EasyChair Preprint

№ 5087

Fuzzy based AODV routing with RC4 and RSA Ciphering for WSNs Security Based on Artificial Intelligence

Alka Pandey and Satya Prakash Singh

March 2, 2021

Fuzzy based AODV routing with RC4 and RSA ciphering for WSNs security based on Artificial Intelligence

Alka Pandey
IFTM University Moradabad
acmp.1986@gmail.com or alka.mpandey@gmail.com
Satya Prakash Singh
Madan Mohan Malaviya University of Technology Gorakhpur (U.P.) (India)
satyaprakash.singh271@gmail.com

Abstract The network security concerns totally depend on cryptography and the QoS is based on routing strategy. WSNs have very limited computation hardware capability because of low energy and high data seed requirements. Hence the cryptography part applied in WSNs is very critical. To cover up the security demand the computation cost is increased that may be compensated by using the simple but efficient protocol for routing strategy. This article is incorporating RC4 and RSA ciphering application in WSNs with smart Fuzzy based AODV routing that supports high data rate in WSNs. RSA and RC4 are figured out separately as cryptographic scheme with intelligent routing strategy that helps to give minimum number of nodes that may gives shortest route in smaller time with fuzzy based artificial intelligence (AI) methodology.

Keywords – WSN, Ciphering, AODV, RC4, RSA, Fuzzy, AI.

I. INTRODUCTION

RC4 is used globally in the security scheme for data ciphering. It was introduced in1987 and undergoes through upgrades. It is very fast and simple ciphering scheme. It has a state vector of 256 bytes with key length 40-256 bits. The effortlessness of RC4 makes it defenceless against diverse security assaults. From the essential structure of RC4 it is watched that it creates a pseudorandom yield succession (bytes) from the permuted interior state which itself is an arbitrary arrangement. The cryptanalyst is dependably looking for the measurable shortcomings of the yield arrangement. Factual shortcomings are the inclinations in the irregular key stream that can be misused with a high likelihood of progress. Another approach proposed in an article [1] gives better security to the information over system by applying RSA calculation scheme. It involves two keys Private Key and Public Key. Open Key is applied for scrambling the information data and it can be seen by anyone but the private key is utilized to decode the messages. To figure out data in RSA it is required to discover prime numbers (p and q) [17]. Additional security is involved

due to modulo n based calculations. A quadratic sifter is applied for factorization in RSA proposed by Arjen et. Al [2,3] . RSA-140 is an upgrade that utilizes number field strainer [4] and the RSA-155is another version that considers simplicity, the RSA-160 and RSA576 was developed in 2003 [5]. RSA-200 came in year of 2004 and the RSA-640 developed in the year of 2005 by Bahr, et. al[6]. In 1976 [8,9,10] first progressive examination performed on the open key cryptography that added necessities for open key cryptosystems.

2. Related work:

The increasing growth of the computing technology and network technology also increased data storage demands. Data Security has become a crucial issue in electronic communication. Algorithms to scramble data which can't be decrypted by party those do not possess the key. Ciphering schemes takes high computing resources in terms of memory and battery and time. A paper accomplished comparative analysis of encryption standards DES, AES and RSA [11].

RC4 is popular stream cipher as symmetric key cryptography. Numerous cryptanalytic results on RC4 stream cipher are based on non-random (biased) events involving the secret key, the state variables, and the key stream of the cipher. An article [12] investigated the effect of RC4 key length on its key stream, and report significant biases involving the length of the secret key.

An article [13] describes that the RSA cryptosystem isn widely used for internet security and authentication in many applications including credit card payments, email and remote login sessions. They discussed another application of RSA algorithm for geo-location (latitude and longitude of source and destination).

Another literature proposed that [14] for scheme with the first three bytes of the RC4 key are public and it gives a strong mutual dependence between the first two bytes of the RC4 key.

3. RSA Algorithm:

RSA has been widely used for many years on the internet for security and authentication in many applications including credit card payments, email and remote login sessions. After seeing several examples of "classical" cryptography, where the encoding procedure has to be kept secret (because otherwise it would be easy to design the decryption procedure), we turn to more modern methods, in which one can make the encryption procedure public, without sacrifice of security: knowing how to encrypt does not enable you to decrypt for these public key systems. To understand how the algorithm was designed, and why it works, we shall need several mathematical ingredients drawn from a branch of mathematics known as Number Theory, the study of whole numbers. In recent times it has been found very useful, as we shall see. Here are the ingredients we will draw from number theory:

- Modular arithmetic
- Fermat's "little" theorem
- The Euclidean Algorithm

A. Public key encryption

This idea omits the need of a carrier to deliver keys to recipients over another secure channel before transmitting the originally intended message. In RSA encryption keys are public, while the decryption keys are not, so only the person with the correct decryption keys can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key cannot be easily deduced from the public encryption key [16].

