Wireless Data Encryption over RF (Radio Frequency) Signals

Introduction

Friendly fire is the act of a military force mistakenly attacking their own forces. Over the years there have been thousands of friendly fire casualties at war [1]. As a remedy for these friendly fire casualties, the development of infantry IFF (Identification Friend or Foe) systems have been attempted to work much like the IFF transponder systems currently utilized on fighter aircrafts and military vehicles [9]. The success of any IFF system is heavily dependent on highly efficient and secure data encryption and decryption over transmitted RF signals. This technical review summarizes commercial applications of wireless data encryption, explains the functionality and advances of the technology, and describes methods for its implementation.

Commercial Applications of Data Encryption

With data security becoming a paramount issue with the growth of IOT (Internet of Things) and Big Data, data encryption and cryptography are a necessity, especially in the protection of confidential military information. There are several commercially used encryption algorithms available, each with its set of advantages and drawbacks, that have been compared based on a set of metrics that include encryption time (desired low), decryption time (desired low), memory usage (desired low), avalanche effect (desired high), entropy (desired high) and the number of bits required for encoding (desired low as it affects cost) [3]. Among these algorithms are DES, 3DES, AES, RSA, and Blowfish with DES, 3DES, AES and Blowfish being symmetric key cryptographic calculations (the same key is used for encryption and decryption [4]), and RSA being a public key cryptographic calculation (a public key is used for an encryption and a secret key is used for decryption [4]) [2].

From a study published on August 10th, 2018 (see [3]), irrespective of file size, Blowfish provides by far the quickest encryption time (≈100 ms for a file size of 25KB and ≈1000ms for a file size of 3MB) whereas RSA consistently provides the slowest encryption time (≈500 ms for a file size of 25KB and ≈2250ms for a file size of 3MB) [3]. Blowfish also has the fastest decryption speed regardless of file size while RSA provides the slowest average decryption speed. AES, 3DES, and DES are respectively second, third and fourth in encryption and decryption speeds [3,5].

In comparing memory usage, Blowfish (using 9.38KB storage) also utilizes the least memory space when compared to AES (14.7KB), DES (18.2KB), 3DES (20.7), and RSA (31.5KB) [3,5]. In the comparison of avalanche effect, a very desirable property that reflects the performance of a cryptographic algorithm, AES rates the highest, followed by DES, 3DES, Blowfish and then RSA. In an application where security and data integrity are of great importance AES would without doubt be the primary option due to its avalanche effect [5]. AES and Blowfish both rank highly in average entropy per byte of

encryption as well (3.84024 and 3.93891 respectively compared to 2.9477 for DES, 2.9477 for 3DES, and 3.0958 for RSA).

After a comparison of the first five metrics, Blowfish would seem to be the best choice for any industry if speed and memory space was the primary concern, and AES would seem to be the best choice from a performance standpoint, however, the reason DES, 3DES, and RSA are still commercially relevant is due to their very low number of bits required for their encryption algorithm (27, 40 and 44 bits for DES, 3DES and RSA respectively while Blowfish and AES require 128 and 256 bits respectively) [5]. The comparatively low number of bits required for the performance of DES, 3DES and RSA make these algorithms a very cost-effective alternative to AES and Blowfish.

Organizations often select different encryption algorithms based on their varying needs and limitations when investing in data security. For example, multiple e-commerce platforms utilize Blowfish for its low latency, whereas standard internet data transfer protocols utilize RSA for its minimal architectural requirements. AES specifically is an algorithm trusted by the US government and other entities requiring high priority data protection due to its high avalanche effect.

How Do Data Encryption and RF Data Encryption Work?

There are two main categories of data encryption methods as mentioned above: symmetric and asymmetric. When a larger volume of data is needed to be encrypted, a symmetric encryption is used where the only way to decrypt a ciphertext (encrypted text) is to use the same key that initiated the encryption. The goal of encryption is to create a ciphertext complicated enough that the only means of decryption by a threat would be to manually try every possible key combination [6]. This kind of strategy used by attackers is called a Brute Force approach. Other forms of security attacks include dictionary attacks (a weakness to Blowfish), side channel attacks (a weakness to AES), and public key factorings (a weakness to RSA) [7].

