International Journal of Computer Applications Technology and Research
Volume 2– Issue 1, 63-66, 2013, ISSN: 2319–8656

Data Transfer Security solution for Wireless Sensor Network

Bhavin Patel
Department of Computer Engineering
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.

Neha Pandya
Department of Information and Technology
Parul Institute of Engineering and Technology,
Vadodara, Gujarat, India.

Abstract: WSN is a wide growth area for specific resource limited application. Factor associated with technology like, the encryption security, operating speed and power consumption for network. Here, we introduce a mechanism for secure transferring of data is WSN and various security related issues. This energy-efficient encryption is a secure communication framework in which an algorithm is used to encode the sensed data using like, RC5, AES and CAST Algorithm. The proposed scheme is most suitable for wireless sensor networks that incorporate data centric routing protocols. An algorithm in sensor network is help to designers predict security performance under a set of constraints for WSNs. This symmetric key function is used to guarantee secure communications between in-network nodes and reliable operation cost. RC5 is good on the code point of view, but the key schedule consumes more resource time for efficient security aspects.

Keywords: WSN, security mechanism, encryption, security issues, WSN algorithm.

1. INTRODUCTION

A wireless sensor networks (WSN) are one of the largest growing technology in area of data processing and communication networks today. Wireless sensor networks (WSNs) are based on physically small-sized sensor nodes exchanging mainly environment-related information with each other [2]. The wide application areas of WSN such as wildlife, real-time target tracking, transportation, entertainment, battlefield, building safety monitoring, Agriculture, etc. A WSN consists of a number of wirelessly interconnected sensor nodes that are used to gather information from the environment. In this paper Figure1 represent the model structure of wireless sensor network. The structure network consists of sensor devices which use a single integrated circuit which embeds all the electronic components required. The whole sensor is powered by a small battery which means the network's life is highly dependent on the energy consumption of the sensor. In addition to the sensors the network uses a base station which is the network's interface point to the rest of the world. However, energy consumption still remains one of the main obstacles to the diffusion of this technology, especially in application scenarios where a long network lifetime and a high quality of service are required [1].

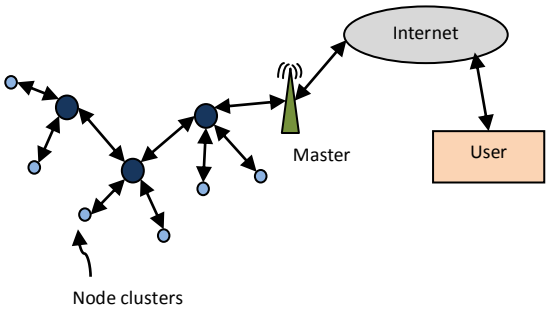

Figure 1. Model structure of WSN System

The major challenges to be addressed in WSNs are coverage and deployment, scalability, quality- of- service, size, computational power, energy efficiency and security [3]. Among these challenges, security is a major issue in wireless sensor networks. Wireless networks are usually more vulnerable to various security threats as the unguided transmission medium is more susceptible to security attacks than those of the guided transmission medium. Secure data transmission over unreliable medium is continuously gaining higher importance. WSN security includes Key management, providing secrecy and authentication; ensure privacy, robustness against communication denial of service attack, secure routing, energy efficiency, and resilience to node capture. It demands improvements in the performance of existing cryptographic algorithms.

Cryptographic algorithms are an essential part of the security architecture of WSNs, using the most efficient and sufficiently secure algorithm is thus an effective means of conserving resources. It is ideal to choose the most efficient cryptographic algorithm in all aspects; operation speed, storage and power consumption [1]. The cryptographic algorithms used in WSNs are generally categories into two parts: symmetric-key algorithms and Asymmetric-key algorithms. In asymmetric public key cryptosystems each node has a public key and a private key. The public key is published, while the private key is kept secret. Asymmetric public key cryptosystems such as the Diffie-Hellman key agreement or RSA signatures are typically too conservative in their security measures, adding too much complexity and protocol overhead to be usable in WSN solutions [2]. Symmetric key cryptographic mechanisms use a single shared key between the two communicating host which is used both for encryption and decryption. Symmetric key algorithms can be further divided into block ciphers for fixed transformations on plain-text data, and stream ciphers for time varying transformations. However, one major challenge for deployment of symmetric key cryptography is how to securely

distribute the shared key between the two communicating hosts. Symmetric key cryptosystems such as the AES, DES, CAST, RC5 algorithm is used in WSN. It is give a comparison for those encryption algorithms at different settings such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/decryption speed. The popular encryption schemes RC5 can be considered as one of the best ciphers in terms of overall performance, when used in nodes with limited memory and processing capabilities.

