Indonesian Journal of Electrical Engineering and Computer Science
Vol. 15, No. 1, July 2019, pp. 421~426
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v15.i1.pp421-426

Robust authenticated encryption scheme with multiple keys for ad hoc networks

Ajay Kakkar[1], Maninder Singh[2]
[1]Department of Electronics and Communication Engineering, T.I.E.T, India
[2]Department of Electronics and Communication Engineering, R.B.U, India

Article Info

Article history:

Received Dec 13, 2018
Revised Feb 14, 2019
Accepted Feb 28, 2019

Keywords:

Ad hoc network
Encryption
Hacking time
Keys

ABSTRACT

Data security in a computing dynamic infrastructure without explicit user intervention is tough to achieve. A robust authenticated encryption scheme with multiple keys for ad hoc networks has been proposed. Real time attacks has been monitored and coped up using re-encryption algorithm. The effectiveness of the work has been validated by extensive simulations on various combination in terms of S-Boxes, key and data length. The proposed work is a collaboration of optimal selection of S-Boxes, key and data lengths with evaluation of heat dissipation. The work has been carried out to develop an optimized efficient key management technique to reduce the time available for hackers. To verify the effectiveness of proposed algorithm, the results have been compared with K. Xue et al., Li X. et al. and S. K. Sood et al.'s protocol.

Corresponding Author:

Ajay Kakkar,
Department of Electronics and Communication Engineering,
T.I.E.T,
Patiala, Punjab, India.
Email: ajay.kakkar@thapar.edu

1. INTRODUCTION

Everyone needs privacy and wants online secured transmission. As the information is frequently shared over the web; therefore, there is an urgent need to meet the security and privacy issues of an individual/organizations [1-2]. The existing schemes are either vulnerable to random attackes or suuffered from siginficiant overheads. The main objective of this work is to improve the safety of data and to preserve the information it contain with minimum overheads. Data encryption with multiple keys have the potential to provide effective and secured transmission [3-5]. The multiple keys with variable lengths have always been preferred over fixed key lengths. Hence, real time adaptively for reliable keys with the focus to provide secured data communication to users is possible. The use of a heavy cryptographic software in itself is a biggest challenge due to the heat dissipated by the algorithm. Therefore, in the ad hoc networks the reduction in bit length and nodes always advisable [6-7]. It improves the performance of cryptographic model, and reduce computational complexity while fulfilling security necessities of a cryptographic technique [8].To prevent illicit access of data and increase the system performance, the concept of re-encryption can be used [9-10]. The work has been segregated in two parts; a) Pre-estimation of processing time (ns) and hacking time (minutes) for ad hoc network, and b) heat dissipation due to algorithm has also been reported. This paper presents a path to the researchers that explore state-of-the-art elaboration associated with the encryption.

The analysis of key length in the encryption process was carried out by M. Naor et al. (1999) [11], H. Chien (2004) [12], J. Cao et al. (2006) [13], Y. Tseng (2007) [14] and A. Kakkar et. al. (2010, 2011) [15-16]. It has been observed that many security schemes designed for homogeneous sensor networks suffer from high communication and computation overhead, and these are not suitable for ad hoc networks. Therefore, the selection of keys and S-Boxes has to be done in accordance with the data sequence to reduce

the hacking time. R. Amin et. al. (2016) [17], M. AlSabah et. al. (2017) [18], K. Xue et. al. (2013) [19] and A. Kakkar et. al. (2012) [20] worked on secured time bound hierarchical key assignment schemes in order to assign time dependent encryption keys. For efficient and reliable model, the keys are generated from the available data. Key recovery mechanisms is used to cope up the key failure problem. Secured data transmission involved encryption, re-encryption, transmission and routing of data across various nodes. The issue of key distribution and efficient group key management in such networks were also analyzed. A secure data collection scheme based on compressive sensing in ad hoc networks was also analyzed. Florian Skopik et. al. (2016) and J. Li et. al. (2018) [21-22] worked on certificateless cryptography and key transparency techniques to avoid key escrow problem. The group key agreement protocols were utilized to provide data security in ad hoc networks. The main flaw of their scheme was that for each independent resource the unique key was required for encrypting the data. Z. Ali et. al. (2013) proposed a new computation of encryption that was based upon symmetric cipher and had a very weak key design method; therefore, security level of the algorithm was very poor as compared to other encryption algorithms. The key used was time bounded which decreased the security level and did not provide the flexibility to the users to upgrade the private key [23]. The various security aspects of threats, vulnerabilities and encryption, and information attack side concerned with encryption algorithm was also considered.

