May 31 International Journal of advanced studies in Computer Science and Engineering
IJASCSE, Volume 3, Issue 5, 2014

Analysis of Key Management Schemes for Secure Transmission in Wireless Sensor Networks

Usha Mahalingam
Professor,
Department of Computer Science and Engineering
Sona College of Technology
Salem, Tamil Nadu, India

Prema Latha. D
PG Scholar,
Department of Computer Science and Engineering
Sona College of Technology
Salem, Tamil Nadu, India

***Abstract*- Messages are transmitted among sensors in a Wireless Sensor Network in a secure way by using cryptographic techniques. Communication complexity is the major challenge in transmitting messages between sensors into the Internet of Things. As IOT consists of different devices, there must be secure and proper communication between sensor nodes in WSNs. In this work, a random key is used in practical time for reducing the communication complexity in IDEA algorithm. This paper proposes a model by combining the Reed Solomon code with IDEA encryption algorithm which used128 bit keys for transmitting the data. If the key gets lost, Reed Solomon code is used for key recovery. Experimental results are presented for RC4 and IDEA encryption techniques.**

Keywords- Internet of Things, Wireless Sensor Networks, IDEA, Key management, Reed Solomon code.

I. INTRODUCTION

A Wireless Sensor Network is a collection of different sensor nodes communicating in different applications like military services, health monitoring, data acquisition in hazardous areas, habitat monitoring, etc. In the message transmission between sensors, communication should be more reliable, authentication, integrity, confidentiality, non-repudiation using cryptographic algorithms. To reduce complexities in WSN through IOT (Internet of Things) [1], many techniques are practiced. Researchers have come up with Bilinear Diffie-Hellman Inversion problem [2] reduces the computation problem

A sensor node that wants to transmit messages into an open environment that potentially includes adversaries has to send these messages confidentially. At the same time, when the keys are to be distributed this has to be done securely with easy key recovery. Otherwise repeated transmissions increases the communication complexity of the key management algorithms and may drain the energy of the sensor nodes.

Light weight Cryptography [3], one of the cryptographic techniques develops a cryptographic system with limited resource. It is best suited for energy conversion need WSNs. It consists of different approaches like decreasing the block size and [4] key length, simplifying layers of transformations, reducing cost, using effective elements, designing key schedules, using cryptographic operations according to the available resources. Light Weight Cryptography approach for Internet of Things gives end-to-end communication efficiency and lower applicability of resource devices [5].Lightweight Cryptography Algorithms are preferred in the IOT to use minimum resources in secure communication [6] between sensors. IOT consists of different devices like sensors, modems, phones, etc., to communicate securely.

Key management [7] and distribution is a challenge in such environment. While the use of predistribution of keys is a predominant solution, researchers go for other enhancements such as key pools. Another approach is Bilinear Diffie-Hellman Inversion problem that is suitable for reducing computation complexity. But if key loss occurs during transmission it complicates the communication between the sensors. To overcome the communication complexity, the key is managed using Reed-Solomon (RS) [2] code recover the key in case of loss.

Reed-Solomon code is a linear code consisting of multiple symbols which provides error correction ability [8] to recover the key. During transmission of the message there is no key error recovery in Bilinear Diffie-Hellman Inversion problem. In order to provide secure communication between a pair of sensors, a unique key is needed. Since the usage of public and private key combination requires significantly more computation than that of secret key techniques, Reed-Solomon code is used

to reduce the communication complexity at the same time since the WSNs are energy constrained networks.

RC4 is a stream cipher [9], [13] and symmetric key algorithm. It is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream [10] is completely independent of the plaintext used. It uses key which is of variable length ranging from 1 to 256 bits. The authors have proposed a framework using RC4 combined with Reed Solomon code for key recovery in their proposed work

The IDEA [11] algorithm is a block cipher operates with 64-bit plaintext and cipher text blocks and it seems to be controlled by a 128-bit key. The algorithm consists of three different algebraic operations. The substitution boxes and the associated table lookups used in the block ciphers available to-date have been completely avoided. The algorithm structure is designed in such a way that different key sub-blocks are used where the encryption and decryption processes are similar.

