Improved Way to Enhance Information Security Using Hybrid Cryptography on WSN: A Research

Sapna Rani
M.Tech(CSE), NCCE, Israna, Panipat, Haryana, India.

Sukhbir Singh
Assistant Professor, NCCE, Israna, Panipat, Haryana, India.

Abstract – The popularity of Wireless Sensor Networks (WSN) has increased rapidly and tremendously due to the vast potential of the sensor networks to connect the physical world with the virtual world. Since sensor devices rely on battery power and node energy and may be placed in hostile environments, so replacing them becomes a difficult task. Thus, improving the energy of these networks i.e. network lifetime becomes important.

Index Terms – WSN , DES , AES , MD5.

1. INTRODUCTION

1.1 Wireless Sensor Networks

Sensor nodes offer a powerful mixture of allotted sensing, computing and communication. The ever-growing skills of those tiny sensor nodes, which includes sensing, statistics processing, and speaking, permit the perception of WSNs primarily based on the collaborative strive of a number of other sensor nodes. They allow an intensive range of packages and, on the same time, provide numerous demanding situations because of their characteristic, basically the stringent strength constraints to which sensing nodes are generally subjected. WSNs include knowledge and technology from three precise fields; Wireless communications, networking and Systems and Control idea.

Due to the deployment in hostile environment, the network lifetime and data availability are extremely important in WSN. The system should provide automatic and effective action in difficult situation. A typical sensor network operates in five phases:

1) Planning phase 2) deployment phase 3) post-deployment phase 4) operation phase 5) post-operation phase

Potential applications for large-scale wireless sensor networks exist in a variety of fields, including medical monitoring, environmental monitoring, surveillance, home security, military operations, and industrial machine monitoring.

To prevent the information or data from unauthorized access and to protect sensitive information transmitted online, Encryption is used which convert that data or information into a code. It converts the data or information into another form called cipher text in such a way that only authorized person can access that.

In practical networking system, network coding offers interesting applications. By using network coding the throughput of the system improved and it also provide a high degree of robustness to the system. "Network coding is a particular in-network data processing technique that exploits the characteristics of the wireless medium (in particular, the broadcast communication channel) in order to increase the throughput of the network." In linear network coding only linear mapping is involved and it can be executed at low computational cost.

2. RELATED WORK

A secure and energy efficient data dissemination protocol is proposed for WSN [1]. By choosing best route from the available routes, we can define a routing metric. This best route involves those routes that consume less energy. [2] This paper analyzed the time needed to diffuse information throughout a network when network coding is implemented at all nodes. [3] A modified Stable Election Protocol (SEP), which employs a mobile sink, has been proposed for WSNs with non-uniform node distribution. The proposed algorithm has better performance than traditional routing algorithms, such as LEACH and SEP. A brief survey work is done on the existing various data dissemination protocols for wireless sensor networks and their performances were compared [4]. This paper systematically analyzed the various components, design choices, and tradeoffs involved in the design of a solar energy harvesting module and their impact on the efficiency [5]. The Proposed schemes show how harvesting aware power management improves energy usage compared to only battery aware approaches. A trajectory-based network coding (TBNC) method is proposed to disseminate data in mobile wireless sensor network (MWSN) [6]. It is designed according to the characteristics of MWSN and is appropriate for the mobile nodes that share anonymously its GPS pre trajectory for the higher bandwidth. A new dissemination protocol called Splash is proposed, that eliminates the need for contention resolution by exploiting constructive interference and channel diversity to

effectively create fast and parallel pipelines over multiple paths that cover all the nodes in a network [7]. In practical networking system, network coding offers interesting applications [8]. By using network coding the throughput of the system improved and it also provide a high degree of robustness to the system. Some drawbacks of applying network coding in real-world sensor network scenarios are described in [9]. An adaptive sampling algorithm is proposed which is based on the Box-Jenkins approach in time series analysis [19]. To measure the performance of our algorithms, we use the ratio of the reduction factor to root mean square error (RMSE). In [11] an extensive guide for the researchers that aim to validate proposed algorithms for wireless sensor networks in MATLAB environment. A model is presented for the lifetime of wireless sensor networks [12].

