NEW ALGORITHM FOR WIRELESS NETWORK COMMUNICATION SECURITY

Sirwan Ahmed¹ and Majeed Nader²

¹Department of CNS/ATM, Sulaimaniyah International Airport,
Sulaimani, Iraq

²Department of Electrical and Computer Engineering, Wayne State University,
Detroit, USA

ABSTRACT

This paper evaluates the security of wireless communication network based on the fuzzy logic in Mat lab. A new algorithm is proposed and evaluated which is the hybrid algorithm. We highlight the valuable assets in designing of wireless network communication system based on network simulator (NS2), which is crucial to protect security of the systems. Block cipher algorithms are evaluated by using fuzzy logics and a hybrid algorithm is proposed. Both algorithms are evaluated in term of the security level. Logic (AND) is used in the rules of modelling and Mamdani Style is used for the evaluations

KEYWORDS

NS2, TCL, C++, Stream Cipher, Block cipher, Fuzzy logic.

1. INTRODUCTION

Information security is the protection of information and its critical elements, including the system and the hardware that process, store, and transmit that information. Cryptography plays an important role in today's digital world. Many cryptographic techniques have been developed to meet the various requirements arising from applications [1][2].

Cryptographic algorithm, which is also called a cipher, is the mathematical function used for encryption and decryption. Generally, there are two related functions: one for encryption and the other for decryption [3]. Encryption/decryption protects information from being used by the attacker. Encryption/decryption is a security mechanism where cipher algorithms are applied together with a secret key to encrypt data so that they are unreadable if they are intercepted [4][5][6]. Encryption algorithm characteristics that were considered for the development of metrics are type, complexity, and attack [7].

Network simulator (NS2) is employed to design wireless communication networks and evaluate security. Two programming languages are used to convert plain text to cipher text, which are terminal command language (TCL) and C++. Compare to the other network simulation tools, The NS2 is an important mean for network research because of its advantages of flexibility, high efficiency, low cost, and unlimited number of nodes for network design. It is designed for Unix systems but runs under Windows CygWin as well; It is freely available for research and education purposes [4][8].

Fuzzy inference systems (FISs) are also known as fuzzy rule based systems, fuzzy model, fuzzy expert system, and fuzzy associative memory. This is a major unit of a fuzzy logic system. The decision-making is an important part of the entire system. The FIS formulates suitable rules and

based upon the rules the decision is made. This is mainly based on the concepts of the fuzzy set theory, fuzzy IF-THEN rules, and fuzzy reasoning [3].

In this research, we use the fuzzy logic m- file in Mat lab for the security evaluation of wireless networks. After we study the existing algorithms, we propose a new algorithm, hybrid system, for wireless network communication security. The traditional algorithm, novel algorithm, clock cipher algorithm, and the proposed algorithm are evaluated to highlight the security level of the new algorithm. We employ Mamdani style for the evaluations and logic (AND) for modelling.

2. PREVIOUS WORKS AND THE PROPOSED ALGORITHM

The security of wireless communication network has been widely studied by researchers. [9] performs a comparative study between DES, 3DES and AES. The comparison is presented into nine factors, which are key length, cipher type, block size, developed, cryptanalysis resistance, security, possibility key, Possible ACSII printable character keys, time required to check all possible keys at 50 billion second. These eligible proved that the AES is better than DES and 3DES. A novel network security evaluation method framework, with a comprehensive analysis of the Multiple Attribute Decision Making (MADM) theory is discussed in [10]. This framework constructed a measurement model of network security, and normalizes the measurement process. It also provided specific evaluation methods for satisfying the practical requirements. There in after, an example of network worm propagation evaluation is illustrated. In comparison to the existing evaluation methods, their methods are more comprehensive and scientific, which can make the rank preference order of each worm life cycle stage of each worm defence strategy. The approach in [10] makes a contribution to the standardization and Scientific of the network security evaluation process.

A cryptographic algorithms (RC5) is also evaluated in [11]. Blowfish and DES block cipher algorithms were compared by using C# program. Comparative analysis of RC5, Blowfish and DES is performed with a set of input files and evaluated the encryption and decryption time. The results conclude that RC5 is 1.54 times faster than Blowfish and 2.57 times faster than DES. The results also conclude that the performance of Blowfish algorithm is inversely proportional to key size, if key size increases, the performance decreases and vice-versa. In resource utilization point of view, RC5 utilize extra memory compared to Blowfish and DES, while CPU utilization is approximately the same for all these three algorithms. So RC5 block cipher algorithm is faster and simpler than Blowfish and DES block cipher algorithms. Using RC5 is beneficial where the high encryption rate is required [11].