2. RESEARCH METHOD

Keys are generated from the available data to avoid key transportation. It improves the bandwidth and performance of the model which enhances the data rate. Risk and security level against random attacks has been shown in Table1. Based on the attacks/minute the re-encryption is done. If the attacks in a given slot are further increased, the key shifting time should be reduced to achieve secured model. The analysis shows that the failure rate plays a vital role in reducing the time available to the hackers. The security level of a cryptographic model was evaluated from the key strength. When the failure rate of key increased from a fixed value, then it was treated as faulty key and was discarded from the system. The fresh keys are generated from the new data sequence. Therefore, these are independent from the previous keys. The process of generation, modification and transportation of keys is carried out by algorithm. The use of reliable keys in the algorithm makes it impossible for a hacker to get access of node which is being protected by multiple keys. It allows user to select and replace their keys without affecting the other keys. The removal of key from the faulty node, removal of key, when users enter/leave the group and key updating mechanism are also addressed. The keys were withdrawn from the users by the system when they leave the network. It is a trade-off between security and overheads. It also help in achieving confidentiality, authentication and integrity of data. Various security levels are proposed for attacks and the recovery mechanism is selected on the basis of these security levels.

Table 1. Evaluation of Risk and Security Level

S. No	Risk Level	Attacks/Minute	Security Level	Remarks
1	Low	0-20	Very Good	Used for long sequences
2	Medium	21-100	Good	Used for short sequences
3	Average	101-200	Average	Use multiple keys of variable length.
4	High	201-500	Weak	Re-encryption of at least single key is required
5	Very High	> 500	Very weak	Re-encryption both the keys is required.

The re-encryption has been done using 2nd key for weak nodes. The 2nd key is required whenever there is a node failure due to random attacks. Both the keys have been generated from different pools enhance the security level. The probability of hacking an alphanumeric keys if generated from the same pool is:

$$P_i = \sum_{i=0}^{35} (M - 1/36)^2 \quad (1)$$

When both keys are generated from same pool and have at least one similar character, the (1) is written as:

$$\sum_{i=0}^{35} (M)^2 = 1$$

hence the probability of hacking is

$$P_i = \sum_{i=0}^{35} (M)^2 - 0.084 \quad (2)$$

It is evident that the security level falls whenever same pool is used for multiple keys. The keys are based upon the mathematical functions; for n number of bits (0/1) key length the possible combinations are 2^n.

3. RESULTS AND ANALYSIS

Eight S-Boxes have been used for encryption with multiple keys of fixed length 8 and 16 bits. The scheme has been applied on the ad hoc network where 10 nodes are considered. The algorithm has been run for 16, 32, 64, 128 and 512 bit data bits separately. Initially, first key is selected which has short key length in comparison to second key.

3.1. Multiple Keys of Fixed Length

It has been observed that when the encryption of short data sequence 16 is done using two keys having key length 8 and 16 bits respectively, the processing time of 17.15ns and 14.32 minute of hacking time is resulted. 2677μW heat will be dissipated. The overall response of the system remains good for a period of 14.32 minutes. It means the security level of the model will degrade after 14.32 minutes. The security level also tends to fall if the data length increase 16 to 32 bits. For the same configuration of data length is increased from 16 to 32 bits, the hacking time will increase from 14.32 to 21.52 minutes which is marginally acceptable. The processing time and heat dissipation also increases which will further ruin the cryptographic model. The system response in terms of processing, hacking time and heat dissipation for various data and key lengths have been shown in Table 2. Evaluation of risk and security level against attacks when 1st key is larger compared to 2nd key as shown in Figure 3.

