the end goal to oppose various types of security assaults and dangers and to guarantee the secrecy of the assignments played out, the unwavering quality of information created, the accuracy of information combination, and the security of information transmission, the security requirements are mainly in the following areas.

- Data Confidentiality
- Data Integrity
- Data Freshness.
- Availability
- Robustness
- Access Control

III. ATTACKS IN WSNS:

A distribution of the attacks consists in different the passive attacks from the active attacks. The passive attack is fixed to listening and analyzes exchanged traffic. This type of attacks is easier to realize and it is difficult to remove. In the active attack, an attacker attempt to evacuate or, then again adjust the messages transmitted on the system. He can also infuse his claim movement or replay of old messages to bother the operation of the system or to cause a DOS.

A. *Tampering:* it is the eventual outcome of physical access to the center by an assailant; the reason will be to recover cryptographic material like the keys used for ciphering [1]

B. *Black hole:* a hub misrepresents steering data to compel the passage of the information independent

from anyone else, later on; its exclusive mission is at that point, nothing to exchange, making a sink or dark opening in the system.

C. *Blackmail attack*: a malicious hub makes report that another true blue hub is noxious to dispense with this last from the system. In the event that the malignant hub figures out how to tackle a noteworthy number of hubs, it will have the capacity to disturb the operation of the system.
D. *Wormhole attack*: Attackers here are deliberately put at diverse finishes of a system. They can get messages and replays them in various parts by methods for a tunnel.

IV. LETRATURE SURVEY

[2] In this paper **Patil, S., P, V** discussed wireless sensor networks have attracted many researchers due to their capability to connect to the real world. The network finds application from military to medicine and is customized according to the task to be performed in the applications. The significant tasks performed by the network includes sensing, monitoring, target tracking and event sensing. Being one of the prominent futuristic technology, wireless sensor network needs to be addressed from different perspectives from design to development to application. With a need to unleash the unlimited potential of Wireless sensor networks along with addressing the challenges posed. In this paper they resent a comprehensive review of work published in wireless sensor networks recently. Hence making our survey unique providing a direction to the future research work in wireless sensor network domain.

[3] In this paper **P Kovendan, A., Sridharan, D.** discussed the rapid increase in the demand for electricity necessitates the power quality improvement for achieving better reliability in smart grids. Wireless Sensor Networks (WSN) is the proven technology for reliable monitoring. This paper proposes a system model for the development and implementation of WSN based communication system for the monitoring of distributed generation, loads and transmission lines in the electrical grid and a controller system for automated control on the electrical grid. This work also aims to reduce the carbon footprints by reducing the dependency of electrical grid through the enhancement of distributed generation and grid sharing for avoiding voltage rise problem. To achieve this, a smarter electrical grid has been developed for the validation of smart grid considering a generation substation, a transmission substation and a distributed generation with loads. The occurrence of power quality issue and voltage rise has been controlled by active power control strategy. The communication network and controller has been modeled and tested for the performance of monitoring system and data communication capability on smart grid.

[4] In This paper, **Bogdanov, A., Knudsen** illustrates the need of new ultra-lightweight block cipher algorithm for the devices which have limited resources such as low power, low gate count, low memory etc. The new block cipher named as PRESENT has 31 rounds with block size 64-bit and two keys with size 80-bit and 128-bit respectively. PRESENT block cipher has the aim of software and hardware efficiency as comparison with today's leading stream ciphers.

[5] In this paper, **Gong, Z., Nikova, S., Law, Y.-W.** describe the portray another group of lightweight square cipher named KLEIN, which is intended for asset compelled gadgets, for example, remote sensors and RFID labels. Contrasted with the related recommendations, KLEIN has advantage in the product execution on inheritance sensor stages, while in a similar time its equipment usage can likewise be conservative. The different key lengths of KLEIN offer an adaptability furthermore, a direct security level for pervasive applications. Along these lines, our plan expands the accessible alternatives of lightweight block cipher for low-asset applications.

[6] In this paper, **Suzaki, T., Minematsu** discussed TWINE another lightweight 64-bit square figure. Our essential objective is to accomplish equipment proficiency proportional to past recommendations, and in the meantime great programming execution on different CPUs, from low-end miniaturized scale controllers to top of the line ones (such as Intel Core arrangement). For this reason, we maintain a strategic distance from equipment situated plan choices, generally quite bit stage, and fabricate a piece block cipher utilizing.

[7]In this paper, **Wu, W., Zhang** describes another lightweight block cipher called LBlock. Like numerous other lightweight square figures, the piece size of LBlock is 64-bit and the key size is 80-bit. Our security assessment demonstrates that LBlock can accomplish enough security edge against known assaults, for example, differential cryptanalysis, direct cryptanalysis, impossible differential cryptanalysis and related-key assaults and so forth. Besides, LBlock can be executed productively not just in equipment environments additionally in programming stages, for example, 8-bit microcontroller.