The model takes into consideration several parameters such as the total number of sensors, network size, percentage of sink nodes, location of sensors, the mobility of sensors, and power consumption. Using network coding allows for a simple, distributed and robust algorithm where nodes do not need any information from their neighbors [13]. In this paper, we analyze the time needed to diffuse information throughout a network when network coding is implemented at all nodes. In [14] we consider a single-hop wireless network consisting of a base station and *N* receivers. We perform an asymptotic analysis, as $N \to \infty$, of the expected delay associated with the broadcasting of a file consisting of *K* packets. A new architecture for wireless mesh networks is designed in [15]. In addition to forwarding packets, routers mix (i.e., code) packets from different sources to increase the information content of each transmission.

In [16] examine the simplest possible information flow problem and explore one of the most attractive features network coding offers: the ability to enable near optimal performance in a completely decentralized and randomized setting. Queue management at the intermediate node improves the chance of network coding at the intermediate node [16]. We used a biologically-inspired algorithm for the energy-efficient data dissemination in wireless sensor networks [16]. Results show that important power savings can be made and that the accuracy of predicted data is adequate.

3. PROPOSED WORK

In our work we have emphasized over the encryption of data in network coding. We also used MATLAB tool to create the environment for the network. At sender nodes level, 2 level encryption algorithms have been applied. One is MD5 encryption and another is RSA encryption decryption. MD5 is stands to protect the data. The whole process block diagram is shown in the figure 3.1. The whole process is divided into two modules. First is encryption of data and second is about network coding.

Module 1: Encryption of Data

For security of this process RSA and MD5 algorithms are required. Decryption of MD5 is not possible and message generated by RSA is secure. To check whether hash code generated by deciphered message is same as the ciphered' has code at the transmitting end RSA deciphered message is again MD5 decrypted at the receiver end.

After matching both hash codes, it believes that there is no interruption with data or messages and through transmission channels message travelled safely.

RSA algorithm:

RSA algorithm has both encryption and digital signature (authentication). It works as follow: take two large primes, p and q and compute their product $n = p.q$ where n is called modulus. Choose a no. e, less than n and prime to $(p-1)(q-1)$. In this $(p-1)(q-1)$ and e have no common factors except 1. Find another number d such that $(ed-1)$ is divisible by $(p-1)(q-1)$. the value of e is called public exponent and value of d is called private exponent. The public key is the pair (n, e) the private key is (n, d). the factors p and q may be destroyed or kept with the private key.

The RSA algorithm involves three steps: key generation, encryption and decryption.

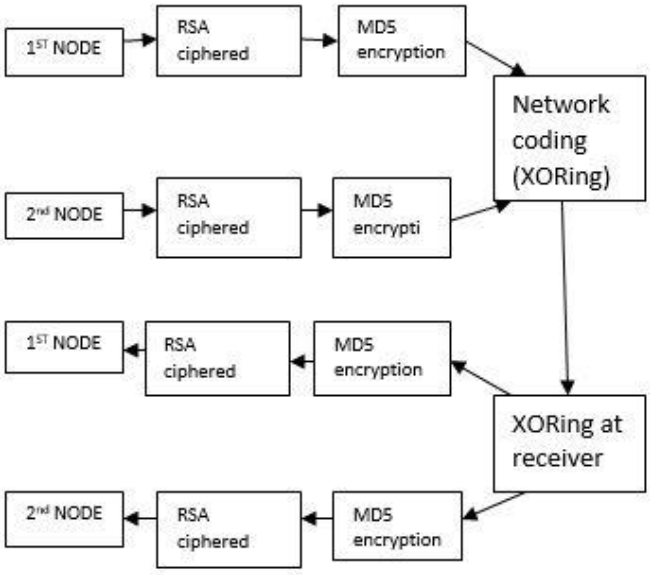

Figure 3.1 block diagram for the encryption process

Key generation:

There are two keys involved by RSA- private and public keys. The public key is used for encrypting the message and known. by everyone. This encrypted message can be decrypted by only private key. Key generation for RSA is as the following way:

- We choose two prime numbers p and q. both should be chosen at random and bit length also should be similar.
- Compute $n = p.q$ where n is the modules for both private and public keys.
- Compute $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = n-(p+q-1)$ where φ is Euler's function.
- Choose an integer e such that $1 < e < \varphi(n) and \gcd(e, \varphi(n)) = 1;\ i.e, e\ and\ \varphi(n)$ co-prime. *e* is released as the public key exponent having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$.
- Determine d as $d \equiv e^{-1}(mod\varphi(n)); i.e., d$ is multiple inverse of e.
- Solve for d given $d.e \equiv 1(mod\ \varphi(n)))$
- d is kept as private key exponent.

Encryption:

Suppose T wants to transmits his public key $(n.e)$ to R and keeps the private key secret. R then wishes to send message M to T. R first turns *M* into an integer *m*, such that $0 < m < n$ *n* by using an agreed-upon reversible protocol known as a padding scheme. He then computes the cipher text *c* corresponding to

$$c = m^e (mod\ n)$$

This can be done quickly using the method of exponentiation by squaring. R then transmits *c* to T.

Decryption:

T can recover *m* from *c* by using her private key exponent *d* via computing

$$m = c^e (mod\ n)$$

Given *m*, T can recover the original message *M* by reversing the padding scheme.

MD5 Algorithm:

MD5 algorithm consists of 5 steps:

STEP 1: Appending Padding Bits: The original message is "padded" (extended) so that its length (in bits) is congruent to 448, modulo 512. The padding rules are:

- The original message is always padded with one bit "1" first.
- Then zero or more bits "0" are padded to bring the length of the message up to 64 bits less than a multiple of 512.

STEP 2: Appending Length: 64 bits are appended to the end of the padded message to indicate the length of the original message in bytes.

STEP 3: Initializing MD Buffer. MD5 algorithm requires a 128-bit buffer with a specific initial value. The rules of initializing buffer are:

- The buffer is divided into 4 words (32 bits each), named as A, B, C, and D.
- Word A is initialized to: 0x67452301.
- Word B is initialized to: 0xEFCDAB89.
- Word C is initialized to: 0x98BADCFE.
- Word D is initialized to: 0x10325476.

STEP 4: Processing Message in 512-bit Blocks: It loops through the padded and appended message in blocks of 512 bits each. It is the main step of the MD5 algorithm.

Step 5: Output: The contents in buffer words A, B, C, D are returned in sequence with low-order byte first.

Module 2: Network Coding

In practical networking system, network coding offers interesting applications. By using network coding the throughput of the system improved and it also provide a high degree of robustness to the system. "Network coding is a particular in-network data processing technique that exploits the characteristics of the wireless medium (in particular, the broadcast communication channel) in order to increase the throughput of the network." In linear network coding only linear mapping is involved and it can be executed at low computational cost. Network reduces the waiting time in case of multicasting and increase the throughput by XORing the data into a single message. XORing is the only way by which two messages which take part in this process and lose their identity to new one, can be reverted back to their identity just by XORing the XORed output with any of them. In our work comparison is done in terms of time consumed, throughput and waiting time.

4. RESULTS

By using its communication and other toolboxes, the proposed work has been implemented in MATLAB. MATLAB allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other languages, including C, C++, Java, Fortran and Python. Graphical user interface developed for proposed work with the help of MATLAB is shown in figure 4.1 below.