Contributions

1. The novel proposal method consists of a model for reducing the loss of key in secure message transmission between sensor nodes using Reed-Solomon code.
2. IDEA is block cipher algorithm combined with Reed Solomon code for loss of key during the message transmission to reduce the communication complexity.
3. Performance RC4 [12] is a stream cipher algorithm combined with Reed Solomon code for number of messages transmitted

II. RELATED WORK

This section discusses the various approaches proposed in the literature. It also describes the Reed Solomon code and IDEA algorithm.

Multipath key Establishment [2] is used to enable two nodes to establish secure communication even if they do not share a common key. It is used to capture the active attacks but there is limitation in communication complexity.

Public key cryptography [14] is used for authentication and advantage is to reduce the overhead in signature amortization but it does not concentrate in recovering the key if it is loss.

Key predistribution scheme [15] provides the secure communication between sensor nodes using three schemes such as polynomial pool-based key predistribution scheme, the probabilistic generation key predistribution scheme and the Q-composite scheme. It provides a better result in network resilience but limitations in communication complexity.

Key establishment [16] scheme used JERT scheme for secret link between sensor nodes through multi-hop paths. It reduces the transmission cost and provides secure information.

Three-tier [17] security scheme is used for pairwise key distribution and authentication. It reduces the damages caused by replication attacks and strengthens the security but does not concentrate in communication overhead.

Balanced Incomplete block designs [18] is used for security properties and computational performance Allocation of resource in WSN based on the access scheduling algorithms GAALS [19] for scalable WSN for single ratio multi hop communication.

A. Reed-Solomon codes

A Reed-Solomon code is a linear code, which means that the code words form a k-dimensional subspace of the vector space Fnq . A commonly used method of encoding a linear code is to construct a generator matrix, denoted by G, whose rows form a basis for the code. Then, to encode a message m, we compute c = mG.

There are different methods to make RS codes. It consists of encoding and decoding algorithms. Here, we only describe the general functionalities of the encoding/decoding algorithms. The input of the RS encoding algorithm is a message m= (m0, m1... m_{k-1}) ϵ F_q, finite field of order q and then the output will be c= (c0, c_{n-1}) ϵ F_q, where $k \leq n \leq q$. c is called a code word. Each element in m or c is called a symbol. K is the key.

It always happen that $c_i = m_i$ for $0 \leq i \leq k-1$, then the encoding is systematic. In this case , $m_0,..,m_{k-1}$ may be called information symbols and $c_k \ldots c_{n-1}$ may be called parity check symbols. Not all RS encoding schemes are systematic.

The above described RS code has length n and dimension k. Its distance is d = n- k + 1 (i.e., any two distinct code words differ in at least n – k + 1 symbols).

B. IDEA Algorithm

IDEA [18] operates on 64-bit blocks using a 128-bit key and consists of a series of eight similar transformations (a complete *round*) and an output transformation (half *of the overall round*). The processes for encryption and decryption [15] are similar. In IDEA much of its security operations are interleaved from different groups — modular addition and multiplication, and bitwise eXclusive OR (XOR) — which are algebraically "incompatible". The above mentioned operators, which all deal with 16-bit:

- Bitwise exclusive OR .
- Addition modulo 2^{16}
- Multiplication modulo $2^{16}+1$, where the all-zero word (0x0000) is interpreted as 2^{16}.

IDEA uses a block cipher with a 128-bit key, and is generally known to be very much secure. It is one of the best [19] publicly known algorithms. No practical attacks on it have been published so far despite of a number of attempts to find some.

III. ANALYSIS OF REED SOLOMON CODE

Reed & Solomon's original view:

To describe all the code words in Reed-Solomon code, the different set of procedures used. Every code word of the Reed–Solomon code is a sequence of low-degree polynomial function values. In order to attain a code word of in Reed–Solomon code, the message is interpretation is done as a report with the help of a polynomial *p* which has a degree less than *k* over the finite field called *F* with finite set of *q* elements. Consecutively, the polynomial *p* is calculated at *n* different points $a_1,...,a_n$ of the finite field *F*, and the sequence of calculated values are the related code word.