4. Description of RC4

RC4 runs in two phases. The first part is the key scheduling algorithm KSA which takes an array S or S-box to derive a permutation of (0; 1; 2;.....;N-1) using a variable size key K. The second part is the output generation part PRGA which produces pseudo-random bytes using the permutation derived from KSA. Each iteration or loop or `round' produces one output value. Plaintext bytes are bit-wise XORed with the output bytes to produce ciphertext. In most of the applications RC4 is used with word length n = 8 bits and N = 256. The symbol l denotes the byte-length of the secret key.

The concept of security is generally interpreted as the idea of confidentiality of data being transmitted, particularly the digital information transmitted over the wireless network. Most commonly security is provided using cryptographic primitives. As shown in Fig. 1 the cryptographic primitives are classified into three main categories; not using key, symmetric key and asymmetric key [1]. Although Fig. 1 is not presenting an exhaustive list of these primitives but is highlighting the important and relevant areas. In this paper we have focused on symmetric key ciphers which are also known as secret key or single key ciphers. Secret key ciphers are further classified as block ciphers and stream ciphers. In block ciphers, a block of bits/bytes is processed at a time. DES, IDEA, RC5, AES, BLOWFISH, TWOFISH are the different available block ciphers. Whereas in stream ciphers one bit or a byte of data is processed at a time. Stream ciphers are further classified as synchronous and self-synchronous stream ciphers. Synchronous stream ciphers (SSC) are prominently discussed in literature. However, generally due to the design problems, self-synchronizing stream cipher (SSSC) are not much explored in literature and are less used in practice [2]. Different synchronous stream ciphers available in the literature are RC4, E0 (a stream cipher used in Bluetooth), A5/1 and A5/2 (stream ciphers used in GSM), SNOW 3G, ZUC (4G stream ciphers), Rabbit, FISH, and HC-256 etc.

