Malaysian Journal of Mathematical Sciences 7(S): 59-72 (2013)
Special Issue: The 3rd International Conference on Cryptology & Computer Security 2012
(CRYPTOLOGY2012)

MALAYSIAN JOURNAL OF MATHEMATICAL SCIENCES

Journal homepage: http://einspem.upm.edu.my/journal

Polynomial Based Key Distribution Scheme for WPAN

[1*]R. Vimalathithan, [2]D. Rossi, [2]M. Omana, [2]C. Metra
and [3]M. L. Valarmathi

[1]KPR Institute of Engineering and Technology, Coimbatore, India

[2]University of Bologna, Bologna, Italy

[3]Government College of Technology, Coimbatore, India

E-mail: athivimal@gmail.com

*Corresponding author

ABSTRACT

Security plays a vital role in Wireless Personal Area Network where the data has to be transmitted in free space. The security of the data depends upon the key used for encryption/decryption. Also a secret key has to be shared among the nodes to establish a secure link. The secret key should be resilient to attacks. Key distribution among the nodes in Wireless Personal Area Network is a challenging task. To guarantee the message freshness, a rolling code sequence is appended with the transmitted message. In this paper, various feedback shift registers were analyzed for generating the rolling code and a polynomial based Key distribution scheme is proposed for secured communication protocol in Wireless Personal Area Network. Nonlinear feedback shift register with high linear complexity is used for generating the rolling code. Also the Node Capture Impact for the proposed scheme is compared with other existing scheme. The proposed scheme features a Node Capture Impact equals to zero for even any number of compromised nodes, which is recommended characteristic of a key distribution scheme.

Keywords: Cryptography, encryption, decryption, rolling code, primitive polynomials, node capture impact, communication protocol, security, sensor nodes.

1. INTRODUCTION

Wireless Sensor Network (WSN) is a network of sensor nodes and all nodes are battery operated devices, usually small in size with an inbuilt low power radio frequency transreceiver which can be capable of transmitting/receiving data within a small range. Sensor networks have a wide range of applications (Ilyas and Imad (2005)) like automation (Jose (2007)), wild life assessment (Geoff and Yen (2010)), traffic monitoring etc., with low implementation cost and low energy requirements. An inexpensive low rate WSN, also named as Wireless Personal Area Network (WPAN) is emerging and slowly becoming an inherent part of our lives.

A WPAN may operate in either of two topologies (Figure 1): the star topology or the peer to peer topology. In the star topology, the communication is established between nodes, which can be Full Functional Devices (FFD) or Reduced Functional Devices (RFD) and a single central controller (which must be an FFD), called the WPAN coordinator. The WPAN coordinator is the primary controller of the WPAN. The peer-to peer topology also has a WPAN coordinator, but any device can communicate with any other device as long as they are in range of one another.

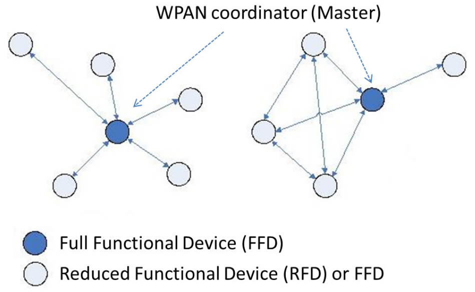
WPAN coordinator (Master)
● Full Functional Device (FFD)
○ Reduced Functional Device (RFD) or FFD

Figure 1: WPAN Star and Peer-to-Peer topology

Since the datas are transmitted in free space, and anyone can access the free space medium, thereby the data, cryptography is applied for secure transmission. A secret key is required among the sender and receiver for encryption/decryption. Usually this secret key is distributed by a trusted third party named Key Distribution centre. Public key cryptography mechanism is well suited for key distribution, but it requires large number of mathematical computation, and therefore it consumes a lot of energy. Since the nodes in WPAN have limited amount of energy, Public Key Cryptography mechanism is not suitable for WPAN. On the other hand, Private-key cryptography is suited for WPAN due to its low energy requirements (Ilyas and Imad (2005)). Key distribution is usually done off-line before deployment of nodes. Once the nodes are placed, they can communicate each other and compute a common key for highly secured data exchange among the nodes.