Formally, the set C of code words of the Reed–Solomon code is defined as follows: [11]

$C = \{(p(a_1), p(a_2)... a_n)) |$p is a polynomial over

F degree < K}

For any two different polynomials p of degree less than k agree in at most k-1 points, this means that any two code words of the Reed–Solomon code disagree in at least n-(k-1)=n-k+1positions. Furthermore, there are two polynomials which agree with k-1 points but are not equal. So, the distance of the Reed–Solomon code is exactly d=n-k+1. Then the relative distance is

$$\delta=d/n=1-k/n + 1/n\sim 1-R \qquad (2)$$

where R=k/n is the rate and the trade-off between them is asymptotically finest since, every code satisfies $\delta + R \leq 1$which is proved by the Singleton bound. Being achieved the best trade-off, the Reed–Solomon code comes under the class of maximum distance separable codes. When the number of different polynomials p of degree less than *k* and the number of different messages are both equal to q^k, every message can be distinctively mapped to such a polynomial [20] and there are alternative ways to do the encoding. In the actual construction of Reed Solomon code the message *x* is interpreted as the coefficients of the polynomial *p*, and in the following constructions the message is interpreted as the values of the polynomial at the first *k* points $a_1,..,a_k$. The polynomial *p* is obtained by interpolating these values $a_{1,...,}a_n$ with a polynomial of degree less than *k*. As the last encoding procedure increases the efficiency it gives another advantage that it increases systematic code. So, the original message is always covered as a subsequence of the code word.

In many contexts, it is suitable to choose the series of evaluation points so that they display some additional structure. In particular, it is useful to choose the sequence of successive powers of primitive root α of the field F and α is the generator of the finite set of field's multiplicative group. The sequence is defined as for all i=1,…, q-1. This sequence contains q-1 elements of F, except 0, and so the block length is n-1. It follows that, whenever p (a) is a polynomial over F, then the function p (αa) is also a polynomial p of the same degree, which gives rise to a code word obtained by the cyclic left - shift of the code word derived from p (a). Thus, this construction of Reed–Solomon code gives rise to a cyclic code.

The receiver will send the response to sender using the broadcast channel. Let e be the maximum error rate that the protocol is designed for (i.e., an e feasible ordered pair (n, k) is chosen for use in the protocol). Here MAC protocol is a secure message authentication protocol.

1. Sender chooses a random message $m = (m_0,\ldots,m_{k-1})$ Є and encodes it into an RS code word $c= (c_0,\ldots c_{n-1})$ Є
2. In each round, the sender sends one code word symbol over each of the pre specified node disjoint paths.
3. After each round, receiver attempts to choose the symbols among which have been received in the current and all previous rounds of the code word. If it is successful, then a message is derived from code word and

a key is derived from message.

4. If the sender is able to compute a key then receiver initiates a conventional message authentication code [21] (MAC)-based mutual authentication protocol with sender over the broadcast channel. In this, sender and receiver both hold the same key. If the authentication succeeds, then both the sender and the receiver halt the process. Since the broadcast channel provides integrity, the adversary is not able to change the message between sender and receiver .In the authentication protocol. If sender and receiver have the same key, then the adversary is not able to prevent the authentication from succeeding.

IV.PROPOSED WORK

The Data Encryption Standard (DES) algorithm is mostly used in commercial and financial applications. The IDEA encryption algorithm provides high level security as a secret, but slightly less in providing secret key. IDEA algorithm can be defined and understood easily and the level of accessibility is also high.

The block cipher IDEA operates with 64-bit plaintext and cipher text blocks and is controlled by a 128-bit key. The design of an algorithm consists of three different algebraic group operations. The algorithm structure is taken such that, with the exception that different key sub-blocks are used, the encoding process is indistinguishable to the decoding process.