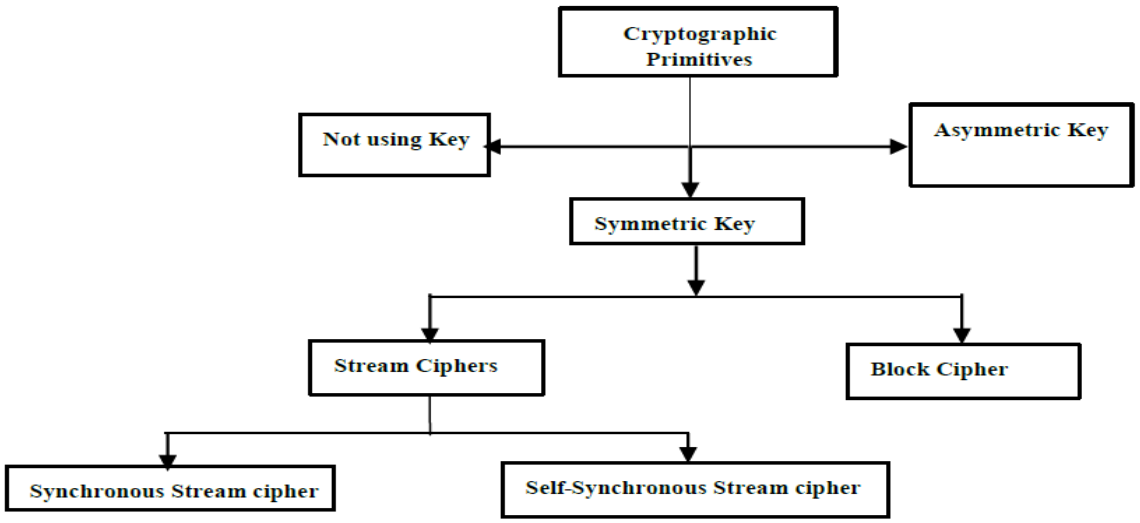

Fig. 1. Cryptographic Primitives

5. Fuzzy based AODV Protocol :

The AODV [7] routing protocol is a reactive routing protocol; therefore, routes are determined only when needed. In this article fuzzy logic is used prior to AODV rioting to intelligently decides minimum nodes that are covered under the zone of current source node and destination node. Hello messages is used to detect and monitor links to neighbours. If Hello messages are used, each active node periodically broadcasts a Hello message that all its neighbors receive. Because nodes periodically send Hello messages, if a node fails to receive several Hello messages from a neighbor, a link break is detected. When a source has data to transmit to an unknown destination, it broadcasts a Route Request (RREQ) for that destination. At each intermediate node, when a RREQ is received a route to the source is created. If the receiving node has not received this RREQ before, is not the destination and does not have a current route to the destination, it rebroadcasts the RREQ. If the receiving node is the destination or has a current route to the destination, it generates a Route Reply (RREP). The RREP is unicast in a hop-byhop fashion to the source. As the RREP propagates, each intermediate node creates a route to the destination. During this route decision the fuzzy logic rejects the request of those nodes which do not exist under the nearby area belongs to the source and destination coordinates. In this way possibility of large routes with unwanted nodes is greatly reduced. When the source receives the RREP, it records the route to the destination and can begin sending data. Small number of RREPs are received by the source, the route with the shortest hop count is chosen by the AI decision mechanism [10].

In the next part as the data moves from the source to the sink, each the timers associated with the routes is calculated. If a route is not used for some period of time, a node cannot be sure whether the route is still valid; consequently the fuzzy decision mechanism removes the route from its routing table. If data is following and a link break is detected, a Route Error (RERR) is sent to the source of the data When the source of the data receives the RERR, it invalidates the route and reinitiates route discovery if necessary.

6. Result and Discussion:

We have developed algorithm in MATLAB that generates a WSN network of MxM field size with N number of nodes. The size of WSN and the nodes i.e. M, N parameters are given by user and as per the user choice this algorithm develops a WSN network with all the nodes are distributed randomly. For N nodes we have consider any one of the node as the source and another as destination node. After generation and distribution of WSN nodes the AODV routingalgorithm is applied to make the path for data transmission in between the source and destination node. This multi-hop routing is as established the algorithm applies ciphering of data packets and then the ciphered packets are transferred from source to destination through the route developed by AODV protocol.

We have compared the RC4 and RSA ciphering techniques performance for different types of networks having 40, 60, 80 and 100 nodes and at the transmission rate of 500.1000 and 1500 data packets. The time taken by both ciphering techniques are observed for different configuration of network named as Na, Nb, Nc, Nd and Ne and results are tabulated in next paragraphs.

Table 1 shows the results for network Na, Nb, Nc, Nd and Ne at 40 nodes for both RC4 and RSA ciphering based transmission over the AODV generated route The time consumed in each network is given in sec

Data Size (Bits)	RC4 associated Fuzzy based AODV results					RSA associated Fuzzy based AODV results				
	WSN1	WSN2	WSN3	WSN4	WSN5	WSN1	WSN2	WSN3	WSN4	WSN5
500	8.5	7.9	7.9	7.8	8.1	42.9	45.0	47.0	43.1	42.1
1000	7.9	8.0	7.9	7.9	7.9	75.9	87.9	91.9	86.8	83.6
1500	8.0	8.1	8.0	8.1	8.1	122.9	128.8	123.3	123.6	119.9

Similarly table 2,3 and 4 are for the 60,80 and 100 node networks. The analysis is performed in terms of time consumed in WSN generation, AODV routing ,ciphering and deciphering of the numeric data.

Table 2: Time consumed in RC4 and RSA ciphering by AODV route generation for 60 nodes..

Data Size	RC4 associated Fuzzy based AODV results	RSA associated Fuzzy based AODV results

(Bits)										
	WSN1	WSN2	WSN3	WSN4	WSN5	WSN1	WSN 2	WSN 3	WSN 4	WSN5
500	7.8	7.9	7.8	7.9	7.9	49.2	39.2	44.8	42.3	42.9
1000	8.0	8.0	8.2	8.2	8.0	83.2	81.2	83.0	80.7	78.8
1500	8.0	8.2	8.2	8.2	8.2	133.8	123.8	130.6	122.9	123.0