In case of the Standard IEEE 802.15.4, the key used for encryption /decryption is stored in the memory of each nodes and can be identified at the time of requirement, by the key identifier mode in the security control filed and key lookup table (IEEE Std 802.15.4™-2006). In this case, the nodes can use only a set of predefined keys. This approach is hardly scalable with the number of nodes: As the number of nodes of the network increases, then a large number of keys have to be stored in the memory, which requires more memory space and key accessing time. Also, it is very difficult to store the keys after the deployment of nodes. Moreover, the key used for data traffic must be periodically refreshed, in order to prevent the antagonist from acquiring the information about key. This may take long and time consuming sequence of procedures. Finally, a further threat to network security comes from the fact that, since the nodes are placed in unmanned environment, there is a possibility of node capture by an antagonist. Node Capture is one type of attack in sensor networks, where an antagonist can acquire the node and have control over the entire node by accessing information stored in the memory. Even a single captured node can imperil the entire network thereby the entire key is known to the antagonist. Node Capture Impact (NCI) is an important metric which gives the information about the number of nodes to be attacked by antagonist to imperil the entire network.

Maala *et al.* (2008) analyzed the Key management schemes for heterogeneous networks, derived the NCI (Maala *et al.* (2009)) and analyzed for Asymmetric Pre-distribution key management (AP), Hierarchical Key Management Protocol for Heterogeneous WSN (HERO), and Two Level Architecture for Key Management Scheme (TLA). From their analysis it can be derived that the secure communication can be broken for AP scheme if 30% of sensor nodes are compromised; for HERO scheme, if 70% of nodes are compromised then the secure communication can be broken. In case of TLA, if 100% of sensor node is captured then the NCI is only 10%.

Patrick and Radha (2007) investigated the node capture attack modeling for key establishment protocol in heterogeneous wireless ad hoc and mesh networks. They have shown how privacy-preserving key establishment protocol can prevent the node capture attack. The adversary can perform Heuristic attack at increased cost to attack the key even for randomized storage.

A novel protocol for WPAN has been proposed by Rossi *et al.* (2010), where the, message integrity and authenticity are guaranteed by a Message Authentication Code (MAC), similarly to the standard IEEE

802.15.4. In case IEEE 802.15.4, to guarantee the message freshness, a simple frame counter is used whose next sequence can be easily predicted by the antagonist. Instead, as for message freshness, Rossi *et al.* (2010) propose to provide it by using a technique based on rolling code (RC) instead of simple frame counter as in IEEE 802.15.4.

In this paper, the WPAN protocol security is improved by using a Non-Linear Feedback Shift Register (NLFSR) to generate the frame counter sequence so that the next sequence cannot be predicted by the attacker. Also a polynomial based key distribution scheme is proposed to improve the security. The proposed scheme can be used for other WPAN where high security is required even after the nodes get compromised.

The rest of the paper is organized as follows: Section 2 describes the Key generation technique using linear feedback shift register. Analysis and selection of the shift registers are discussed in section 3, while our proposed polynomial based Key distribution scheme is explained in Section 4. Node Capture Impact is derived in Section 5 for the proposed key distribution scheme and is compared with that of alternative solutions. Section 6 concludes our paper.

2. KEY GENERATION WITH LINEAR FEEDBACK SHIFT REGISTERS

In our proposed approach, a Linear Feedback Shift Registers (LFSR) is employed to generate 128 bit key used for AES encryption. Feedback shift registers perform two functions: One for shifting the input in the forward path and other for performing a linear function in the feedback path. A simplest form of feedback shift register is linear feedback shift registers that, when clocked, shifts the data through the register from one bit to the next most-significant bit (Shun-lung Su *et al.* (2006)). LFSR is used as keystream generators, Design for Test (DFT), Built in Self-Test design (BIST) and in wireless communication systems employing spread spectrum techniques. Moreover, an LFSR constructed using primitive polynomial can produce strong cryptographic binary sequences with a large period. LFSRs can be implemented both in hardware and software (Liang and Jing (2010)): the main advantages of hardware LFSRs are that they are faster and easy to implement, since the hardware uses simple XOR gates and summation.