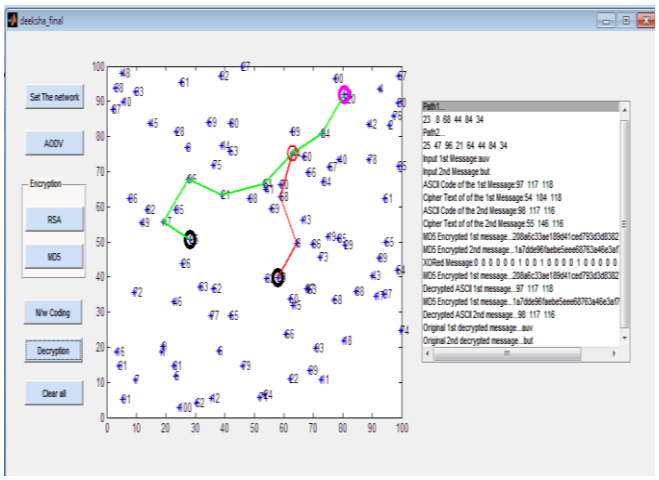

Figure 4.1: graphical user interface developed for proposed work

As AODV selects the path by transmitting the RREQ and RREP messages to destination node, so moving message functionality is added in our GUI as shown in figure4.2 Once paths are set by AODV protocol, same path has to be followed by the network coding. When the button for encryption by RSA is pressed in the GUI, then message box will appear asking for the input message as shown in figure 4.3.

The right side pane in the GUI inherits the all input and output of simulation. The AODV path established through nodes are also displayed in the right side pane.For the test purpose we have entered the message 'AODV' for the first node and 'NET2' for the second node. Both messages are of 4 letters long and the algorithm is not affected by the affected by the data type used in the message.

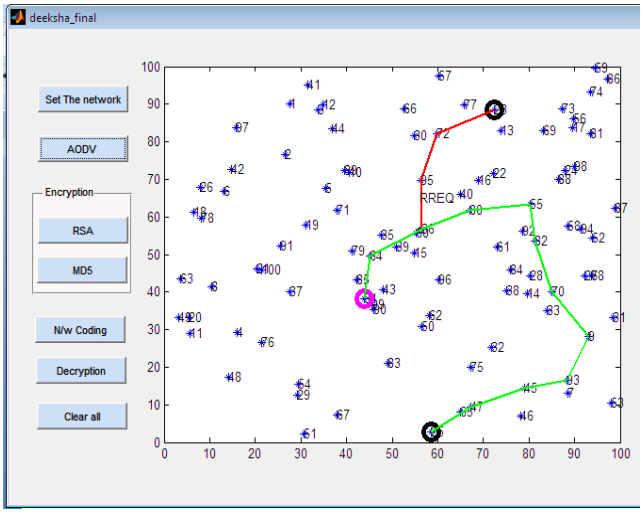

Figure 4.2: RREQ message moving along the path

The RSA ciphered message is shown in figure 4.4 of the right plane.

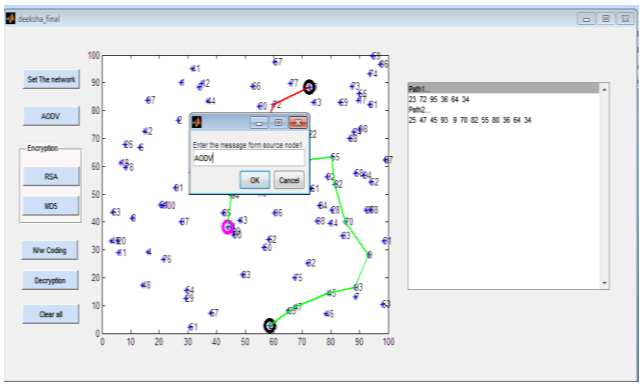

Figure 4.3: Input message for RSA algorithm

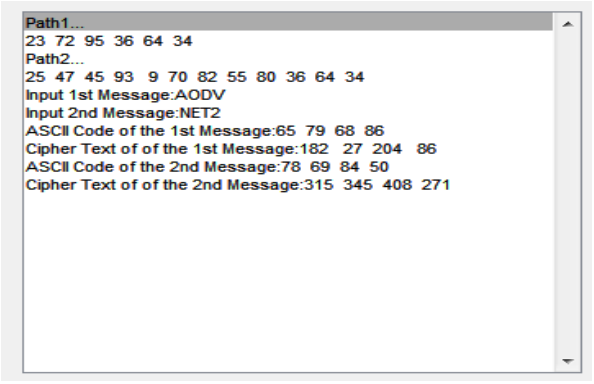

Figure 4.4: RSA ciphered input messages

Ciphered message is converted to hash value using MD5 algorithm as shown in figure 4.5. This encrypted message is put on the transmission channel and at the common node in the path XORing takes place where these hash messages are converted into binary for XOR operation. The flow of message is visible in the GUI.