NS2 is employed in [12] to simulate the end user performance of the wireless network consisting of two access points and five nodes for variable data and transmission rate of the nodes. The simulation results about network behaviour. First variable throughput and transmission rate for the nodes of access point 1 and access point 2, the performance of the network remains constant and there is high fluctuation for a single node. Second comparative study between packet drop rate and transmission rate for the nodes of Access point 1 and Access point 2 in [12] shows that the performances of the observed networks differ and there is high fluctuation for a single node in a 3 node network. A third important feature of performance study is an average packets end to end delay and transmission rate for the nodes of access point 1 and access point 2. The performance of the whole network is finding to be transient initially, but it comes to a stable state after a certain amount of time [12].

A performance evaluation of different symmetric algorithms is studied in [13]. The selected algorithms are AES, DES, 3DES, RC6, Blowfish and RC2. Several points can be concluded from the simulation results and it is found that Blowfish provides the best performance among all algorithms. Then after that the best algorithm which consumes less power, and less time is RC6.

Also the worst approach among all the algorithms in terms of CPU load is RC2 because it leads to heavy workload of CPU as it is very time consuming factor [13].

Two of the common cipher techniques are stream cipher and block cipher. Both are well studied and implemented in the current cipher systems [14] [15]. Stream cipher, which is a symmetric key cipher technique, is a technique of combining some plaintext data digits with a digit stream of pseudo-random cipher that is known as keystream. The cipher text stream digits in stream cipher are generated by encrypting each digit of the plaintext with the specified digit of the keystream separately. The encryptions of the digits are dependent on the cipher state at the time. Therefore, it is called state cipher. In stream cipher exclusive-or (XOR) is employed as bit operation to implement the cipher technique [14].

Unlike stream cipher, block cipher is a scheme of encryption and decryption where instead of a digit we treat with a block of digits of the plaintext digits. The scheme generates an equal size ciphertext block with the chosen block of the plaintext. In most cases, the block cipher has a structure of Feistel which has multi identical processing rounds. Half of the processed data is substituted in each round and the two halves are interchanged and put after the substituted half. The main goal is to expand the original key as technique to use different key for each round [15].

Both stream and block cipher has pro and cons. However, we could improve the performance by taking the advantage of both of them and combine them in one technique. We name the new technique as Hybrid Algorithm which is a new combination of the previous two algorithms. We combine both algorithm and control them. One of the new idea we use is controlling the new algorithm by the user. There is a communication between the transmitter and receiver of the information bits. We evaluated the new algorithm by comparing the performances and study the security of the wireless communication network. We change the algorithm according to the network supervisor as it is shown in Figure 1.

Figure 1. The Diagram of the Hybrid Algorithm.

3. SYSTEM MODELLING

A wireless communication network is designed and developed by utilizing NS2 package. Network security algorithms, such as stream cipher and Block cipher, are employed for exchanging the information between the nodes. We change the algorithm according to the network supervisor as it is illustrated in Figure 1. The security of the wireless network by using fuzzy logic for Hybrid algorithm (stream cipher with Block cipher) and conventional block cipher algorithms is evaluated. We compare both algorithms for network security. Evaluating the Block

cipher, it can be noted that this algorithm has weaknesses and it can be broken by the hackers easily.

The fuzzy logic tool has been widely used for modelling of the evaluation of the network security algorithms. Figure 2 shows a case where only traditional algorithm is used for network security evaluation by using three measures.

Figure 2. The Variable Input and Output of the Traditional Algorithm

It is proven that the networks security depends on the algorithm that is used in the networks. The results of the evaluations show that it is necessary we to develop the algorithms to be more sophisticated so that we can improve the security of the networks and Figure 3 shows this fact. The new algorithm is evaluated by using Fuzzy logic.

Figure 3. The Variable Input and Output Functions of the Hybrid Algorithm

3.1 DESIGN AND SIMULATION

The results reveal that the network security is limited based on the utilized algorithm in the network evaluation. The first set of experiments (Table 1), it can be noted that if the conventional algorithm is used for network security, only in few cases the system has good security. For instance, only a case with the following parameters: key Size =512 bits, block size=64 bits, and

number of rounds =64 has a good security as it's shown in Table 1. Table 1 contains the results for the cases where three measures are used for the network security evaluation. It can be noted that the more sophisticated algorithm is used, the better security of the network is achieved. This fact can be seen in the second set of experiments where five measures are used for the network security evaluation. Table 2 shows the improvements of the second experiments which uses the proposed method of the evaluation. It can be noted that increasing the measures improves the security of the network.