The rest of the paper is organized as follows. Section 2 provides an overview of security issues & semantics in WSN. Section 3 presents different encryption algorithm schema for WSN. Section 4 provides security mechanism analysis. The paper then concludes in section 5, with insight to future work.

2. SECURITY ISSUES & SEMANTICS OF WSN

A sensor network is a special type of network. The whole network represented using layered architecture to represent its different level security aspect.

2.1 Security requirements

The basic functional security requirement for any WSN application listed as below:

Confidentiality: It refers to limiting information access and disclosure to authorized users. The standard approach for keeping sensitive data secret is to encrypt the data with a secret key that only intended receivers possess, hence achieving confidentiality [1, 3].

Availability: It assures that the services of the system nodes are available to any authorized users as when they require. WSN should have mechanisms to tolerate the interference of malicious nodes. Techniques such as in-network processing, en-route filtering can be used to minimize the impact of unavailability [4].

Integrity: It guarantees that a message being transferred over network is delivered to its destination without any modification. In nature of WSN Integrity handle using MAC code data packet.

Authenticity: Enables a node to safeguard the characteristics of the peer node it is communicating, without which an attacker would duplicate a node, thus attaining unauthorized admission to resource and sensitive information and snooping with operation of other nodes. In WSN data authentication can be achieved through a symmetric mechanism.

Non-repudiation: It ensures that the information originator/ receiver cannot deny of performing its task. Non-repudiation is useful for detection and isolation of compromised nodes.

Robustness and Survivability: The purpose of robustness and survivability in WSN to reduce/recover effect of compromise the node performance. The attack on single node not leads to entire network breakdown.

Self Synchronization: Self- Synchronization is an important requirement for WSN because when point identification is necessary to prevent large scale attacks.

2.2 Attacks scenarios

Any Action that compromises the security of information is called Security Attack. It can be classified into two major categories, namely passive attacks and active attacks. Commonly security attacks are performing over the node of network. The most popular types of attacks are:

Denial of Service Attacks: An attacker jams the communication channel and avoids any member of the network in the affected area to send or receive any packet. A compromised node can send continuous messages to overflow the network and to deplete the life time of other sensor nodes. Another way is exhaustion of power, in which an attacker repeatedly requests packets from sensors to deplete their battery life [5].

Injection attack: An intruder might add a node to the system that feeds false data or prevents the passage of true data [1]. The false message could lead to wrong decision for the whole network. Such messages also consume the scarce energy resources of the nodes.

Protocol- specific Attack: Routing protocol is also one of the vulnerable way in WSN to Spoofed routing information-corruption of the internal control information such as the routing tables, selective forwarding of the packets. Also perform action of forwarding packet to other network.

Wormholes Attack: The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. In this type of attack uses tunneling mechanism to establish malicious node between them by confusing the routing protocol. By spoofing, altering, or replaying routing information, adversaries may be able to create routing loops, attract or repel network traffic, extend or shorten source routes, generate false error messages [1].

The Sybil Attack: In this attack the attacker gets illegally multiple identities on one node [7]. The Sybil attack can significantly reduce the effectiveness of fault-tolerant schemes such as distributed storage and multipath routing. Sybil attacks are generally prevented by validation techniques.

2.3 Constraints related to WSN

Some basic constraints are most commonly affected in the security mechanism for wireless sensor network:

Resource Consumption: WSN has storage, memory and Power limitations. In addition, when implementing a Cryptographic protocol within a sensor the energy impact of Security code must be considered. Energy consumption usually derives from two areas: computational costs and communication costs. Computational cost relates to the cost incurred by calculation of hash functions and primitives while communication cost derives from additional byte transfer among sensor nodes. Usually communication cost is much higher than computational cost.