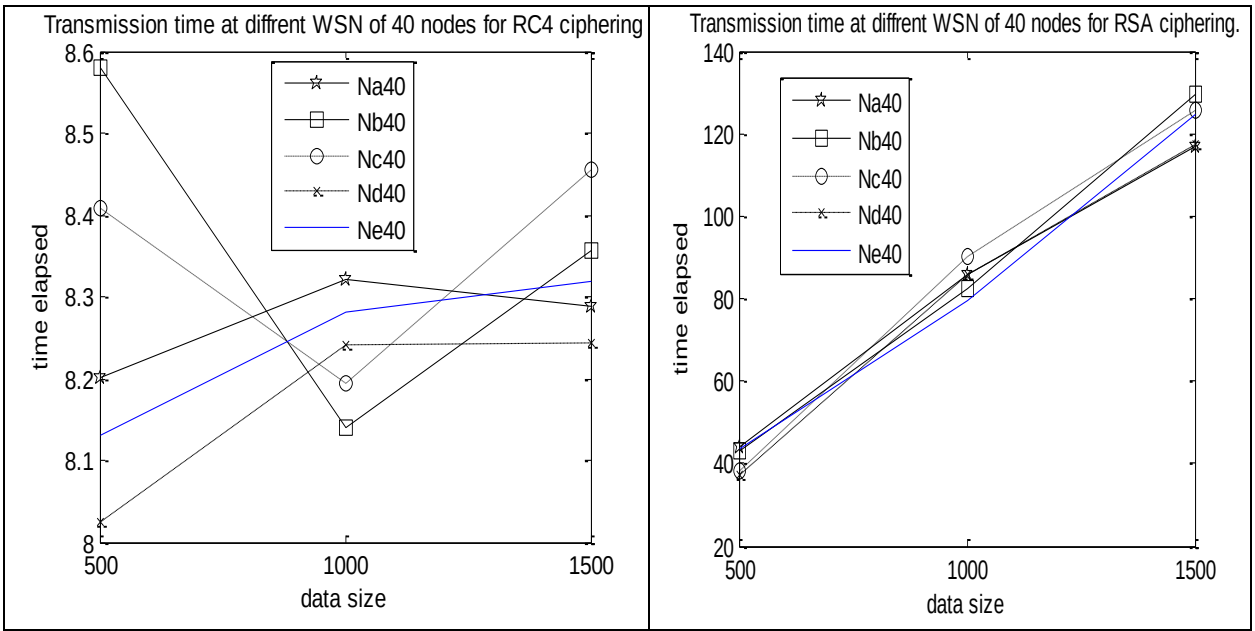

Figure 1: Transmission time required at WSN of 40 nodes at different packet size of 500,1000 &1500
For RC4(left) and RSA ciphering(right) using table 1.

