International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-3, January 2020

A Smart Cryptographic measure for Data Survivability in Unattended Wireless Sensor Networks

Hegde Nischaykumar, Kulkarni Linganagouda

Abstract: ***An Unattended Wireless Sensor Network (UWSN) wherein a sporadically visiting sink tries to collect data absorbed by the motes. This setup is most suitable in hostile environments where the collected valuable data becomes the target for a mobile adversary. Unattended sensors cannot instantly transmit collected data to some safe external entity. Though there is an intermittent visit by the sink, a powerful mobile adversary can easily compromise the valuable data collected by sensor nodes between the intervals. Therefore, the data needs to be preserved to be handed over to the sink in its next visit. This property of unattended WSN is called as Data Survivability. We propose a symmetric key cryptosystem that tackles sensor collected data erasure, modification, or disclosure as a support for data survivability in UWSNs. The proposed model has been designed using Linear Feedback Shift Registers (LFSRs) embodied with less power dissipation mechanism that operates on mask method. This is critical to any application running in unattended environments. We have compared our design with other standard works and have substantially proved the trustworthiness. Our work has been assessed using NIST test suite and found reliable.***

Keywords: Unattended Wireless Sensor Networks (UWSNs), mobile adversary, Sink, Symmetric Key Cryptosystem, Data Survivability, Linear Feedback Shift Registers (LFSRs), NIST test suite.

I. INTRODUCTION

An emerging and challenging paradigm of WSNs is the Unattended Wireless Sensor Networks (UWSN) [1]. UWSN [2] (Figure 1) is a complex and special kind of WSN where data sensed by the sensors is not collected continuously by the sink. Sink visits the setup sporadically to collect valuable data absorbed by the participating sensors. Collected data need to be protected from mobile adversaries by implementing appropriate mechanisms. The inability of motes to communicate with sink continuously is due to their deployment in hostile places, limited transmission ranges, power constraints and or signal propagation problems [3].

Revised Manuscript Received on January 30, 2020.
***** Correspondence Author
Hegde, Nischaykumar*, Computer Science and Engineering Department, Research Scholar, Visvesvaraya Technological University, Belagavi, India. E-mail: meetnischay@gmail.com
Kulkarni, Linganagouda, Professor, Computer Science and Engineering Department, KLE Technological University, Hubballi, India E-mail: linganagouda@yahoo.co.uk

In order to secure the collected data by sensors for a longer duration, a smart mechanism is essential which must consider basically two critical factors - a) Power dissipation rate and 2) Defending against mobile adversaries.

Hence a trade-off needs to be done between the logic and power factor. In this view, we are proposing a symmetric key cryptosystem which is built using low power LFSRs [4], [5] and is a variation of A5 family- a standard stream cipher system [6].

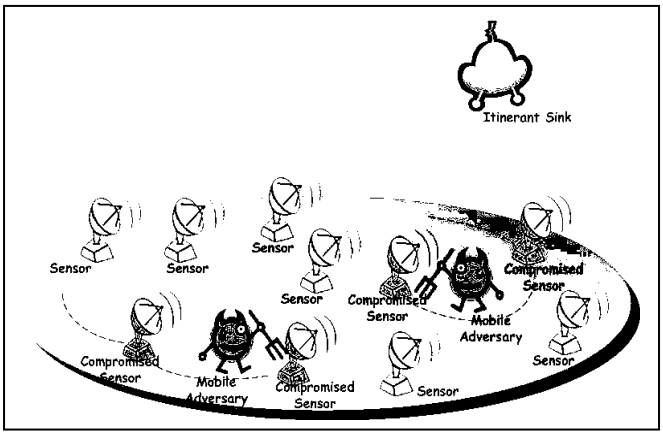

Fig. 1: Unattended Wireless Sensor Network Scenario

Our design has overcome high rate of power dissipation and has overtaken the performance of systems based on A5 family. Since systems based on A5 family has been the preferred crypto-system for GSM based communication, we have adapted its base working for our work [11]. Also the cryptosystem has produced good results compared to variants of A5 family. Fourth section of the paper describes the trustworthiness of our work.