Network Operability: Certainly, unreliable network is another threat to sensor security. The security of the network relies heavily on a defined protocol, which in turn depends on communication. It can be classified in mainly three fields: Unreliable Transfer, Conflicts, and Latency**.** Normally the packet-based routing of the sensor network is connectionless and thus inherently unreliable. Wireless communication

channel also results in damaged Packets. The multi-hop routing, network congestion and node processing can lead to greater latency in the network, thus making it difficult to achieve synchronization among sensor nodes.

Node reliability/ freshness: Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time. Its lead to exposure of physical attacks mainly of environment causes. Remote management of a sensor network makes it virtually impossible to detect physical tampering and physical maintenance issues [4]. If designed incorrectly, it will make the network organization difficult, inefficient, and fragile.

3. ENCRYPTION ALGORITHM SCHEMA FOR WSN

In this section, we provide an overview of three symmetric key cryptographic algorithms like. AES Algorithm, RC5 Algorithm and CAST Algorithm.

3.1 RC5 Algorithm

RC5 is suitable for resource-constrained sensor nodes for the following reasons [2]. RC5 is a fast symmetric block cipher with a two-word input block size plaintext and output block cipher text. The RC5 encryption algorithm is used in different modes like. Counter, feedback. RC5 is a block cipher with variable parameters: block size (32bits, 64 bits, and 128 bits), key size and encryption rounds, and it can be expressed as RC5-w/r/b [1]. The general operation performed by RC5 algorithm such as modular addition, XOR, and cyclic shift. The rotation operations depend on both the key and the data. The different combinations of values for these parameters are used to fully understand their influence on the energy consumption caused by the encryption algorithm. In normal way 18-20 round operation is enough to provide data encryption in WSN. RC5 uses an "expandable key table", S, that is derived from the secret key K and the size t of Table S also depends on Nr, with S has $t = 2(Nr + 1)$. RC5 does not rely on multiplication and does not require large tables. Hence, RC5 block cipher offers a computationally inexpensive way of providing secure encryption. The advantage of RC5 encryption schema in WSN is: high speed implementation, simplicity, arbitrary message length and a low rate of error propagation.

3.2 CAST Algorithm

The CAST encryption algorithm is one type of symmetric key base encryption schema for WSN. It was developed by Stafford Tavares and Carlisle Adams. Mainly two types of CAST schema consider like, CAST-128 and CAST-256. CAST-128 is a12- or 16-round Feistel network with a 64-bit block size and a key size of between 40 to 128 bits [cast]. In this approach symmetric key always perform composition with substitution boxes (s) related to fewer bits. CAST-256 was derived from CAST-128. It is a 48-round Feistel network with a 128-bit block size and acceptable key sizes are 128, 160, 192, 224 or 256 bits [3]. The strength of the algorithm lies in its S-boxes. CAST does not have fixed S-boxes while new S-boxes are constructed for each application. Round function of the CAST algorithm performs faster. So it is more suitable for wireless network application which exchanges small size packets.

3.3 AES Algorithm

The Advanced Encryption Standard (AES) algorithm, also known as Rijndael, is a block cipher in which both the sender and the receiver use a single key for encryption and decryption. The data block length is fixed to be 128 bits with 4 x 4 array, while the key length can be 128, 192, or 256 bits and the number of rounds Nr is 10, 12 or 14 respectively[5]. The mail goal of this AES algorithm performed based on substitution- permutation of data block. In the encryption of the AES algorithm, each round except the final round consists of four iterative transformations: the Sub Bytes, the Shift Rows, the Mix-Columns, and the Add Round Keys, while the final round does not have the Mix Columns transformation. It is composed mainly of nonlinear components, linear components, and round keys, and though it employs an iterative structure, is does not have a Feistel network structure but an SP structure instead [1]. AES is fast in both software and hardware and is relatively easy to implement.

4. SECURITY MECHANISM ANALYSIS

Evolution of different symmetric key cryptographic algorithm based on following criteria:

4.1 Energy efficiency/consumption

Energy is the asset that has to be paid to obtain security. It is therefore generally accepted that a security mechanism will be less efficient and slower than a plain one. The energy consumed by a processor during the execution of a piece of software, such as a block cipher, corresponds to the product of the average power dissipation and the total running time. The power consumption of sensor network given each cryptographic algorithm AES, RC5 and CAST is executed on Mica2 mote of sensor node. The energy consumptions show that source node using RC5 saves about 72% of the energy Consumed by the hybrid scheme and 82% of the energy consumed ECC. Also for the CAST and AES algorithm the ratio of power consumption is about 67% and 78% respectively. The computational complexity of an algorithm translates directly to its energy consumption.

