Light Weight Secure Encryption Scheme for Internet of Things Network

Security of transmitted information is a major area of concern in Internet of Things (IoT) networks especially with large number of dynamically connected devices. One of the major challenges is to design an efficient encryption and decryption mechanism for securely transmitting the data between the devices in the network. Tiny Encryption Algorithm (TEA) is the most attractive encryption technique among all, with its less memory utilization and ease of implementation in both hardware and software scales. But one of the major issues of TEA and its numerous developed versions is the usage of the same key through all rounds of encryption, which yields a reduced security evident from the avalanche effect of the algorithm. This article discusses the working of a novel encryption scheme termed as Tiny Symmetric Encryption Algorithm (NTSA) which provides enhanced security for the transfer of text files through the IoT network by introducing additional key confusions dynamically for each round of encryption. Experiments are carried out to analyze the avalanche effect, encryption and decryption time of NTSA in an IoT network with embedded devices. The proposed scheme is found to have better performance compared to all the existing techniques.

1. Introduction

Internet of Things (IoT) includes millions of connected devices that can sense, compute and communicate data. Every second, large amount of data is transferred among these devices. Considering the sensitivity of applications in IoT network such as connected vehicles or wearable health devices, security of transmitted information has remained a major area of concern. Over these years, numerous cryptographic algorithms have been used to ensure the security of transmitted data. With numerous IoT devices having different computational capabilities, one of the major requirements for an efficient security protocol in IoT network is that it should be light weight. The processing time taken by the protocol should be minimal for less delay and better performance. Also the security algorithm needs to be less complex with minimal overhead. Because of these reasons many protocols used with normal computer networks does not give good performance in IoT networks and are not preferred. Considering these features, Tiny Encryption Algorithm (TEA) is the most widely used symmetric algorithm with Feistel cipher for secure transmission of data through the IoT network. The popularity of TEA is mainly due to the ease of implementation and less memory utilization compared to all other encryption algorithms. But one of the major issues with TEA is the usage of same keys through all the rounds of encryption which leads to reduced security. This is undoubtedly observed from the avalanche effect of TEA. Moreover, the time taken for encryption and decryption is high, leading to reduced efficiency of TEA. Although many versions of TEA have been proposed over these years, none of them have given concrete solutions to the above problems.

This article proposes an algorithm named NTSA (Novel-T Symmetric Algorithm) that improves the security features of TEA by introducing more key confusions. Most of the works with TEA and its variations has focused only on decreasing the delay in delivery. Very few researches have been done on key alteration as a method to enhance the security of the transmission algorithm. In the proposed method we introduce multiple key alterations dynamically and secure the key from intruders. Since the key is computed dynamically, the key values are changed during the execution time and cannot be pre-computed. Furthermore, our proposed algorithm (NTSA) takes less time for encryption and decryption compared to TEA and thus provides both better security and efficiency for all the modern applications in IoT networks. In our next work we will discuss how the method can be integrated to ad hoc, sensor and underwater networks.

2. Novel Tiny Symmetric Encryption Algorithm (NTSA)

The TEA algorithm and its variations use the same key in all rounds of encryption and thus more prone to relative key attack where the attacker tries to realize some relationship between different keys used by the user. The proposed NTSA algorithm is intended to provide more confusion to the keys in each round dynamically. It uses 64-bit plaintext and key of 128 bits. There are 32 cycles and each cycle is composed of 2 rounds resulting in 64 Rounds. The plaintext is divided into two halves v0 and v1 with 32 bits each. The round function op is applied to each half of plaintext. The 128-bit key is divided into 4, 32 bit partial keys k1, k2, k3 and k4. Partial keys k1 and k3 are applied to the odd numbered round and
partial keys k2 and k4 are applied to even numbered round. Compute key schedule constant \( k_{sc} = \text{floor} \left( \frac{2^{31}}{\phi} \right) \) where \( \phi \) is the golden ratio. The golden ratio \( \phi \) is 1.618033988749895 and computed as \( \frac{(1+\sqrt{5})}{2} \).