An LFSR of length L consists of L flip-flops each capable of storing one bit and having one input and one output. A common clock is used to control the shifting of data stored in each FF. As an example, let us consider a simple LFSR as shown in Figure 2. For each clock pulse, a bit in the each shift register is shifted to the right, and the new left-most bit is computed as a function of the other bits in the register as follows:

$$C_L = \sum_{k=0} C_k S_k \tag{1}$$

The output of the register S_0 is the output of the LFSR which is 1 bit for a single clock.

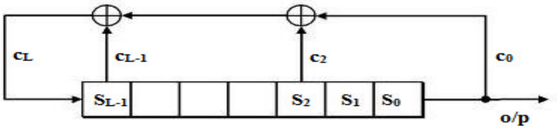

Figure 2: Linear Feedback Shift Register.

An LFSR is usually denoted by <L, C(D)>, where $C(D)=1+{}_{C_1}D+{}_{C_2}D^2+{}_{C_3}D^3+\ldots+{}_{C_L}D^L$. The parameter L is the number of FSR or the order of the polynomial, D^i is the content of register $S_{i\,,}$ and the connection to the feedback position is defined by the power of D in the polynomial.

Starting from the XOR (XNOR) gates, shift registers and properly selected coefficients c_i in C(D) (provided c_0 and c_L always takes the value one), a pseudorandom binary sequence with large period 2^L-1 can be generated. The pattern with all zeros is excluded in order to avoid the system get stuck into the same all zeros sequence (in case if XNOR gates are used in the feedback, all ones must be excluded). An LFSR is said to be Non-singular if C_L=1 i.e., C(D) is of order L. As already said if C(D) is primitive then maximum period sequence can be obtained. Also the reciprocal of a primitive polynomial C(D) is primitive, which is denoted by C^*(D) and reciprocal of Non-Primitive Polynomial is also Non-Primitive. A polynomial $C(D)$ is said to be reciprocal if $C^*(D)=D^L.C(1/D)$.

There is no reciprocal for a primitive polynomial with L=2 and 3, since the polynomial and its reciprocal are the same. The sequence produced by the LFSR that uses reciprocal polynomial is in reverse order and LFSR using reciprocal polynomial is called reverse order Pseudo Random Binary sequence Generator PRBG. The sequence generated by LFSR is used as key for encryption and decryption (Menezes *et al.*(1996)).

3. ANALYSIS OF NLFSR-BASED GENERATION FOR ROLLING CODE SEQUENCE

Non-Linear Feedback Shift Registers (NLFSR) is an alternative to LFSR. The current output of NLFSR is a non-linear function of the previous state. NLFSR can be easily implemented in hardware (Pey-Chang and Sunil (2010)) and due to the non-linearity, it is cryptographically stronger than LFSR. Geffe generator is one of the non-linear combination generators where the outputs of LFSR's are combined by a non- linear function. This combining function is used in order to break the linearity in the built-in LFSR. The clock controlled generators, namely Alternating Step Generator (ASG) and the Shrinking Generators (SG) are NLFSR structures composed by multiple LFSRs, where the output of one LFSR is used to control the clocking of other LFSR (Menezes (1996)). Since the second LFSR is clocked in an "irregular" manner, the output of the second LFSR turns out to be unpredictable. Particularly, the ASG uses three LFSRs. LFSR R_1 is used to control the stepping of two LFSRs, R_2 and R_3. The output sequence of the ASG is the XOR of the output sequences of R_2 and R_3 (Shun-lung *et al.* (2006)). The algorithm for generating the output is clearly described in Table 1. An important metric defining security level of feedback shift register is Linear Complexity, denoted by LC(S) for a sequence 'S', defined as the length of the shortest Linear Feedback shift register which can produce the same sequence 'S' generated by an LFSR. If the Linear complexity of a sequence is small, then the equivalent LFSR which generates the same sequence can be easily obtained using Berlekamp-Massey algorithm (Massey (1969)). The structure of an LFSR can be easily identified by observing 2L consecutive sequences (Berlekamp (1968)). The period and LC of various Shift Registers were analyzed and reported in the Table 2.