Table 1. The Modelling Results of the Traditional Algorithm using Mamdani Style.

	Input one	Input two	Input three	Output
No.	Key Size (bit)	Block Size (bit)	Number of Rounds	Security Level %
1	16	32	16	21.3
2	32	32	16	50
3	64	32	16	30.2
4	128	32	16	50
5	256	32	16	48.3
6	512	32	16	75
7	1024	32	16	75
8	2040	32	16	50
9	32	64	16	50
10	64	128	16	47.8
11	128	64	32	50
12	256	128	32	48.3
13	512	64	64	81.7
14	1024	128	64	50
15	2040	64	128	50
16	2040	128	128	50
17	32	32	128	50
18	64	64	128	50
19	128	128	128	50
20	256	32	128	50

4. ANALYSIS OF THE HYBRID ALGORITHM

A wireless network is designed based on a hybrid algorithm of network security by using NS2 based on TCL and C++ programs. We also evaluated the networks for the conventional and the hybrid algorithm. Evaluating the network securities by using fuzzy logic, we can conclude the followings:

- Cryptography algorithms (block cipher) is used to secure information in designing of wireless network for data package transfer between nodes.
- Improving the security of a wireless network is still a complicated process and it requires periodical evaluations. Building security of wireless network systems requires a comprehensive security model referring to results of the modelling of evaluation.
- Different metrics of conventional algorithms, key length of stream cipher and sequence code are used as measures to improve the security level of the network. It is noticed in the results in Table 1 and Table 2 that the structure of the crypto algorithms effect on security level. The structure and controlling of the algorithm effect on security level.

Table 2. The Modelling Results of Hybrid Algorithm Using Mamdani Style.

No	Input one Key Size(bits)	Input two Block size (bits)	Input Three Number of Rounds	Input four Sequence code (bits)	Input five Key length (Stream cipher)(bits)	output Security Level
1	16	32	16	2	1	43
2	32	32	16	4	2	55
3	64	32	16	6	4	45
4	128	32	16	8	8	57
5	256	32	16	16	16	64
6	512	32	16	32	32	79
7	1024	32	16	64	64	82
8	2040	32	16	128	128	93
9	32	64	16	256	256	87
10	64	128	16	512	512	88
11	128	64	32	2	1	45
12	256	128	32	4	2	54
13	512	64	64	8	4	83
14	1024	128	64	16	8	76
15	2040	64	128	32	16	87
16	2040	128	128	64	32	94
17	32	32	128	128	64	74
18	64	64	128	256	128	78
19	128	128	128	512	256	93
20	256	32	128	2	512	80
21	512	32	16	4	1	35
22	1024	64	16	8	2	45
23	2040	128	16	16	4	67
24	512	32	16	32	8	50
25	1024	64	16	64	16	48
26	2040	128	16	128	32	80
27	512	32	32	256	64	83
28	64	64	32	512	128	83
29	128	128	64	2	256	76
30	256	32	64	4	512	55
31	512	64	128	8	512	92
32	1024	128	128	16	1	65
33	2040	32	128	32	2	78
34	64	64	128	64	4	65
35	128	128	128	128	8	76
36	256	32	128	256	16	89
37	64	64	16	512	32	87
38	128	128	16	2	64	65
39	256	32	16	4	128	75
40	512	64	16	8	256	94

- The fuzzy logic is used to evaluate the complexity of the wireless network, then the given parameters of the conventional algorithm, the key length of stream cipher algorithm, and sequence code for modelling are used to choose more secure algorithms and select a secure structure. Fuzzy logics have facility tools to evaluate the security of the network.
- Some novelties of this work compared to the others designs, are: a. in this work the security evaluation of network based on five metrics of cryptographic algorithms are used, while other projects have used only three metrics. b. compare to existing modelling and techniques that are used, the model which is used in this work has more facility.

5. CONCLUSIONS

The hybrid algorithm is proposed and used to secure information in the wireless network design for data package transfer between the nodes. 65 mobile node wireless networks for the network simulation are constructed and NS2 is employed to study and analyse the performance of the network. The evaluation modelling results reveal that a comprehensive security model is required to develop the security of wireless network systems. As the security of wireless network is still a complicated process, it needs a periodical evaluation. Utilizing the fuzzy logic for the evaluation of the complexity of the wireless network, we proved that the hybrid system is more complex than conventional system for security in the wireless network and it has a better performance.