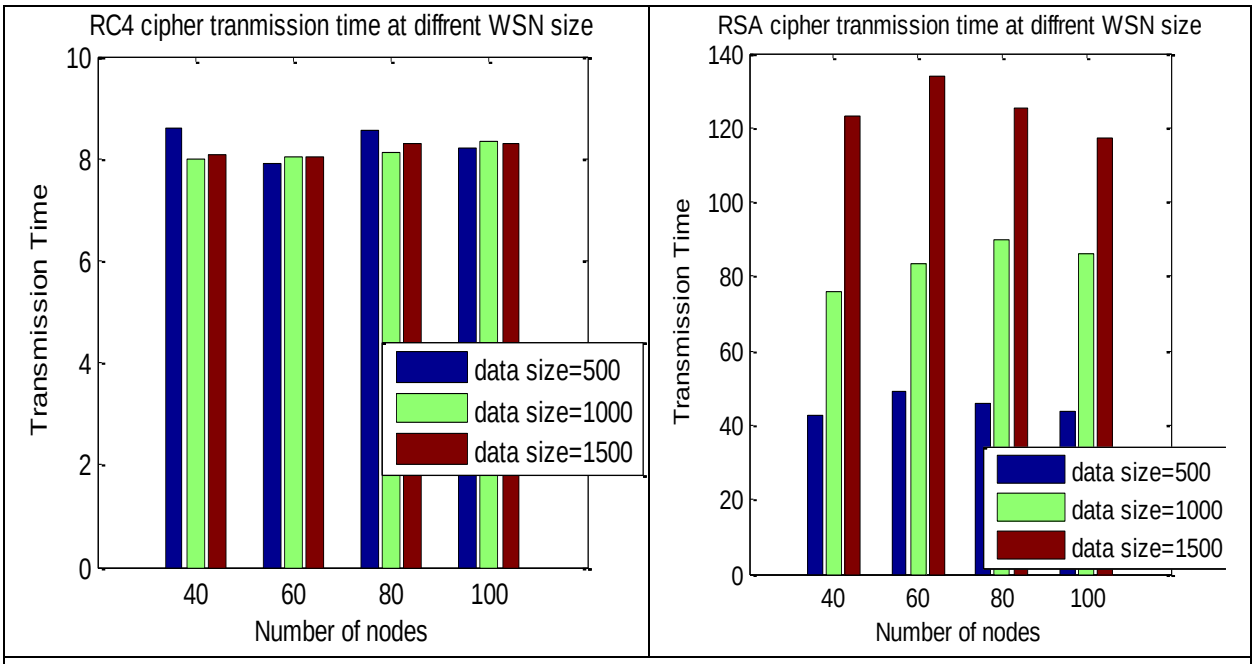

Figure 2: Transmission time at network size of 40,60,80 and 100 nodes where each bar represent time elapsed at particular data packet size of 500,1000 and 1500 for RC4(left) and RSA(right) using table 1 to 4.

7. Conclusion:

This work describes an intelligent approach for security concerns in WSN network with Fuzzy based smart AOCV routing and security scheme. RC$ and RSA as two ciphering schemes are associated to calculates performance over the transmission delay. Different types of networks with different number of sensor node are observed in terms of time consumed in transmission mode with Fuzzy base AODV routing time associated with RC4 and RSA ciphering. It has been observed that for all the cases RC4 ciphering consumes less time as compared to RSA ciphering. Hence it proves that for WSN networks RC4 ciphering provides higher transmission rate due to small time consumption in ciphering deciphering. In future we can also check performance for routing technique other than AODV. We may also consider composite routing mechanism that involves other artificial intelligence tools for determining the shortest possible route in minimum time. It can also helps in minimizing time delay in data transmission in WSN network with high security concerns.

References:

[1] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Hand- book of Applied Cryptography. CRC Press, August 2011 edition, 1996. Fifth Printing.

[2] Douglas R. Stinson. Cryptography: Theory and Practice. CRC Press, third November 2005) edition, 1995.

[3] Thomsan D. Bruce D. Arjen L. and Mark M.,"On the Factoring of RSA-120", (169), pp.166-174, 1994

[4] Cavallar S, Dodson B, Lenstra A, Leyland P,Lioen W, Montgemery P, Murphy B, and Zimmermann P, “Factoring of RSA-140 using the number field sieve”, 1999
[5] Eric W “Prime Factorization Algorithm”, Mathworld.woiframe.com/news/ 2003
[6] Bahr F, Boehm M, Franke J and Kleinjung T, “For the Successful Factorization of RSA-200” www.rsasecurity.com
[7] C. E. Perkins, E. M. Belding-Royer, and S. Das. Ad hoc On- Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.
[8] Diffie W and Hellman M, “New Direction in Cryptography, IEEE Transaction on Information Theory, IT-22(6): 644-654, 1976
[9] Rivest R, Shamir A and Adelman L, “A Method for Obtaining Digital Signature and Public Key Cryptosystems”, Communications of the ACM, 21, pp. 120-126, 1978
[10] C. E. Perkins and E. M. Royer. The Ad hoc On-Demand Distance Vector Protocol. In C. E. Perkins, editor, Ad hoc Networking, pages 173–219. Addison-Wesley, 2000.
[11] Priteshkumar Prajapati et. al., " Comparative Analysis of DES, AES, RSA Encryption Algorithms", International Journal of Engineering and Management Research, Volume-4, Issue-1, February-2014.
[12] Sourav Sen Gupta and Subhamoy Maitra, "(Non-)Random Sequences from (Non-) Random Permutations—Analysis of RC4 Stream Cipher" J. Cryptol. (2014) 27: 67–108.
[13] Avala Ramesh et. al., " Analysis On Biometric Encryption using RSA Algorithm", International Journal Of Multidisciplinary Educational Research, Volume 2, Issue 11(2), October 2013.
[14] Ayesha Khan, " Geo Location Based RSA Encryption Technique", International Journal on Advanced Computer Theory and Engineering (IJACTE), Volume-2, Issue-2, 2013.
[15] Sourav Sen Gupta et. al., " Dependence in IV-related bytes of RC4 key enhances vulnerabilities in WP" IACR 2014.
[16]. Ankita Bajpai et.al. "A-Genetic-Algorithm-Optimized-Security-using-Chaotic-Key-Generation-Scheme-for-Image-Encryption" International Journal of Research and Development in Applied Science and Engineering, Volume 7, Issue 2, July 2015.
[17] Mohd. Naseem et al. "Energy Efficient Routing Protocol in Wireless Sensor Network" International Journal of Research and Development in Applied Science and Engineering, Volume 7, Issue 1, May 2015.