TABLE 1: Algorithm for generating the output using ASG

```
1.        Clock the register R1
2.        Check the output R1
If R1= 1 : clock the R2; repeat the previous output bit of R3
Else : clock the R3; repeat the previous output bit of R2
3.        XOR R2 and R3 to form the keystream.
Note: For the first clock cycle, the "previous output bit" of R2 and R3 are taken to
be 0.
```

TABLE 2: Period and Linear complexity of various FSRs

Generators	Number of LFSR	Period	Linear Complexity LC
LFSR	1	2^L-1	2L
Geffe Generator	3	$(2^{L}{}_{1}- 1) (2^{L}{}_{2}- 1) (2^{L}{}_{3}- 1)$	L_1L2+ L2+L1L3
ASG	3	$2^{L}{}_{1} .(2^{L}{}_{2}-1) (2^{L}{}_{3}-1)$	$(L_2+L_3).2^{L}{}_{1}{}^{-1} < LC \leq (L_2+L_3).2^{L}{}_{1}$
Shrinking Generator	2	$(2^{L}{}_{2}-1). (2^{L}{}_{1}{}^{-1})$	$L_2.2^{L1-2}< L(x) \leq L_2.2^{L1-1}$

TABLE 3: Linear complexity of FSR for variable length

Generators	Linear Complexity LC (bits)		
	L=32	L=64	L=128
LFSR	64	128	256
Geffe Generator $L_1= L_2= L_3=L$	2080	8256	32896
ASG $L_1= L_2= L_3=L$	$1.3744x10^{11}$	$1.1806x10^{21}$	$4.3556x10^{40}$
Shrinking Generator $L_1= L_2= L$	$3.4360x10^{10}$	$2.9515x10^{20}$	$1.0889x10^{40}$

Table 3 shows the linear complexity of shift registers with various shift register's lengths. From the Table 3, it is concluded that ASG have highest LC and hence Alternating Step Generator is selected for generating the rolling code (RC) sequence so that the next sequence cannot be easily predicted by the antagonist which overcomes the disadvantage of IEEE 802.15.4. Figure 3 shows the linear complexity of the LFSR and Geffe generator whereas Figure 4 shows the linear complexity of ASG and shrinking generator. The LC of ASG is high when compared to Geffe and Shrinking Generator.

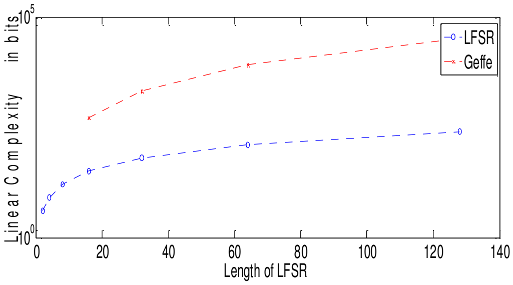

Figure 3: Linear complexity vs length for LFSR and Geffe generator

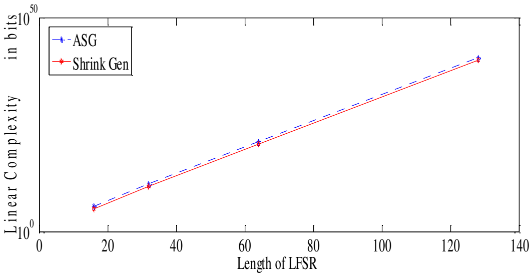

Figure 4: Linear complexity vs length for ASG and shrinking generator

4. POLYNOMIAL BASED KEY DISTRIBUTION SCHEME

Here we propose a polynomial based key distribution scheme for secured communication protocol. Figure 5 and Figure 6 shows the message structure to be used at the transmitter and receiver side, respectively.

At the transmitter side (Figure 5), transmitter id, receiver id, RC sequence (employed to guarantee message freshness) and useful message, transmitted in clear text, are encrypted using AES to generate the MAC. The numbers shown in each block represent the corresponding bit size. The number of transmitter/receiver nodes can be up to 2^6. The message type indicates the type of payload like command/data. While transmitting the data, Message Authentication Code (MAC) is appended to the useful message and transmitted. For key selection, a set of primitive polynomial is stored in all the nodes and the information about the polynomials stored in each node must be shared with the Master node. Some of the primitive polynomials used are {128,126,101,99,0}, {128,123,78,64,0}, {128,7,2,1,} which represent the coefficients for the LFSR. The remaining polynomials are taken from the table of Primitive polynomial derived by Miodrag (1985).