[8] In this paper, **Kushwaha, P., Singh, M., Kumar** proposed another lightweight piece block cipher named RECTANGLE. The fundamental thought of the outline of RECTANGLE is to permit lightweight and quick executions utilizing bit-cut procedures. RECTAN-GLE utilizes a SP-arrange. The substitution layer comprises of 16 4 × 4 S-confines parallel. The stage layer is made out of 3 revolutions. As appeared in this paper, RECTANGLE offers extraordinary execution in both equipment furthermore, programming condition, which gives enough adaptability to various application situation. RECTANGLE is extremely hardware-friendly block cipher.

V. LIGHTWEIGHT BLOCK CIPHERS

A. PRINT: PRINT [9] is a lightweight block cipher designed to integrated circuit printing. PRINT lightweight cipher algorithm contains SPM structure. Block size is 48 or 96 bits, key size 80 or 160 bits with 48 or 96 rounds. key size always fixed no need to update key. each round contain 5 steps:

- Key XORed with cipher text
- Cipher drag using linear diffusion
- Cipher text XORed with round constant
- Bits permutation
- Cipher is compound using S-box

B. DES, DESL, DESX and DESXL [10]:- DES is a data encryption standard which has 64 bit plaintext,56 bit key size and 16 rounds. DESL is lightweight block cipher of DES algorithm.DESX block cipher provide higher security then DES and DESL.DESX has key size 184 bits.DESXL is the lightweight block cipher algorithm of DESX algorithm which has plaintext 64 bit,key size 184 bit and 16 rounds.

C. TWINE:TWINE [8] lightweight block cipher has two types, TWINE-80 and TWINE-128.block size is 64 bits and 36 rounds for both algorithms but key size is different for each block cipher.TWINE-80 contain 80 bits key size and TWINE-128 contain 128 bits key size.

D. LBlock: [8] It is a lightweight block cipher algorithm. Block length is 64 bit and key size is 80 bit.Lblock use the Feistel structure and consists of 32 rounds. LBlock algorithm divided into three parts:
- Encryption algorithm,
- Decryption algorithm
- Key scheduling.

E. KATAN and KTANTAN:KATAN [8] is hardware dependent block cipher which has block size 32,48,64 and key size 80 bits.KATAN block cipher divided into two parts:first part containKATAN,KATAN-32,KATAN-48 and KATAN-64.second part contain KTANTAN,KTANTAN-32, KTANTAN-48 and KTANTAN-64.KTANTAN only suitable for fixed key size devices.

F. Rectangle: [8]Rectangle is an rapeated block cipher. The block length is 64 bits and the key length is 64 bits or 128 bits. It consists following steps:
- The cipher state and sub key state
- The Round Transformation
- Shift row
- Key schedule

G. PRESENT: PRESENT [4]is an ultra lightweight algorithm. PRESENT lightweight block cipher is an example of SP network .It contains 31 round and block length is 64 bits. Two keys used to encrypted the plaintext (key length 80 and 128 bits).It contain following steps:
- Add Round Key
- Substitutions
- Permutations
- Key schedule

H. KLEIN: KLEIN [8] has block size 64 bits and 64 or 80 or 96 bits key size with 12 or 16 or 20 rounds. Key (n=16/20/24) plaintext (n = 16) and cipher text (n = 16) pictured as n * nibbles (4 bits).Each round consists of the following 4 steps:
- Add round key
- Sub Nibbles
- Rotate Nibbles
- Mix Nibbles

I. LED: [8] light encryption device block cipher which has 64 bit plaintext with four key sizes 64 bits,80 bits,96 bits and 128 bits. It contain 8 round for 64 bits key size and 12 round for other key sizes.It contain four steps:
- Add constants
- Sub cells
- Sift row
- Mix columns serial

VI. COMPARISONS

Distinctive lightweight block cipher algorithm shows in table as indicated by their key size, block size, structure, cycle per block two types of structures, serialized and round-based. Serialized structure is utilized for low area in this information way of calculation is equivalent to 4 bits and round-based models are utilized for high throughput in this information way of calculation is equivalent to block size. Three sorts of structure, SPN (Substitution Permutation Network), Feistel Network and LFSR.SPN utilize substitution by S-box and change by P-layer. Feistel organize utilizes twofold XOR and moving of left-right bit of figure. LFSR utilizes move enlist whose info bit is a component of past state.