Table 2. Evaluation of Risk and Security Level Against Attacks when 1st Key is Small Compared to 2nd Key

Data Length (Bits)	1st key = 8 bits, 2nd key = 16 bits			
	Processing time (ns)	Hacking Time (min)	Heat Dissipation (μW)	Remarks
16	17.15	14.32	2677	Accept
32	21.18	21.52	2704	Marginally Acceptable
64	49.57	24.65	2757	Reject
128	57.64	35.80	2792	Reject
512	87.15	39.63	2801	Reject

Table 3. Evaluation of Risk and Security Level Against Attacks when 1st Key is Larger Compared to 2nd Key

Data Length (Bits)	1st key = 16 bits, 2nd key = 8 bits			
	Processing time (ns)	Hacking Time (min)	Heat Dissipation (μW)	Remarks
16	24.19	12.41	2705	Accept
32	47.25	15.14	2761	Accept
64	54.95	19.12	2794	Marginally Acceptable
128	64.56	24.06	2816	Reject
512	95.02	36.12	2886	Reject

It has been observed from the Table 2 that whenever the bit length of first key is small in comparison to second key, the hacker has more time to generate the attacks. As the data bits are increased the heat dissipation and hacking time increases. Therefore, it is always worthy to have first key of higher length in comparison to second key. Using this combination the hacking time is reduced but the a small increase in heat dissipation has been observed.

3.2. Multiple Keys of Variable Length

Multiple keys are the effective solution for key replacement in case of faulty key. Table 3 shows that the single key of variable length does not offer a secured cryptographic model. Therefore, multiple keys of variable length are used to achieve data security. If multiple keys of variable length are used to encrypt the 64 bit data sequence, the hacking time has been reduced 10.84 minutes from 24.65 minutes which is observed encryption is done using two fixed key length 8 and 16 bits respectively. If the key lengths are interchanged

i.e. 16 and 8 bits respectively for first and second key, the hacking time 19.12 minutes has been observed. Evaluation of heat dissipation, processing and hacking time for two keys of variable length as shown in Table 4.

Table 4. Evaluation of Heat Dissipation, Processing and Hacking Time for Two Keys of Variable Length

Keys	Data Length (Bits)	Processing time (ns)	Hacking Time (min)	Heat Dissipation (µW)	Remarks
Single Key Length (8-16 Bits)	16	11.21	64.02	2216	Reject
	32	14.47	72.26	2329	Reject
	64	19.44	84.49	2344	Reject
	128	21.56	89.09	2359	Reject
	512	28.68	96.54	2963	Reject
Two Keys of Length (8-16 Bits)	16	34.16	09.09	3023	Accept
	32	38.19	09.23	3125	Accept
	64	42.08	10.84	3227	Accept
	128	47.92	10.96	3256	Accept
	512	50.02	11.01	3275	Accept

The comparison for the processing, hacking time, heat dissipation and data lengths for fixed and variable key lengths have been shown in Figures 1, 2 and 3. It has been found that the heat dissipation and hacking time increases as the input data stream increases.

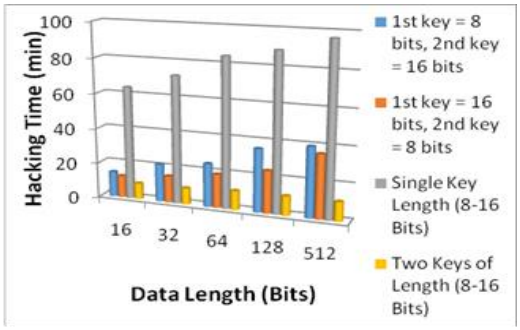

Figure 1. Evaluation of hacking time (minutes) for fixed and variable key lengths

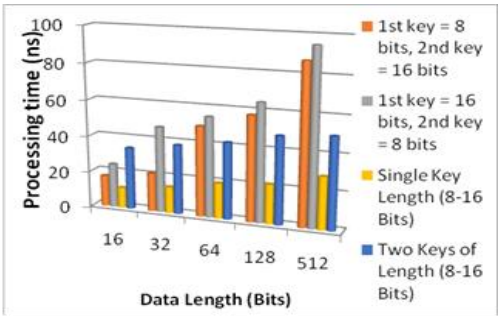

Figure 2. Evaluation of heat dissipation (µW)for fixed and variable key lengths

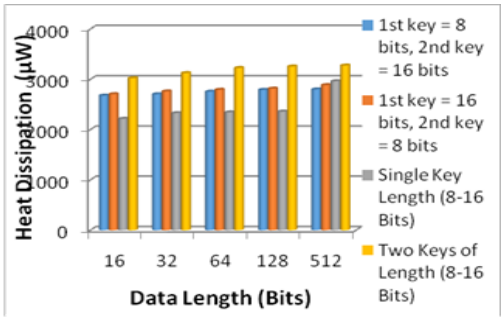

Figure 3. Evaluation of heat dissipation (µW) for fixed and variable key lengths

To keep the model secured from hacker the higher data length sequences have to be encrypted using multiple keys of variable length (8-16), otherwise the hacker gets ample time to hack the crucial information. This exercise will affect the heat other parameters such as heat dissipation and cost, but the increase in heat dissipation is not so much high thus can be ignored. However, the correct combination of data and key length can be selected based on the impact of application using Table 1 to 4. The aim is to encrypt the data with minimum number of overheads and provide high security level. It improves the computational performance

and reduced the implementation cost of the cryptographic model.