The plaintext is divided into four sub blocks as 16 bits then all operations used in the encryption process performs on 16 bit numbers. Next process produces for each of the encryption round, six 16-bit key sub blocks from the 128-bit key. Since a further four 16-bit key-sub-blocks are required for the subsequent output transformation, a total of 52 (= 8 x 6 + 4) different 16-bit sub-blocks have to be generated from the 128-bit key.

In Reed Solomon code the message can be transmitted between sensors m= (m0, m1... m_{k-1}) ϵ F_q, finite field of order q and then the output will be c= (c0, …, c_{n-1}) ϵ F_q, where $k \leq n \leq q$. RS codes are essential linear block codes that are of significant theoretical and practical interest. A (n, k) RS code C, defined over a finite field F, is a k dimensional subspace of the n dimensional space F^n for a message polynomial $m(x) = m_0 + m_1x + ... + m_{k-1}x^{k-1}$. The encoding operation is to evaluate m(x) at x_1, x_2,....., x_n, where the x_i's are n distinct elements of F. The decoding algorithm guarantees correct decoding as long as the number of errors exceed the value of t= Γ(d-1)/2I, where d=n-k+1 is the minimum distance of the code.

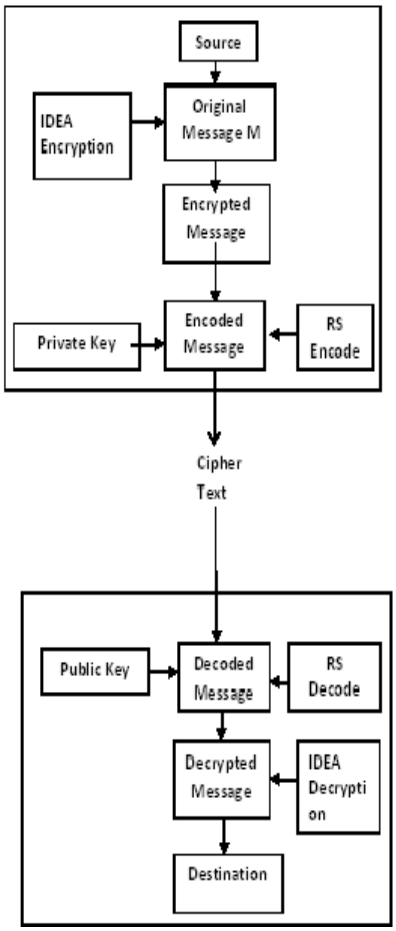

Figure 1: System Architecture

The message which is to be transmitted is first encrypted by using IDEA algorithm combined with Reed Solomon code. After combining the Reed Solomon Encode with the message, it is encrypted with the private key of the sender. After encryption, the encoded message is transmitted. At the receiver side, the transmitted message is decrypted using the public key and Reed Solomon decode will separate the message and code and it is again decrypted by IDEA which gives the original cipher text.

V RESULTS AND DISCUSSIONS

These two graphs show a comparison between two algorithms such as IDEA and RC4 with Reed Solomon code.