NTSA round function is as follows

**Round \( r \) (\( i \) is odd)**

\[
v_0 += ((v_1 \text{ LSHIFT} 4) \text{ AND } k_0) \text{ XOR } (v_1 \text{ AND } k_c) \text{ XOR } ((v_1 \text{ RSHIFT} 5) \text{ AND } k_1)
\]

**Round \( r \) (\( i \) is even)**

\[
v_1 += ((v_0 \text{ LSHIFT} 4) \text{ AND } k_2) \text{ XOR } (v_0 \text{ AND } k_c) \text{ XOR } ((v_0 \text{ RSHIFT} 5) \text{ AND } k_3)
\]

**For 1st cycle:** the partial keys are k0, k1, k2 and k3.

**From 2nd cycle onwards**

For odd round k0 is kept constant but k1 changes for all odd rounds as follows,

\[
k_1 = k_1 + (k_0 \text{ XOR}(\text{xtract}(v_0)))
\]

For even round k2 is kept constant but k3 changes for all even rounds as follows,

\[
k_3 = k_3 + (k_2 \text{ XOR}(\text{xtract}(v_1)))
\]

The function \( \text{xtract}() \) will compute an integer in the range 0 to 32 from v0 or v1 depending upon the parameter being passed. This integer value is an index to an array that is generated dynamically based on the key value selection. The \( \text{xtract}() \) function will return the value from the array that is pointed by the index value computed. Thus the key confusion is created dynamically and cannot be predicted prior to execution and the value changes on each execution of the algorithm. The NTSA Encryption and Decryption Model is shown in Figure 1.
References

1. Pawani Porambage; Jude Okwuibe; Madhusanka Liyanage; Mika Ylianttila; Tarik Taleb; Survey on Multi-Access Edge Computing for Internet of Things Realization. *IEEE Communications Surveys & Tutorials 2018*, 20, 2961-2991, 10.1109/comst.2018.2849509.

2. P.G Vinoj, Sunil Jacob, and V. G. Menon; Hybrid brainactuated muscle interface for the physically disabled. *Basic & Clinical Pharmacology & Toxicology 2018*, 123, 8-9, 10.1111/bcpl.13100.

3. Neha Sharma; Madhavi Shamkuwar; Inderjit Singh; The History, Present and Future with IoT. *Combinatorial Optimization 2018*, 154, 27-51, 10.1007/978-3-030-04203-5_3.

4. Borja Bordel; Ramon Alcarria; Diego Martin De Andres; IIISun You; Diego Martin; Securing Internet-of-Things Systems Through Implicit and Explicit Reputation Models. *IEEE Access 2018*, 6, 47472-47488, 10.1109/access.2018.2866185.

5. Varun G. Menon; Joe Prathap; Vehicular Fog Computing. *International Journal of Vehicular Telematics and Infotainment Systems 2017*, 1, 15-23, 10.4018/ijvts.2017070102.

6. David J. Wheeler; Roger M. Needham; TEA, a tiny encryption algorithm. *Algorithms and Discrete Applied Mathematics 1995*, 1008, 363-366, 10.1007/3-540-60590-8_29.

7. Simon J. Shepherd; The Tiny Encryption Algorithm. *Cryptologia 2007*, 31, 233-245, 10.1080/01611190601090606.

8. I. Sima; D. Tarmurean; Victor Greu; A. Diaconu; XXTEA, an alternative replacement of KASUMI cipher algorithm in A5/3 GSM and f8, f9 UMTS data security functions. *2012 9th International Conference on Communications (COMM) 2012*, 1, 323-326, 10.1109/iccomm.2012.6262617.

9. Menon, V. Optimized Opportunistic Routing in Highly Dynamic Ad hoc Networks. Preprints 2019, 2019020130

10. Menon, Varun G., and Joe Prathap. "Analyzing the behavior and performance of opportunistic routing protocols in highly mobile wireless ad hoc networks." International Journal of Engineering and Technology 8.5 (2016): 1916-1924.

11. Varun G. Menon; P. M. Joe Prathap; Opportunistic Routing with Virtual Coordinates to Handle Communication Voids in Mobile Ad hoc Networks. *Advances in Intelligent Systems and Computing 2015*, 425, 323-334, 10.1007/978-3-319-28658-7_28.

12. Varun G. Menon; P. M. Joe Prathap; Comparative analysis of opportunistic routing protocols for underwater acoustic sensor networks. *2016 International Conference on Emerging Technological Trends (ICETT) 2016*, 1, 1-5, 10.1109/icett.2016.7873733.

Keywords

avalanche effect;efficiency;encryption time;key confusions;NTSA;symmetric encryption;Tiny Encryption Algorithm