II. RELATED WORKS

In the past recent years, ample amount of works related to our design have been proposed which includes modified A5/1 [9], enhanced A5/1 [10] and the initial work i.e., A5/1 stream cipher system itself [6]. To prove the reliability of any designed crypto system must undergo various tests prescribed by NIST test suite recommended by Govt. of India [7]. Our work has shown comparatively good results under all the tests which is shown in fourth section of this paper.

A. The Base A5/1 Stream Cipher System

The first design under A5 family comprises of three LFSRs with sizes19, 22 and 23-bits,

denoted by R1, R2, and R3, respectively. One bit emerges out of the system at evry iteration.

This is generated by performing XOR Boolean operation of the most significant bits (MSBs) of R1, R2 and R3 registers. Every register is associated with one clocking bit and few tapping bits [6]. The overall operation is carried out in terms of n iterations (n is an arbitrary value). At every iteration, the clocking bit values of - R1 (8th bit), R2 (10th bit), and R3 (10th bit) are fed as inputs to one special function termed as majority function [6] to apply clocking operations. Each LFSR is clocked if its clock bit is equal to this majority value [6]. It can be observed that at least two among R1, R2 and R3 are clocked at every iteration with a probability factor of 0.75/ Register. The architecture for this system is depicted in the below shown figure.

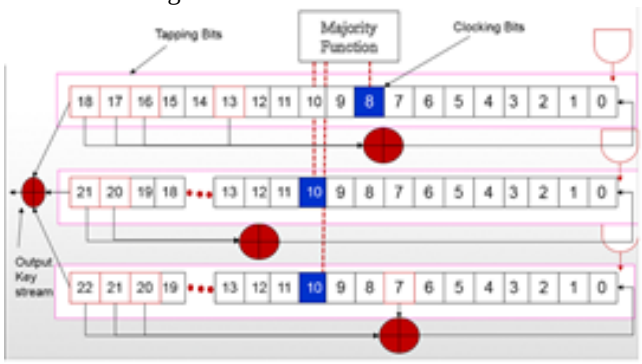

Fig. 2 The Standard A5/1 stream cipher system

B. Enhanced A5/1 Stream Cipher System

In this work, two modifications have been introduced considering the design of A5/1 scheme. First modification is in feedback tapping unit and next is in the rule associated with clocking mechanism.

Shuffling LFSRs: This is a modification given to the existing A5/1 system that is all the LFSRs are resized to 23-bits. The intention is to shuffle these LFSRs and prove randomness.

Varying Feedback polynomials: In A5/1 scheme, the participating registers (LFSRs) have fixed polynomials for tapping bits to generate feedback, but in this work, polynomials change over the period of time.

Further, a new clocking rule has been introduced named as N-rule [10].

C. Modified A5/1 Stream Cipher System

In this scheme, two variants have been experimented. First, by changing the tapping bits of original A5/1 system. Secondly, by adding two more LFSRs of size 24-bit and 25-bit. In both these variants, the majority function has been eliminated. The authors have depicted the performance analysis of the system by conducting the tests prescribed by NIST test suite which is recommended.

Security analysis of all these aforementioned systems is shown in the fifth section and also have been compared with our proposed design.

III. PROPOSED SYSTEM

Over a recent decade, many cryptographic schemes have been proposed for protecting the data collected by sensor nodes. Most of these schemes are based on asymmetric cryptography which will be based on Public Key Infrastructure (PKI) could be for securing the keys exchanged between the motes or securing the data from mobile adversaries[8]. Asymmetric key cryptographic measures are generally not preferred in wireless sensor networks because of their high usage of power [5]. Hence we have proposed a scheme that is based on symmetric key cryptography by properly handling the trade-off between power dissipation rate and underlying operations. Of course, we have chosen A5/1 as the base module for our plan but is equipped with a special register termed as Clocking Bit Nominating Register (CBNR) built using a new design of LFSR for reduced power consumption based on mask method [12]. The role of CBNR is to nominate clocking bits for R1, R2, R3, over the iterations. The special register CBNR is shown below in Fig 3. CBNR size is 12-bits. Each nibble contributes to one among R1, R2 and R3 and remains fixed throughout the operation. This CBNR register is left rotated by 1 position for every iteration which results in the change of clocking bits for the participating LFSRs. Due to this, clocking bits will change for every iteration and the output generated will not have any kind of correlation. Hence, we would claim that by changing the clocking bits the system can be made more powerful against security attacks. The Initial Vector for CBNR is depicted in the below shown figure.

