Global Journal of Computer Science and Technology
Volume 12 Issue 9 Version 1.0 April 2012
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Sensor Data Encryption Protocol for Wireless Network Security

By Bharat Singh, Parvinder Singh & Dr. V.S. Dhaka
Central University of Rajasthan, Ajmer, Rajasthan

Abstract - Wireless Sensor Network consisting of a large number of sensor nodes that connected through wireless media has emerged as a ground breaking technology that offers unprecedented ability to monitor the physical word accurately. The privacy preservation is an important issue in wireless sensor network. Developing effective security solutions for wireless sensor networks are not easy due to limited resources. In this paper we propose new techniques for the purpose of security in wireless sensor network called as SDEP sensor data encryption protocol. In the scheme we use the RC 6 method for the purpose of encryption and decryption. RC 6 provide best confusion and diffusion properties with the less computational overhead. In order to confirm effectiveness of SDEP, a comparative performance evaluation with AES and RC 5 algorithms are presented in terms of memory requirement and execution time criteria. Our proposed scheme provides better performance than AES and RC 5 in the term of execution time and total memory requirement. We also provide simulation results for proposed method in the term of overhead and energy according to this result SDEP is strong block cipher for wireless sensor networks.

Keywords : SDEP, Security, RC 6 cryptography, AES.

GJCST Classification: C.2.0,D.4.6

SENSOR DATA ENCRYPTION PROTOCOL FOR WIRELESS NETWORK SECURITY

Strictly as per the compliance and regulations of:

Sensor Data Encryption Protocol for Wireless Network Security

Bharat Singh [α], Parvinder Singh [α] & Dr. V.S. Dhaka [σ]

Abstract - Wireless Sensor Network consisting of a large number of sensor nodes that connected through wireless media has emerged as a ground breaking technology that offers unprecedented ability to monitor the physical word accurately. The privacy preservation is an important issue in wireless sensor network. Developing effective security solutions for wireless sensor networks are not easy due to limited resources. In this paper we propose new techniques for the purpose of security in wireless sensor network called as SDEP sensor data encryption protocol. In the scheme we use the RC 6 method for the purpose of encryption and decryption. RC 6 provide best confusion and diffusion properties with the less computational overhead. In order to confirm effectiveness of SDEP, a comparative performance evaluation with AES and RC 5 algorithms are presented in terms of memory requirement and execution time criteria. Our proposed scheme provides better performance than AES and RC 5 in the term of execution time and total memory requirement. We also provide simulation results for proposed method in the term of overhead and energy according to this result SDEP is strong block cipher for wireless sensor networks.

Keywords : SDEP, Security, RC 6 cryptography, AES;

I. Introduction

A wireless Sensor Network is simple defined as a large collection of sensor nodes, equipped with its own sensor, processor and radio transceiver. A wireless sensor network has been widely used in different application areas to know the battlefield situation data, monitoring building parameters and reports about malfunction in a system.

The evolution leading to RC6 has provided a simple cipher yielding numerous evaluations and adequate security in a small package. After describing the structure of the algorithm, the prominent goal that stands out is simplicity. Through this simplicity, multiple evaluations have been performed, including AES-related evaluations, which will be discussed at a high level, due to complexity and number of articles. The fact that such a small, simple algorithm contended for AES with such high security requirements is noteworthy.

The main objective of our approach is to provide better performance than AES and RC 5 in the term of execution time and total memory requirement. We also provide simulation results for proposed method in the term of overhead and energy according to this result SDEP is strong block cipher for wireless sensor networks. In this new technique for the purpose of security in wireless sensor network called as SDEP sensor data encryption protocol. In the scheme we use the RC 6 method for the purpose of encryption and decryption. RC 6 provide best confusion and diffusion properties with the less computational overhead. In order to confirm effectiveness of SDEP, a comparative performance evaluation with AES and RC 5 algorithm are presented in terms of memory requirement and execution time criteria. Our proposed scheme provides better performance than AES and RC 5 in the term of execution time and total memory requirement.

II. Attacks on Wireless Sensor Network

Wormhole Attacks: In the wormhole attack an adversary builds a virtual tunnel through a low latency link that takes the messages from one part of the network and forwards them to another. The simplest case of this attack is when one node is located between two other nodes that are forwarding. However, wormhole attacks commonly involve two distant nodes that are colluded to underestimate the distance between them and forward packets through an external communication channel that is only available to the adversary.

Sinkhole Attacks: In a sinkhole attack, the adversary's goal is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the center. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm. Effectively, the adversary creates a large "sphere of influence", attracting all traffic destined for a base stations from nodes several hops away from the compromised node.

Subversion of a Node: A particular sensor might be captured, and information stored on it (such as the key) might be obtained by an adversary. If a node has been compromised then how to exclude that node, and that node only, from the sensor network is at issue defines an efficient way to do so.