Table 1: [8]Comparison of lightweight block ciphers

Block ciphers	Architecture	Structure	Key size	Block size	Rounds	Cycles/block
PRINT-48*	Serialized	SPN	80	48	48	768
PRINT-48*	Round-based	SPN	80	48	48	48
PRINT-96*	Serialized	SPN	160	96	96	3072
PRINT-96*	Round-based	SPN	160	96	96	96
LED-64*	Serialized	SPN	64	62	32	1248
LED-80*	Serialized	SPN	80	64	48	1872
LED-96*	Serialized	SPN	96	64	48	1872
LED-128*	Serialized	SPN	128	64	48	1872
KTANTAN-32*	Serialized	LFSR	80	32	254	255
KTANTAN-48*	Serialized	LFSR	80	48	254	255
KTANTAN-64*	Serialized	LFSR	80	64	254	255
PRESENT-80	Serialized	SPN	80	64	32	516

PRESENT-80	Round-based	SPN	80	64	32	32
PRESENT-128	Serialized	SPN	128	64	32	528
PRESENT-128	Round-based	SPN	128	64	32	32
DES	Serialized	Feistel	56	64	16	144
DESL	Serialized	Feistel	56	64	16	144
DESX	Serialized	Feistel	184	64	16	144
DESXL	Serialized	Feistel	184	64	16	144
TWINE-80	Round-based	Feistel	80	64	36	36
TWINE-80	Serialized	Feistel	80	64	36	540
TWINE-80	Round-based	Feistel	80	64	36	36
TWINE-128	Round-based	Feistel	128	64	36	36
TWINE-128	Round-based	Feistel	128	64	36	36
KLEIN-64	Round-based	SPN	64	64	12	13
KLEIN-80	Round-based	SPN	80	64	16	17
KLEIN-96	Round-based	SPN	96	64	20	21
KLEIN-64	Serialized	SPN	64	64	12	207
KLEIN-80	Serialized	SPN	80	64	16	271
KLEIN-96	Serialized	SPN	96	64	20	335
KATAN-32	Serialized	LFSR	80	32	254	255
KATAN-48	Serialized	LFSR	80	48	254	255
KATAN-64	Serialized	LFSR	80	64	254	255
LED-64	Serialized	SPN	64	64	32	1248
LED-80	Serialized	SPN	80	64	48	1872
LED-96	Serialized	SPN	96	64	48	1872
LED-128	Serialized	SPN	128	64	48	1872
LBLOCK	Round-based	Feistel	80	64	32	32
LBLOCK	Serialized	Feistel	80	64	32	576
RECTANGLE-80	Round-based	SPN	80	64	25	26
RECTANGLE-128	Round-based	SPN	128	64	25	26
RECTANGLE-80	Serialized	SPN	80	64	25	461

VII. CONCLUSIONS

Wireless communication plays a vital role in today's modern world. Wireless Sensor Network attracts more and more attention due to their promising application such as monitoring, tracking etc. Wireless Sensor network has become the essential part of our daily lives. This paper illustrated the need of wireless sensor network and number of attacks on the sensor network. Block ciphers are the ciphers which permutes N-bit blocks of plaintext with the secret key and output the N-bit block of ciphertext. This paper has depicted about the various ultra-lightweight block cipher whose goal is to be software and hardware efficient. Comparison of various block cipher has been done on the basis of some parameters such as key size, block size, rounds and cycles. According to the comparison between various block ciphers, they need to have high throughput and low complexity.

REFERENCES

1. Boyle, D., Newe, T.: Securing Wireless Sensor Networks: Security Architectures. journal of networks 3 (2008)
2. Patil, S., P, V.: Overview of Issues and Challenges in Wireless Sensor Networks. International Journal of Application innovations in engineering and management 5 (May 2016)
3. P Kovendan, A., Sridharan, D.: Wireless Sensor Networks Based Control Strategies for the Enhancement of Reliability in Smart Grids., 2499-2506 (2016)
4. Bogdanov, A., Knudsen, L., Leander, G., Poschmann, A.: PRESENT An ultra lightweight block cipher., vol. 4727, pp.450-466 (2007)
5. Gong, Z., Nikova, S., Law, Y.-W.: KLEIN: A New Family of Lightweight Block Ciphers.
6. Suzaki, T., Minematsu, K., Morioka, S., Kobayashi, E.: TWINE: A Lightweight Block Cipher for Multiple Platforms.
7. Wu, W., Zhang, L.: LBlock: A Lightweight Block Cipher⋆.
8. Kushwaha, P., Singh, M., Kumar, P.: A Survey on Lightweight Block Ciphers. International Journal of Computer Applications 96 (june 2014)
9. Knudsen, L., Leander, G., Poschmann, A., Robshaw, M.: Printcipher: A block cipher for icprinting,In Cryptographic Hardware and Embedded System. Springer 6225, 16-32 (2010)
10. Leander, G., Paar, C., Poschmann, A., Schramm., K.: New lightweight des variants. In Fast Software Encryption. springer, 196–210. (2007)