The proposed model has been compared with K. Xue et al. (2013) [9], Li et al. (2011) [24] and S. K. Sood et al.'s protocol (2011) [25] on the basis of different parameters and shown in Table 5. It offers low computational complexity and is more robust to random attacks.

Table 5. Comparison of Proposed Model with Existing Models

Parameters	Proposed	K. Xue et al.	Li et al.'s	Sood et al.'s
Key type/length (bits)	Variable (8-16)	Fixed (56)	Fixed (56)	Fixed (56)
Re-encryption	Yes	No	No	No
Resistance to attacks	Yes	Yes	No	No

4. CONCLUSION

A comparison of fixed and variable key length has been done by considering S-Boxes, nodes and heat dissipation. It has been found that the use of single key of fixed/variable length (8-16 bits) is not worthy for encryption of data (16-512 bits). The multiple keys of variable length are used to improve the security level but the heat dissipation is slightly increased. The number of attacks will increase with time; therefore, more hacking time degrades the security level. The large and variable length keys can prolong node's security level but have to confront the added cost. The work could be extended whenever there is resizing of group. It can be done using the concept of sub-keys.

ACKNOWLEDGEMENT

The authors would like to thank the editor and the anonymous reviewers for their insightful comments and suggestions. We are also deeply grateful to T.I.E.T, Patiala for providing the technical and financial support to carry out this research work.

REFERENCES

[1] H. Qu et. al.Lin Sun, "Certificateless Public Key Encryption with Equality Test" *Information Sciences*, vol. 462, 76-92, 2018.
[2] M. R. Manesh *et al.*, "Security Threats and Countermeasures of MAC Layer in Cognitive Radio Networks," *Ad Hoc Networks*, pp. 85-10, 2018.
[3] P. S. Teh *et al.*, "A Survey on Touch Dynamics Authentication in Mobile Devices," *Computers and Security*, vol. 59, pp. 210-235, 2016.
[4] S. Kokolakis, "Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon," *Computers and Security*, 64, pp. 122-134, 2017.
[5] T. Caulfield *et al.*, "Improving Security Policy Decisions with Models," *IEEE Security & Privacy*, vol. 13, no. 5, pp. 34-41, 2015.
[6] M. Singh *et al.*, "Impairment Aware Routing and Wavelength Assignment Employing Binary Logic Operators," *IEEE Optical Network Design and Modeling (ONDM), University of Cartagena, Spain*, 2016, pp. 9-12.
[7] A. Sharma *et al.*, "Dynamic Programming Based Optimal Renewable Energy Allocation in Sustained Wireless Sensor Networks," *Journal of Renewable and Sustainable Energy*, vol. 10, no. 6, pp. 063705-731, 2018.
[8] A. Sharma *et al.*, "Machine Learning Based Optimal Renewable Energy Allocation in Sustained Wireless Sensor Networks," *Wireless Networks*, pp. 1-29, 2019.
[9] S. Sachdeva *et al.*, "Implementation of AES-128 Using Multiple Cipher Keys," *International Conference on Futuristic Trends in Network and Communication Technologies, J.U.I.T., Solan, India, 2018*, pp. 3-16.
[10] H. Kaur *et al.*, "Implementation of AES-128 Using Multiple Cipher Keys," *4th International Conference on Signal Processing, Computing and Control (ISPCC), J.U.I.T., Solan, India, 2017*, pp. 97-101.
[11] M. Naor, *et al.*, "Privacy Preserving Auctions and Mechanism Design," *Proceedings of the ACM Conference on Electronic Commerce-EC'99, Denver, USA, 3-5th November*, 1999, pp. 129-139.
[12] H. Chien, "Efficient Time-Bound Hierarchical Key Assignment Scheme," *IEEE Transactions on Knowledge and Data Engineering*, vol. 16, no. 10, pp. 1301-1304, 2004.
[13] J. Cao, *et al.*, "Scalable Key Management for Secure Multicast Communication in the Mobile Environment," *Journal of Pervasive and Mobile Computing*, vol. 2, no. 2, pp. 187-203, 2006.
[14] Y. Tseng, "A Heterogeneous Network Aided Public-Key Management Scheme for Mobile Adhoc Networks," *International Journal of Network Management*, vol. 17, no. 1, pp. 3-15, 2007.
[15] A. Kakkar *et al.*, "Comparison of Various Encryption Algorithms and Techniques for Secured Data Communication," *International Journal of Engineering and Technology*, vol. 2, no. 5, pp. 787-795, 2010.
[16] A. Kakkar *et al.*, "Mathematical Analysis and Simulation of Multiple Keys and S-Boxes in A Multinode Network for Secure Transmission," *International Journal of Computer mathematics*, vol. 89, no. 16, pp. 2123-2142, 2012.
[17] R. Amin *et al.*, "A Secure Light Weight Scheme for User Authentication and Key Agreement in Multi-Gateway Based Wireless Sensor Networks," *Ad Hoc Networks*, vol. 36, no. 1, pp. 58-80, 2016.