Physical Attacks: Sensor networks often operate in hostile environments. In those environments, the size of the nodes plus the unattended operation mode contributes to make them very vulnerable to physical

Author α : M.Tech. Scholar Central University of Rajasthan, Ajmer, Rajasthan.
Author σ : Prof. & Dean Rajasthan Institute of Engineering &Technology, Jaipur Rajasthan.

attacks. In contrast to other types of attacks, physical attacks destroy the nodes permanently, thus, their loss is irreversible. For instance, an adversary could extract cryptographic keys, alter the node's circuitry, and reprogram it or replace it with malicious nodes.

Passive Information Gathering: An intruder with an appropriately powerful receiver and well designed antenna can easily pick off the data stream. Interception of the messages containing the physical locations of sensor nodes allows an attacker to locate the nodes and destroy them. Besides the locations of sensor nodes, an adversary can observe the application specific content of messages including message IDs, timestamps and other fields. To minimize the threats of passive information gathering, strong encryption techniques needs to be used.

False Node and Malicious Data: An intruder might add a node to the system that feeds false data or prevents the passage of true data. Such messages also consume the scarce energy resources of the nodes. This type of attack is called "sleep deprivation torture".

The Sybil Attack: In a Sybil Attack, a single node presents multiple identities to other nodes in the network. They pose a significant threat to geographic routing protocols, where location aware routing requires nodes to exchange coordinate information with their neighbors to efficiently route geographically addressed packets. Authentication and encryption techniques can prevent an outsider to launch a Sybil Attack on the sensor network.

Acknowledgement spoofing: Some routing algorithms require the use of acknowledgement signals (ACK). In this case, an adversary could spoof this signal in response to the packets that the adversary listens to. This results in convincing the transmitting node that a weak link is strong. Thus, an adversary could perform a selective forwarding attack after spoofing ACK signals to the node that the adversary intends to attack. Attacks to Data Aggregation Techniques Data aggregation in wireless sensor networks can significantly reduce communication overhead compared to all the nodes sending their data to the base station. However, data aggregation complicates even more network security. This is due to the fact that every intermediate node could potentially modify, forge, or discard messages. Therefore, a single compromised node could be able to alter the final aggregation value. Intruder node and compromised node attacks are two major threats to security in sensor networks that use data aggregation techniques. An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

III. Key Expansion Algorithm

The key expand algorithm is used to expand the user supplied key to fill the expanded array S, so that S resembles an array of t=(2*r+4) random binary words determine by user supplied key K. it is differ from RC5 version where more words are derived from user supplied key K. These drive words are star in array S which are uses later encryption or decryption. in our proposed method we simplify the key expansion terms of RC6.

In first step:

key expansion is to copy the secret key K [0…….b-1] into array L[0………..c-1] this operation is done in natural manner, using u consecutive key bytes of K to fill up each successive word in L, in little endian order. The two magic constraints Pw and Q_w define for arbitrary were follows:

$$P_w = Odd((e-2)2^w$$

$$Q_w = odd((Ø-1)2^w$$

These magic constant Pw and Q_w are uses for arithmetic progression modulo 2^w which provide randomness in table S.

In Second step:

In this step of key expansion we initialize array S to a particular pseudorandom bit pattern using an arithmetical progression modulo 2^w with magic constraint.

create and expanded key table S [0…………………2r+3] now we initialize this table by using magic constraints

$$S[o] = P_w$$

For i = 1 to (2r+3) do

$$S[i] = S[I-1] + Q_w$$

In third step:

The third algorithm steps of key expansion are to mix in the user's secret key in three phrases over the array S and L. More precisely, due to the potentially different sizes of S and L, the larger array will be processed three times, and the other array may be handled more times.

Mix the secret key into table, S

```
I = j = 0 ;  A = B = 0;
V = 3 x max { c, 2r + 4 }
For s = 1 to v do
{
 A = S [ i ] = S [ i ] + A + B) < < < 3
B = L [ j ] = ( L [ j ] + A + B ) < < < ( 3 + i )
J = ( j + 1 ) mod c
}
```

Key expansion function is an one way function so no one can determine secret key

Encryption :

This is a second phase of proposed scheme it composed with three states: pre-whitening, an inner loop of rounds, and post-whitening. Pre-whitening and post-whitening remove the possibility of the plaintext revealing part of the input to the first round of encryption and the cipher text revealing part of the input to the last round of encryption.

We uses four W bit input register A, B, C, D registers B and D undergo pre-whitening the register B and D put through the quadratic equation and rotated ($\log_2$ w) bits to the left respectively and these value store in variable t and u now register A XOR with t and left shift by u bits and added to round key S [2i].