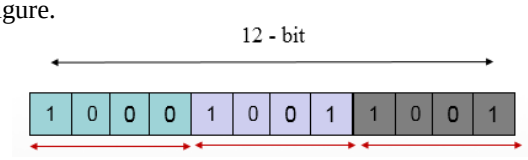

Fig. 3 Clock Bit Nominating Register (CBNR)

TABLE-I : Nibble Values of CBNR over n iterations

Iteration.	4-bit CBNR(FSR3)	4-bit CBNR(FSR2)	4-bit CBNR(FSR1)
1	8	9	9
2	1	3	3
3	2	6	6
4	4	10	10
.	.	.	.
n	6	4	9

IV. RESULTS AND DISCUSSIONS

A. Security analysis

We have conducted a series of tests prescribed by NIST test suite [7] and made a thorough inspection of performance of the proposed work against the variants of A5 family. We have designed all the tests using Python programming language. For every test, a p-value is recorded and is compared with the p-values of variants of A5 family. Each test under NIST test suite calculates a P-value to declare the status of a cipher system. If a P-value for a test is determined to be equal to 1, then the sequence appears to have perfect randomness. A P-value of zero indicates that the sequence appears to be completely non-random [7]. A cipher system is deemed to be strong only if it satisfies randomness property. Registers R1, R2 and R3 is padded up with Initial Vector (IV) based on the primitive polynomials discussed in [13]. Our system has comparatively high P-values under almost all the tests (Table 2).

Hence, the effect of varying clocking bits for participating registers has been analyzed against randomness of the proposed stream cipher.

TABLE- II: Comparison of test results with variants of A5 Family

Test No.	A5/1	Modified A5/1	Enhanced A5/1	Proposed Work
1	0.75	0.66	0.155	0.76
2	0.87	0.9	0.33	0.89
3	0.15	0.57	0.43	0.75
4	0.57	0.14	0.42	0.37
5	-1.0 (NR)	-1.0 (NR)	0.41	0.65
6	0.56	0.77	0.48	0.38
7	0.37	0.01 (NR)	0.51	0.85
8	-1.0 (NR)	-1.0 (NR)	0.43	0.57
9	-1.0 (NR)	-1.0 (NR)	0.50	0.68
10	0.81	4.11 (NR)	0.62	0.92
11	0.85	0.5	0.52	0.5
12	0.99	0.99	0.52	0.99
13	0.94	0.48	0.45	0.93
14	0.68	0.88	0.51	0.79
15	R	R	NT	R

In the above shown table, P-value obtained for our system and variants of A5 family has been recorded. In all the tests, the P-value obtained for our system is positive (>0.001). Also comparatively higher values have been obtained. From the above shown table it can be observed that test no. 15 has not been conducted for the work - Enhanced A5/1 [10]. The higher the P-value for a given test, the stronger is the cipher system [7].

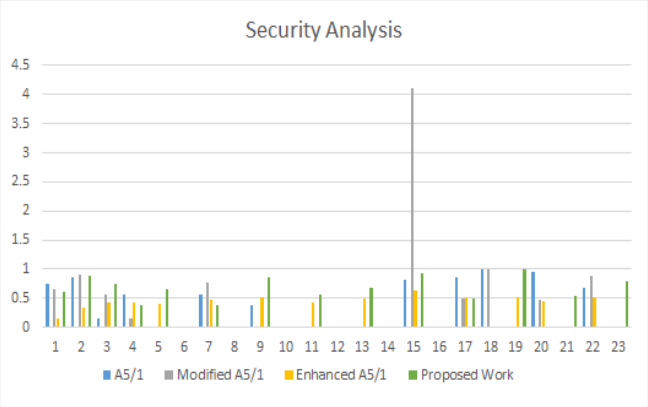

Fig. 4 Security Analysis and comparison

B. Power Consumption

We have taken use of new design of LFSR basing on power model using the mask method [12]. The capability of these LFSRs against the power attack is robust. The new design can be carried out easily by circuits. Since only XOR gates and flip-flops are adapted, the better synchronization performance will be achieved, which makes the new LFSR suitable in the context of Unattended Wireless Sensor Networks.