[18] M. AlSabah *et al.*, "Privipk: Certificate-Less and Secure Email Communication," *Computers and Security*, vol. 70, pp. 1-15, 2017.
[19] K. Xue *et al.*, "A Temporal-Credential-Based Mutual Authentication and Key Agreement Scheme for Wireless Sensor Networks," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 316-323, 2013.
[20] A. Kakkar *et al.*, "Key distribution Scheme for Multinode Network," *IJCA Network Security and Cryptography*, NSC, pp. 30-34, 2011.
[21] F. Skopik *et al.*, "A Problem Shared is A Problem Halved: A Survey on the Dimensions of Collective Cyber Defense Through Security Information Sharing," *Computers and Security*, vol. 60, 154-176, 2016.
[22] Jiguo Li et. al. "Anonymous Certificate-Based Broadcast Encryption with Constant Decryption Cost," *Information Sciences*, vol. 454, pp. 110-127, 2018.
[23] Z. Ali *et al.*, "New Computation Technique for Encryption and Decryption Based on RSA and Elgamal Cryptosystems," *Journal of Theoretical and Applied Information Technology*, vol. 47, no. 1, pp. 73-79, 2013.
[24] Li. X, *et al.*, "Cryptanalysis and Improvement of A Biometrics-Based Remote User Authentication Scheme Using Smart Cards," *Journal of Network Computer Application* vol. 34, no. 1, pp. 73-79, 2011.
[25] S. K. Sood *et al.*, "A Secure Dynamic Identity Based Authentication Protocol for Multi-Server Architecture," *Journal of Network and Computer Applications*, vol. 34, no. 2, pp. 609-618, 2011.

BIOGRAPHIES OF AUTHORS

Dr. Ajay Kakkar was born in Punjab, India, in 1980. He received the B.E. and M.E degree in Electronics Engineering from H.E.C, Haryana in 2002. In 2004, he hsas done his masters in Electronics and Communication from T.I.E.T, Patiala, India, and Ph.D. degrees in Electronics Technology from Guru Nanak Dev University, Amritsar, India in 2013. He is presently working in the ECED of T.I.E.T, Patiala, India. He has chaired session in various conferences organized by different agencies. He has published more than 30 research papers in different Journals and conferences. His research area is Data Security, reliable communication and Ad hoc Networks, Renewable and Sustainable Energy.

Dr. Maninder Singh was born in Punjab, India, in 1980. He received the B.E. and M.E degree in Electronics and Communication Engineering from Punjab Technical University, Jalandhar, India, and Ph.D. degrees in Electronics Technology from Guru Nanak Dev University, Amritsar, India in 2016. In 2017, he joined Simon Fraser University, Burnaby, Canada as Post-Doc research scholar. Since January 2018, he has been working in Rayat-Bahra University, Mohali, India. His current research interests include Machine Learning algorithms, Routing and Wavelength assignment models, reliable data communication and digital circuits. Dr. Singh is a Life Member of the Indian Society for Technical Education (ISTE) and Punjab Academy of Sciences. He has published more than 25 research papers in reputed journals and IEEE conferences.