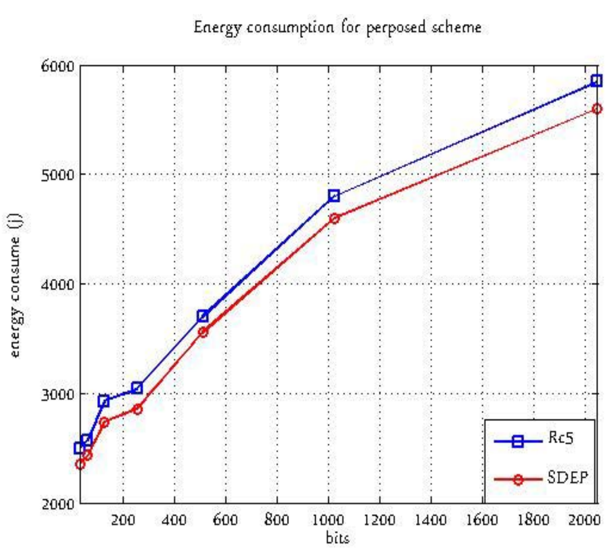
Similarly C is XOR with the value of u and left shift by t bits. Now it added to round key S [2 i + 1]

for I = 1 to r do

{
T = (B * (2 B + 1)) < < < $\log_2$ W
U = (D * 2 (2 D + 1)) < < < $\log_2$ W
A = ((A XOR t) < < < u + S [2i]
C = ((C XOR u) < < < t) + S [2i + 1]
(A, B, C, D) = (B, C, D, A)
}

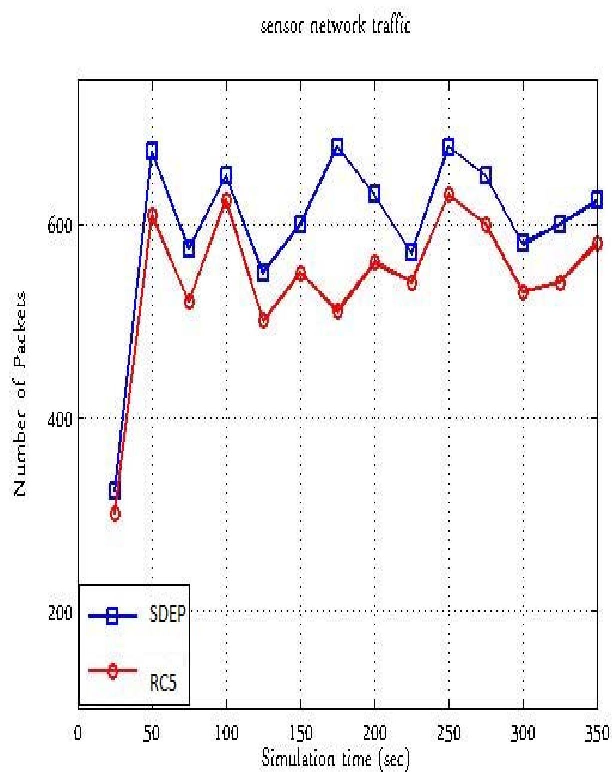
IV. Results

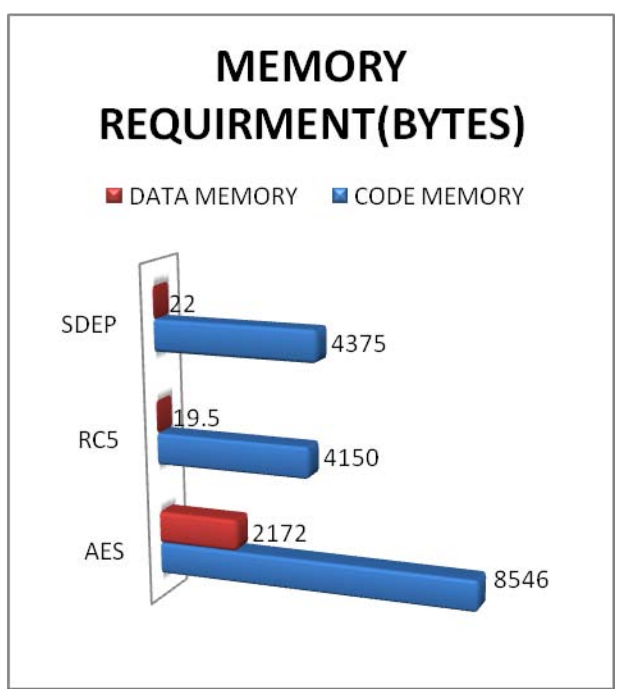
In this paper we have proposed a new algorithm for the security purpose in wireless sensor network. We also perform evaluation this new approach by comparing with two alternative popular algorithm AES and RC5. We investigate performance of this new algorithm based on memory requirements and the bandwidth according to our result the bandwidth for SDEP is much less than AES and RC5. Memory requirement for both code and data is less than AES and nearly equal to RC5. According to these simulation results our new algorithm SDEP much better than RC5 and AES in term of memory requirement, bandwidth requirement and time delay. It is also very much energy efficient.