Whenever a Master wants to communicate with a particular node, it has to send two components: First component is the information about the seed of the NLFSR, which is determined from the RC sequence and the second component is the polynomial identifier, which is determined from the two least significant bits of RC. It should be noted that Master node does not require any extra bits to identify these parameters, which instead can be derived from the RC sequence, thereby reducing the transmission and computational time, as well as power.

The seed is generated using 16-128 bit expansion algorithm (it copies 16 bit RC eight times to generate 128 bit). Using a simple hardware and minimum number of polynomials, a large number of keys can be generated by simply varying the seed. The key is generated using 128 bit Galois Type LFSR. For each and every communication the seed and primitive polynomials are varied, hence a variety of key can be generated using simple hardware. Since different keys are used for each transmission, the number of encrypted data available in channel for an attacker is considerably smaller than the other schemes with shared keys for all nodes, thus making the proposed solution highly secured against attacking. Particularly, using 128 bit LFSR, 2^{128}-1 sequences can be generated. A system operating at 100GHz would require 10^{12} years to circulate all possible sequences.

At the receiver side (Figure 6), the data received are encrypted using AES to generate MAC and compared with the received MAC. If they are equal then the receiver validates the received message. To generate the key at the receiver, RC is used as input for expansion algorithm to generate the seed for LFSR. The 128bit key generated by LFSR is used by AES encryption algorithm to generate the MAC for validation. In this case, even if a node gets compromised, only the polynomial coefficient is accessed by the antagonist. Since the seed value is changed for each transmission (encryption/decryption), the key used for each transmission will be different. This is equivalent to one key per transmission, which provides high level of security. In fact, the difficulties usually encountered to exchange one key for each transmission are elegantly overcome by using polynomial based key distribution.

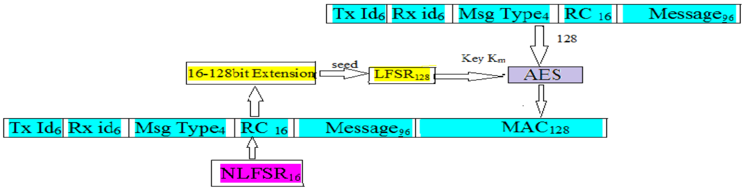

Figure 5: Transmitter Protocol

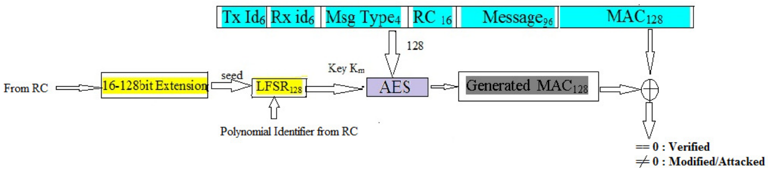

Figure 6: Receiver Protocol

5. NODE CAPTURE IMPACT EVALUATION

Node Capture attack is an atrocious attack in WPAN, where antagonist try to capture the nodes placed in an unmanned environment. It is unavoidable to prevent these unmanned nodes from the antagonist. The Ultimate goal of the antagonist is to access the memory and find out the keys stored in the node to hear the future communication amongst the non-compromised (con-captured) nodes. NCI is an important metric that says about the minimum number of nodes required to imperil the entire network.

Here we derive the Node Capture Impact factor for our proposed key distribution scheme and compared it with TLA scheme. An attacker may attack the network through compromising one or more sensor nodes which may be super node or normal node. Usually the super node (WPAN coordinator, FFD) is highly secure and tamper resistant to such attacks. Hence we assume that the attacker can hack only normal nodes (RFD).