REFERENCES

- [1] J. Markus, Y. Moti, & Z. Jianying, (2004) *Applied Cryptography and Network Security*, Berlin Heidelberg: Springer-Verlag.
- [2] S. William, (2011) *Network Security Essential: Application and Standards*, United States of America: Fourth Edition.
- [3] S. Mohammed & S. Sadkhan, (2013) "Block cipher security evaluation based on fuzzy logic," in *The First International Conference of Electrical, Communication, Computer, Power and Control Engineering (ICECCPCE)*, Iraq, Mosul.
- [4] I. Teerawat & H. Ekram, (2008) *Introduction to Network Simulator NS2*, United States of America: Second Edition.
- [5] M. Matin, (2009) "Performance evaluation symmetric encryption algorithm in MANNET and WLAN," in *International Conference for Technical Postgraduates (TECHPOS)*, Kuala Lumpur, pp. 1-4.
- [6] J. Fu, L. Huang, & Y. Yao, (2010) "Application of BP neural network in wireless network security evaluation," in *IEEE International Conference on Wireless Communications, Networking and Information Security (WCNIS)*, Beijing, China, pp. 592-596.
- [7] G. Germano, et al. (2005) "Evaluation of Security Mechanisms in Wireless Sensor Networks," in *Proceedings of the Systems Communications (ICW05)*, p.1-6.
- [8] G. E. Almargni & G. Abdalla, (2012) "Design and simulation of wireless network using NS2," in *second International Conference on Computer Science and Information Technology (ICCSIT)*, Singapore, pp. 157-161.
- [9] Alanazi Hamdan.O., Zaidan B.B., Zaidan A.A., Jalab Hamid A., Shabbir M. and Al-Nabhani Y., (2010) " New Comparative Study Between DES, 3DES and AES within Nine Factors" , *Journal of Computing* , Volume 2, issue 3, pp. 152-157.
- [10] Ezreik Almargni, Gheryani Abdalla, (2012) "Design and Simulation of Wireless Network using NS2", *second International Conference on Computer Science and Information Technology (ICCSIT'2012)* Singapore, pp.157-161.
- [11] Jinjing ZHAO, Yan WEN, and Dongxia WANG, (2011) "A Network Security Evaluation Method Framework Based on Multiple Criteria Decision Making Theory", *Fifth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, IEEE computer society, PP. 371-375.
- [12] Singh Rajender, Misra Rahul , and Kumar Vikas , (2013) "Analysis the Impact of Symmetric cryptographic Algorithms on Power Consumption for various data types", *International Journal on Recent and Innovation Trends in Computing and Communication*, Volume: 1 Issue: 4, pp 221-226.
- [13] Verma Harsh Kumar, Singh Ravindra Kumar, (2012) "Performance Analysis of RC5, Blowfish and DES Block Cipher Algorithms", *International Journal of Computer Applications*, Volume 42, No.16, PP. 8-14.
- [14] A. Menezes, P. van Oorschot, & S. Vanstone, (1996) *Handbook of Applied Cryptography*, CRC Press, 1996.
- [15] S. William, (2011) *Cryptography and Network Security*, United States of America: Fifth Edition.

AUTHORS

Sirwan Mohammed has received the B.S. in Electrical Engineering from University of Salahaddin, in 2005, and the M.S. in Computer and Automation from University of Slemani, Kurdistan of Iraq, in 2014. He is currently a CNS/ATM manager at Sulaimaniyah International Airport. Mr. Mohammed is an IEEE student member and he is also a member of Union Engineering of Kurdistan. He has been working as telecommunication engineer for more than ten years for Sulaimaniyah International Airport. His research interest is security, telecommunication and networks. He is the co-author of multiple publication in IEEE conferences and other relevant conferences.

Majeed Nader has received the B.Sc. in electrical engineering from University of Salahaddin in 2005, the M.Sc. in Electronic and Communication Engineering from University of Slemani in 2009, in Iraq. He also has earned M.S in Computer Engineering from Wayne State University, Michigan, USA. He is currently a Ph.D. Candidate in ECE department and a part time faculty in Engineering technology in Wayne State University. Mr. Nader is an IEEE member. He has worked as Telecommunication Engineer for 7 years and he is currently a senior Electrical Engineer. He is an honoured member of Tau Beta Pi in USA. Mr. Nader's research interest is processor design, FPGA, and Embedded Network system for automotive applications.