For basic data encryption across a radio, the implementation would be to use simple cryptography algorithms for encoding signal frequencies. By frequently scrambling and inverting radio frequencies at irregular rates, RF signals can be encrypted and decrypted with a symmetric encryption technique [8]. Of course, more sophisticated alternatives exist as was discussed in the section above, but these are costlier. One such algorithm, DES, was largely used in the FBI and Military after its development in the 1970's however it has since been improved to the new Advanced Encryption Standard (AES) which is widely used [8].

Encryption keys for the algorithms stated above require a "Key Variable Loader" (KVL). The KVL is what allows the primary user to pass an encryption key within a specific radio device. A "Key Management Controller (KMC) is also vital to manage the constantly changing encryptions. Another

factor to consider when utilizing data encryption for radio frequencies is the system compatibility of encryption methods between different brands of radios, however AES was designed to be a standardized method and therefore would be compatible between otherwise incompatible radios [8].

Implementation of Data Encryption in an IFF System

For an IFF system to work at a basic level, two devices (weapons or body armor) would need to communicate via radio frequency signals. The first device would transmit an IFF query that would then be received and sent back to the host device. For practical usage however, this signal would have to be heavily encrypted to ensure safety. Ideally sophisticated encryption methods such as AES would be the best candidates for an infantry IFF system, however utilizing simple encryption methods such as signal scrambling and inversion would be viable and cost effective for a proof of concept.

A 2018 study further explored utilizing AES to perform secure RF communication by testing the performance of encryption of three different types of data (plaintext, ciphertext, and ciphertext with padding over RF) [10]. It was found that the padded ciphertext outperformed the unpadded text in transmission time by 7.92%, however was ultimately slower than plaintext transmission time (which makes sense since plaintext is not encrypted). What this study shows is that although transmission time over RF is increased with encryption, there are methods of reducing transmission delay (padding for example). This would be of great importance to implement in an IFF system for a signal exchange to be performed both swiftly and securely.

Sources

[1] Mark Thompson, "The Curse of 'Friendly Fire'", Time Magazine, Jun. 11, 2014. [Online]. Available: http://time.com/2854306/the-curse-of-friendly-fire/. [Accessed Mar. 4, 2019]

[2] Shin Woo Jang, "Comparative Analysis of AES, Blowfish, Twofish and Threefish Encryption Algorithms," Journal of Analysis of Applied Mathematics, vol. 10, no. 1–24, 2017.

[3] Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD (2018) A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. J Comp Sci Appl Inform Technol. 3(2): 1-7.

[4] Dr. Bill Young. Foundations of Computer Security. Class Lecture 44, Topic: "Symmetric vs Asymmetric Encryption." Department of Computer Sciences, University of Texas at Austin, Austin, Texas. Available: https://www.cs.utexas.edu/users/byoung/cs361/lecture44.pdf. [Accessed Mar. 4, 2019]

[5] Priyadarshini P, Prashant N, Narayan DG, Meena SM. A Comprehensive Evaluation of Cryptographic Algorithms: DES, 3DES, AES, RSA, and Blowfish. Procedia Computer Science. 2016;78:617-624

[6] "Cryptography", May 30, 2018. [Online]. Available: https://docs.microsoft.com/en-us/windows/desktop/seccrypto/data-encryption-and-decryption. [Accessed Mar. 5, 2019].

[7] Zoran Hercigonja, "Comparative Analysis of Cryptographic Algorithms", International Journal of Digital Technology & Economy, vol. 1, no. 2, 2016.

[8] "How Does Radio Encryption Work", Quality Two-Way Radios, Encryption Basics. [Online]. Available: https://quality2wayradios.com/store/Encryption-Basics-Help.

[9] "Identification Friend or Foe (IFF) Crypto Systems", General Dynamics Mission Systems. [Online]. Available: https://gdmissionsystems.com/en/encryption/embedded-encryption/identification-friend-or-foe-crypto-systems. [Accessed Mar. 6, 2019]

[10] Mohamed, N.N. & Hashim, Habibah. (2018). Securing RF Communication Using AES-256 Symmetric Encryption: A Performance Evaluation. International Journal of Engineering and Technology. 7. 217-222. 10.14419/ijet.v7i4.11.20810.