4.2 Operation time-speed

The data transfer time from sensor nodes to cluster head is computed below by including the data transmission time only for in case of the conventional data aggregation algorithm. Encryption speed is used to measure the throughput per unit time of an encryption scheme [3]. The encryption speed is calculated as the total plaintext in bytes divided by the encryption time and also calculates key setup time and decryption time for data value. For all three algorithms CAST, AES-128 and RC5 the encryption time is about 38%, 43%, and 40% of the decryption time. Encrypting data arrays handle operation speed of different size up to 8192 byte with RC5/AES.

4.3 Security strength

Security strength is referred differential cryptanalysis and linear cryptanalysis approach for the security mechanism implementation to handle bit wise operation of the key with data. The bits rotation for each random position in round of RC5 involves data dependent rotations which may help frustrate differential cryptanalysis and linear cryptanalysis since bits are rotated to random positions in each round [6].

The RC5 block cipher has built-in parameter variability that provides flexibility at all levels of security and efficiency. Also for the other symmetric key algorithm CAST and AES-128,256 the strength of security increase with no. of round is increased. The RC5 is better than DES in security strength and implementation efficiency.

4.4 Performance overhead

The measurement criteria for performance overhead consists of energy overhead, communication overhead, computational overhead and Memory space. Major performance overhead generates from the key setup operation, encryption operation and decryption. The initialization overheads are significant for all encryption algorithms like RC5, CAST and AES especially for small plaintexts. Thus they are suitable for large data size. RC5 requires that a pre-computed key schedule to be stored in memory taking up significant bytes memory for each key. RC5 is faster compared to AES-Rijndael and therefore more energy-efficient under memory constraints for both encryption and decryption, but it suffers from a relatively costly key expansion [6]. The group size, secret-key length, and the number of iterations of RC5, which can be used flexibly in systems with different resource configurations.

5. CONCLUSION & FUTURE WORK

In this paper we have describe the different security encryption mechanism for Wireless sensor network. Encryption algorithm plays a crucial role for information security due to various approach of resource constrains. Paper presented a systematic model of cryptographic algorithms complexity and in particular analyzed the suitability of RC5, CAST and AES encryption techniques to provide efficient link layer security. It provides one of the major security services namely confidentiality by the help of RC5 Encryption scheme which is based on the permutation codes on the blocks of data. One future research is to explore dynamic key assign cryptographic mechanisms to optimize energy consumption by varying cipher parameters using strong primitive arithmetic operation in WSN.

6. REFERENCES

[1] Soufiene Ben Othman, Abdelbasset Trad, Habib Youssef, "Performance Evaluation of Encryption Algorithm for Wireless Sensor Networks" International Conference on Information Technology and e-Services, 2012.

[2] Juha Kukkurainen, Mikael Soini, Lauri Sydanheimo, "RC5-Based Security in Wireless Sensor Networks: Utilization and Performance" WSEAS TRANSACTIONS on COMPUTERS, ISSN: 1109-2750, Issue 10, Volume 9, October 2010.

[3] Tingyuan Nie, Yansheng Li, Chuanwang Song, "Performance Evaluation of CAST and RC5 Encryption Algorithms" International Conference on Computing, Control and Industrial Engineering, year-2010.

[4] Abu Shohel Ahmed, "An Evaluation of Security Protocols on Wireless Sensor Network" TKK T-110.5190 Seminar on Internetworking, 2009.

[5] S.Prasanna, Srinivasa Rao, "An Overview of Wireless Sensor Networks Applications and Security" International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-2, May 2012.

[6] Dhanashri H. Gawali, Vijay M. Wadhai, "RC5 ALGORITHM: POTENTIAL CIPHER SOLUTION FOR SECURITY IN WBSN" International Journal of Advanced Smart Sensor Network Systems (IJASSN), Volume 2, No.3, July 2012.

[7] Abhishek Pandey, R.C. Tripathi, "A Survey on Wireless Sensor Networks Security" International Journal of Computer Applications (0975 – 8887) Volume 3 – No.2, June 2010.