Suppose that the key pool is $\chi=\{K_1,K_2,K_3,K_4,K_5,K_6,K_7,K_8\}$ and the number of keys stored in each node is $\sigma=2,$ we assume that the nodes a, b and c store the keys $\{K_1,K_2\}=\sigma_a\{K_3,K_4\}=\sigma_b$ and $\{K_5,K_6\}=\sigma_c,$ respectively. Each set of keys stored in a node is called key ring. In this case the key rings are independent, because there is no common element between any two nodes, that is: $\sigma_a\cap\sigma_b=\sigma_a\cap\sigma_c=\sigma_b\cap\sigma_c=\{\phi\}.$ These types of key rings are called independent key rings. Instead, if at least one common key is found between any subset of key ring (as it is usually the case in normal sensor nodes) then the corresponding key ring is called dependent key ring. For example if a, b and c store the keys $\{K_1,K_2\}=\sigma_a\{K_2,K_4\}=\sigma_b$ and $\{K_1,K_4\}=\sigma_c,$ respectively. In this case it is $\sigma_a\cap\sigma_b=\{K_2\},\sigma_a\cap\sigma_c=\{K_4\}$ and $\sigma_b\cap\sigma_c=\{K_1\}.$

Let us assume that each normal node stores σ keys, and let χ be the total number of keys in the pool. Let us consider also the following notation:

(i) λ_1 is the event that the key rings of the compromised nodes are independent.

(ii) λ_2 is the event that the key rings of the compromised nodes are non-independent.

(iii) P_1 is the probability of the total number of compromised keys when the key rings of the compromised nodes are independent. Then, P_1 = Prob(λ_1).

(iv) P_2 is the probability of the total number of compromised keys when the key rings of the compromised nodes are non-independent. Then, P_2=Prob (λ_2).

Therefore, the Node Capture Impact is

$$NCI = P_1 + P_2 \tag{2}$$

The probabilities P_1 and P_2 are calculated as described in the next paragraphs.

The probability that a key belongs to a particular node N_n is σ/χ, while the probability that a key does not belong to a particular node N_n is $1-(\sigma/\chi)$, while the probability that a key does not belong to a particular node N_n is $1-(\sigma/\chi)$.

Considering C_P compromised nodes, the probability that a key does not belong to a compromised node is

$$x_1 = \left(1 - \frac{\sigma}{\chi}\right)^{C_P} \tag{3}$$

Therefore, the probability of the total number of compromised keys when all key rings are independent is

$$P_1 = 1 - x_1,$$

while the probability of the total number of compromised keys if all key rings are not independent is

$$P_2 = \left[1 - \left(1 - \frac{\sigma}{\chi}\right)^{C_P}\right] * \sum_{j=2}^{C_P} \sum_{i=1}^{\sigma} P(i,j) \tag{4}$$

where $j \in [2,c]$ is the number of compromised N_n normal sensor nodes and $P(i,j)$ is the probability of having $i \in [1,\sigma]$ shared keys between any j compromised N_n sensor nodes. It is

$$P(i,j) = \frac{(\chi!)^{(1-j)} * (\sigma!(\chi-\sigma)!)^{j}}{i! * (\chi - i - j*(\sigma-i))! * (\sigma-i)! * (j*(\sigma-i)-\sigma+i)!} \tag{5}$$

From these equations we can derive NCI as

$$NCI = P_1 + P_2 = \left[1 - \left(1 - \frac{\sigma}{\chi}\right)^{C_P}\right] * \left[1 + \sum_{j=2}^{C_P} \sum_{i=1}^{\sigma} P(i,j)\right] \tag{6}$$

For TLA, the number of keys stored in each node is $\sigma = 1$ (therefore i =1). Hence, $P(1,j) = \chi^{1-j}$. Therefore, the NCI for the TLA solution is

$$NCI_{TLA} = \left[1 - \left(1 - \frac{\sigma}{\chi}\right)^{C_P}\right] * \left[1 + \sum_{j=2}^{C_P} (x)^{1-j}\right] \tag{7}$$

Instead, for the proposed Polynomial based Key Distribution scheme (*Poly*), the number of keys stored in each node is $\sigma = 0$ (therefore i =0). Therefore, the NCI turns out to be

$$NCI_{poly} = 0 \tag{8}$$

Figure 7 shows the plot of NCI for TLA and Polynomial based scheme. From the figure7 it is observed that, for TLA, the NCI increases as the number of capture node increases. If the breaking point is 0.25 then for TLA, 700 nodes is enough to imperil the entire network, whereas in our case, the NCI is zero for any number of captured nodes. This confirms that polynomial based Key Distribution scheme can be effectively used for key distribution among the nodes.