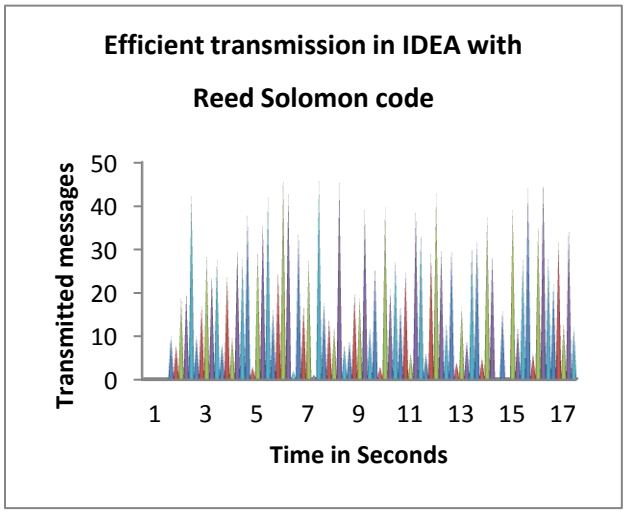

Figure 2: Efficiency Transmission in IDEA with Reed Solomon code

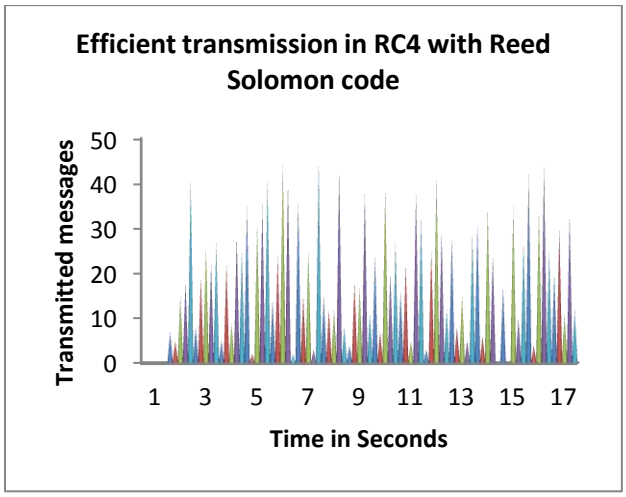

Figure 3: Efficiency of Transmission in Reed Solomon code with RC4

The first graph shows the transmission of messages using IDEA algorithm with RS code. The no of messages transmitted is taken in y-axis and the time taken is in x-axis in seconds. Using IDEA algorithm with RS code, the average time taken is above 20.

The second graph shows the transmission of messages using RC4 with RS code. The no of messages transmitted is taken in y-axis and the time taken in x-axis in seconds. Using RC4 algorithm with RS code, the average time taken is below 20.

It is clear from the observation that the transmission of messages using RC4 with RS code [22], the average time taken for transmission of messages is less than the time taken in IDEA with RS code. So the efficiency in transmitting messages is better in RC4 with RS code.

VI CONCLUSION AND FUTURE WORK

We have presented a key management scheme for wireless sensor networks. The scheme encrypts a message by using IDEA algorithm and Reed Solomon code. We believe that the following facts are addressed:

1. In memory constrained WSNs, key retransmission overhead is reduced by recovering the key using RS codes.
2. The energy efficiency is achieved by the key recovery and also reduces the communication complexity.
3. This algorithm is a strong block cipher as the cipher key size is 128 bits compared with efficiency encryption for IDEA with Reed Solomon code and RC4 with Reed Solomon code.

In future, key recovery can be achieved more efficiently by comparing different cryptographic algorithms which is most suited for wireless sensor during transmission of messages.

ACKNOWLEDGEMENT

The authors wish to thank their institution for partial funding support through SONANET Network Computing Research Center. Part of this work is supported by ACITE-RPS (FNo.: 8023/BOR /RID/RPS-68/2009-10). The authors also thank Prof S. Jayabharathi, Associate Professor/Mathematics and Mrs.G.Sarathalakshmi, Assistant Professor/English at Sona College of Technology for the review and suggestions.

REFERENCES

[1] Fagen Li and Pan Xiong "Practical Secure Communication for Integrating Wireless Sensor Networks into the Internet of Things", IEEE Sensors Journal, 2013.

[2] Jiang Wu and Douglas R. Stinson, "Three Improved Algorithms for Multipath Key Establishment in Sensor Networks Using Protocols for Secure Message Transmission", in IEEE Transactions on Dependable and Secure Computing, Vol.8, No.6, November/December 2011.

[3] Sergey Panasenko and Sergey Simagin, "Lightweight Cryptography: Underlying Principles and Approaches" in International Journal of Computer Theory and Engineering, Vol.3, No.4, August 2011.

[4] Masanobu Katagi and Shiho Moriai, "Lightweight Cryptography for the Internet of Things" in Sony Corporation, 2008.