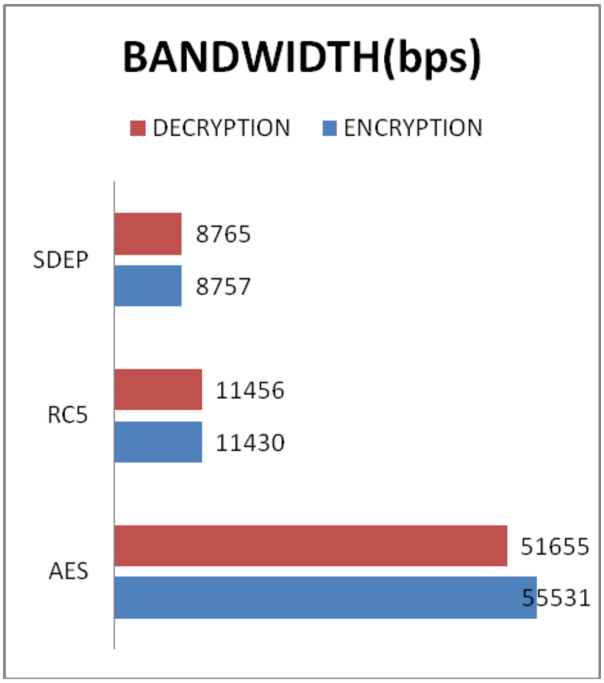


Sensor Network traffic

An Experiment was performed with 15 sources and a simulation time 350s. The maximum packets transmission of the sensor nodes could be achieved in 50 s. the number of packet transfer at that time are 680 in SDEP and 600 in RC5 so the delay time for SDEP is less than RC5 Figure2 show the estimated maximum transmission network packet for the sensor node.







V. Conclusion

This paper proposed a new security scheme for wireless sensor network in which we use the concept of RC6 for encryption and decryption of sensor data. In first modification of RC6 in key expansion step is static number of rotation and in encryption method we perform some function parallel based on RC 5 concept so it increase the throughput of SDEP. In this paper we also compare our new algorithm with AES and RC5 which show that proposed scheme is best useful in end to end encryption in wireless sensor network.

References Références Referencias

1. R. L. Rivest, "The RC5 Encryption Algorithm", in Proc. 1994 LeuvenWorkshop on Fast Software Encryption, 1995, pp. 86.96.
2. C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In SenSys 04: Proceedings of the 2nd international conference on Embedded networked sensor systems, pages 162.175, New York, NY, USA, 2004. ACM Press.
3. B. Kadri, A. Mhamed, and M. Feham "Secured Clustering Algorithm For Mobile Ad Hoc Networks", *International Journal of Computer Science and Network Security*, Vol.7, No.3, pp 27-34.2007.
4. J. Albath, and S. Madria. 'Practical Algorithm for Data Security (PADS) in Wireless Sensor Networks'. *MobiDE'07, , Beijing, China.2007*
5. Koo Woo K, Lee H, Kim Yong H, Lee Dong H (2008). Implementation and Analysis of New Lightweight Cryptographic Algorithm Suitable for Wireless Sensor Networks, Information Security and Assurance, ISA, pp. 73-76.
6. A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar. SPINS: Security Protocols for Sensor Networks, in Wireless Networks Journal (WINE), September 2002.
7. P. Ganesan, R. Venugopalan, P. Peddabachagari, A. Dean, F Mueller, and M Sichitiu, "Analyzing and Modeling Encryption Overhead for Sensor Network Nodes", WSNA"03, September 19, 2003, San Diego, California,USA.
8. *Pawan Kumar Goel* , *Vinit Kumar Sharma* , International Journal of Science Technology & Management , IJSTM Vol. 2, Issue 2, April 2011
9. Sencun Zhu, Sanjeev Setia, Sushil Jajodia. "LEAP: Efficient Security Mechanisms for Large Scale Distributed Sensor Networks", *In The Proceedings of the 10th ACM Conference on Computer and Communications Security*, 2003.
10. S. M. Hwang, and E. N. Huh. 'An Efficient Topology Control and Dynamic Interval Scheduling Scheme for 6LoWPAN', in Gervasi et al. (Eds.): ICCSA, Part I, LNCS 5592, pp. 841–852. 2009
11. Anushiya A Kannan, Guoqiang Mao and Branka Vucetic, "Simulated Annealing based Wireless Sensor Network Localization", *Journal of Computers,* Vol. 1, No. 2, pp 15-22, May 2006.