V. CONCLUSION

In this paper, we have proved that by changing the clocking bit associated with the participating registers leads to performance improvement. Modifications have resulted in complexity improvement of the base scheme to make it robust towards attacks. Substantial results under different tests have proved the efficiency of the proposed scheme. The operations in our system have been cost economic. Mobile adversaries have to put more effort to compromise sensor collected data. The special register in our design i.e., CBNR has been the vital in proving randomness property. Based on the results obtained, we say that the proposed scheme is robust to various security attacks compared to the conventional A5/1 stream cipher and its other variants. Hence the proposed scheme can be considered trustworthy in the context of UWSN operations.

REFERENCES

1. Di Pietro, R., Mancini, L. V., Soriente, C., Spognardi, A.,and Tsudik, G. Catch Me (If You Can): Data Survival inUnattended Sensor Networks. 2008 Sixth Annual IEEE nternational Conference on Pervasive Computing and Communications (PerCom) (Mar. 2008), 185–194.
2. Di Pietro, Roberto and Mancini, Luigi V. and Soriente, Claudio and Spognardi, Angelo and Tsudik, Gene, "Playing hide-and-seek with a focused mobile adversary in unattended wireless sensor networks," Ad Hoc Netw., vol. 7, no. 8, pp. 1463-1475, November 2009.
3. K. Dasgupta, M. Kukreja, K. Kalpaki, Topology-aware placement and role assignment for energy-efficient information gathering in sensor networks, in: IEEE International Symposium on Computer and Communication, 2003, pp. 341–348
4. Hamid, Muhammad E., and Chien-In Henry Chen. "A note to low-power linear feedback shift registers." IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing 45.9 (1998): 1304-1307.
5. Vracar, Ljubomir M., et al. "Influence of Encryption Algorithms on Power Consumption in Energy Harvesting Systems." Journal of Sensors 2019 (2019).
6. Ekdahl, Patrik, and Thomas Johansson. "Another attack on A5/1." IEEE transactions on information theory 49.1 (2003): 284-289.
7. NIST SP 800-22 Revision 1a, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-22r1a.pdf
8. Hegde, Nischaykumar, and Linganagouda Kulkarni. "An Optimal Cryptographic Approach for Addressing Security Breaches to Build Resilient WSN." Information and Communication Technology for Intelligent Systems. Springer, Singapore, 2019. 21-27.
9. Zeghid, Medien, et al. "A modified AES based algorithm for image encryption." International Journal of Computer Science and Engineering 1.1 (2007): 70-75.
10. Bajaj, Nikesh. "Effects of Parameters of Enhanced A5/1." International Journal of Computer Applications 2.2 (2011): 7-13.
11. Recommendation GSM 02.09, European Telecommunications Standards Institute (ETSI), Security aspects.
12. Yongbin, Zhao. "Design of feedback shift register of against power analysis attack." Computers, Materials & Continua 58.2 (2019): 517-527.
13. C Stroud, "Linear Feedback Shift Registers", CSE Dept., Auburn University, 10/04

AUTHORS PROFILE

Hegde, Nischaykumar completed B.E in 2005 and M.Tech in 2011. Currently pursuing PhD at Visvesvaraya Technological University, Belagavi. Teaching experience more than 14 years.

Kulkarni, Linganagouda obtained his PhD from Mysore University in 1992. Teaching experience more than 30 years. His research interest is in the field of Image Processing and Computer Networks. He has been research supervisor for 8 plus scholars.