[5]]Mihai T. Lazarescu, "Design of a WSN Platform for Long- Term Environmental Monitoring for IOT Applications", *Trans. on IEEE Journal on Emerging and Selected Topics in Circuit and Systems*, VOL. 3, No. 1, March 2013.

[6]Yang Zhou, Chuan Huang, Tao Jiang and Shuguang Cui, "Wireless Sensor Networks and the Internet of Things: Optimal Estimation with Nonuniform Quantization and Bandwidth Allocation", *Trans. on IEEE Sensors Journal*, VOL. 13, No. 10, October 2013.

[7]Maria Rita Palattella, Nicola Accettura, Luigi Alfredo Grieco, GennaroBoggia, MischaDohler and Thomas Engel, "On Optimal Scheduling in Duty-Cucled Industrial IOT Applications Using IEEE802.15.4e TSCH", *IEEE Sensors Journal*, VOL. 13, No. 10, October 2013.

[8]Mortuza Ali and MargretaKuijper, "A Parametric Approach to List Decoding of Reed-Solomon Codes Using Interpolation", *Trans. on IEEE Transactions on Information Theory*, VOL. 57, No. 10, October 2011.

[9]S.R. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4", Selected Areas in Cryptography, volume 2259 of Lecture Notes in Computer Science, pages 124 Springer 2001.

[10]S. R. Fluhrer and D. McGrew, "Statistical analysis of the alleged RC4 key stream generator", FSE, volume 1978 of Lecture Notes in Computer Science, pages 1930 Springer, 2000.

[11] Serigo L. C. Salomao, Joao M. S. De Alcantara, Vladimir C. Alves and Felipe M. G. Franca "Improved IDEA",Miltary Institute of Engineering.

[12]William Stallings, "Cryptography and Network Security: Principles and Practices", Fouth Edition, chapter6, 2009.

[13]Nadhem J. Alfardan, Daniel J. Bernstein, Kenneth G. Paterson, Bertram Poettering and Jacob C. N.Schuldt, "On the Security of RC4 in TLS and WPA", proceedings of the *USENIX Security Symposium* 2013.

[14] Yongshegliu,Jie Li and Mohsen Guizani,"PKC Based Broadcast Authentication using Signature Amortization for WSNs" , in IEEE Transactions on Wireless Communications, Vol.11, No.6, June 2011.

[15] Amar Rasheed and Rabi N.Mahapatra,"Key Predistribution Schemes for Establishing Pairwise Keys with a Mobile Sink in Sensor Networks",in IEEE Transaction on parallel and Distributed Systems,Vol.22, No.1,January 2011.

[16]Jing Deng and Yunghsiang S. Han, "Multipath key Establishment for Wireless Sensor Networks Using Just Enough Redundancy Transmission", *Trans. on IEEE Transactions on Dependable and Secure Computing*, Vol. 5, No.3, July-September 2008.

[17]Amar Rasheed and Rabi N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks", *Trans. on IEEE Transactions on Parallel And Distributed Systems*, VOL. 23, No. 5, May 2012.

[18]Seyit A.Çamtepe and BülentYener, "Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Networks", *Trans. on IEEE/ACM Networking* VOL.15, No. 2, April 2007

[19]Di Wu, LichunBao and Chi Harold Liu, "Scalable Channel Allocation and Access Scheduling for Wireless Internet of Things", *IEEE Sensors Journal*, VOL. 13, No. 10, October 2013.

[20]Hyunsung Kim, "Efficient and Non-Interactive Hierarchical Key Agreement in WSNs", *International Journal of Security and Its Applications* VOL. 7, No. 2, March, 2013.

[21] SushmitaRuj, AmiyaNayak, Ivan Stojmenovic, "Pairwise and Triple Key Distribution in Wireless Sensor Networks with Applications", *IEEE Transactions on Computers*, VOL. 62, No. 11, November 2013.

[22] Usha Mahalingam, D. Prema Latha, Amlan Chakrabarti, "A Novel Key Recovery Scheme in Wireless Sensor Networks for the Internet of Things", Asia Pacific Conference on Wireless and Mobile, 2014, pp 1-5.