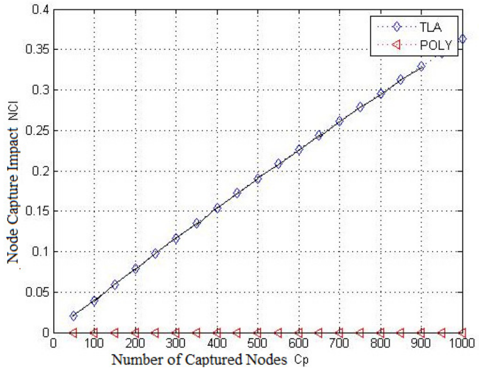

Figure 7: Node capture Impact (NCI) for TLA and Polynomial based key distribution

6. CONCLUSIONS

A Secured communication protocol is proposed which uses rolling code sequence for guarantee the message freshness and a polynomial based key distribution scheme is also proposed. From the analysis of shift registers, AGS is used for generating the Rolling code, and from the Node Capture Impact analysis, we found that, differently from alternative solutions, for the proposed scheme NCI is zero independently of the number of nodes that are captured or compromised. Hence the node can be placed in any environment, even in unsecured environment. Also the number of nodes is scalable, therefore any number of nodes can be introduced in the network without increasing the memory capacity. This proposed protocol provides high level of security and is suitable for WPAN.

REFERENCES

Berlekamp, E. R. 1968. *Algebraic Coding Theory*. New York: Mc Graw Hill.

Geoff, V. M. and Yen, Kheng Tan. 2010. *Wireless Sensor Networks: Application-Centric Design*. InTech Publishers.

IEEE Standard for Information technology Telecommunications and information exchange between systems Local and metropolitan area networks Specific requirements. 2006. IEEE Std 802.15.4™.

José, A. G. 2007. On the Use of IEEE Std. 802.15.4 to Enable Wireless Sensor Networks in Building Automation. *International Journal of Wireless Information Networks*. **14**(4): 295-301.

Liang, W. and Long, J. 2010. A Cryptographic Algorithm Based on Linear Feedback Shift Register. *International Conference on Computer Application and System Modelling (ICCASM 2010)*, pp. 526-529.

Maala, B., Bettahar, H. and Bouabdallah, A. 2008. TLA: A Tow Level Architecture for Key Management in Wireless Sensor Networks. *Proceeding of IEEE SensorComm 2008*, CapEsterel, France, pp. 639-644.

Maala, B., Challal, Y., Bettahar, H. and Bouabdallah, A. 2009. Node Capture Attack Impact on Key Management Schemes for Heterogeneous Wireless Sensor Networks. *Information Infrastructure Symposium (IEEE).*

Massey, J. L. 1969. Shift-register synthesis and BCH decoding. *IEEE Trans. Inf. Theory*. **15**(1): 122-127.

Menezes, A., van Oorschot, P. and Vanstone, S. 1996. *Handbook of Applied Cryptography*. CRC Press.

Miodrag, Z. 1985. *Table of Primitive Binary Polynomials*.

Mohammad Ilyas and Imad Mahgoub. 2005. *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems.* CRC Press.

Patrick, T. and Radha, P. 2007. Modeling Adaptive Node Capture Attacks in Multihop Wireless Networks. *Elsevier Ad Hoc Networks*. **5**(6): 801-814.

Pey-Chang Kent Lin and Sunil P. Khatri. 2010. VLSI Implementation of a Non-Linear Feedback Shift Register for High-Speed Cryptography Applications. *GLSVLSI'10 ACM*.

Rossi, D., Omana, M., Giaffreda, D. and Metra, C. 2010. Secure Communication Protocol for wireless Networks. *IEEE East- West Design and Test Symposium.*

Shun-lung Su, Ko-ming Chiu and Lih-chyau Wuu. 2006. The Cryptanalysis of LFSR/FCSR Based Alternating Step Generator. *IEEE 2006.*