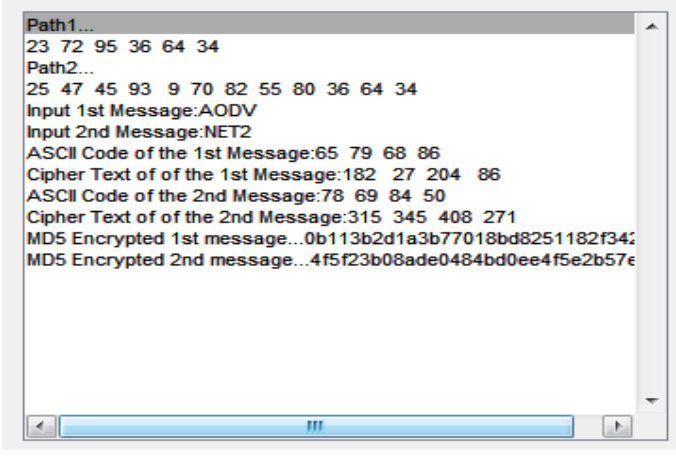

Figure 4.5: MD5 encrypted cipher message

The binary message converted at the common node is shown in figure 4.6 below

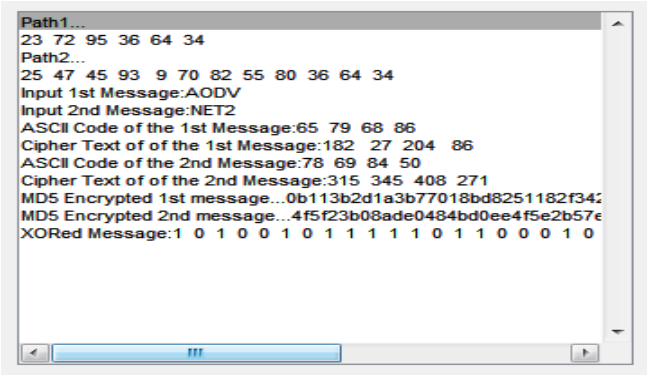

Figure 4.6: XORed message

At the receiver node initially message is XORed again to get each source node's message and then for each message is deciphered by RSA algorithm followed by MD5.

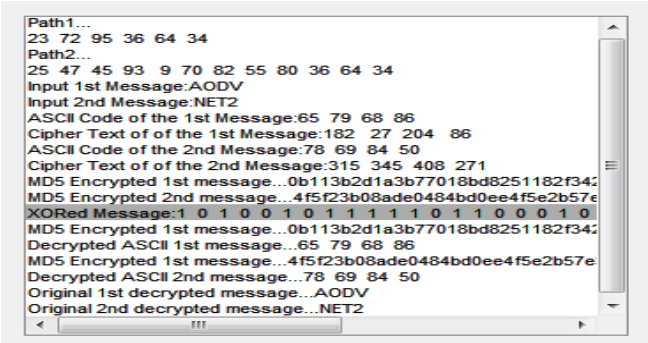

Figure 4.7: Decrypted message at the destination node

5. CONCLUSION

Network coding increases the solution space by solving optimization problems. Thus, we can achieve points we could not achieve before – such as the min-cut to each receiver when multicasting. We know that routing allows to achieve the min-cut capacity, however, pre-supposes a static knowledge of the network. If the network dynamically changes, routing will not be able to achieve good performance. However, with random coding, each receiver, to decode, needs to know the transfer matrix and solve linear equations. To learn the transfer matrix, we need to employ coding vectors that essentially are a form of training. Coding vectors allow for a very simple, distributed operation, at the cost of an overhead. In our work we have simulated a network for network coding and tested it for two level security algorithms. For this purpose RSA and MD5 encryption algorithm has been used and if at the end same MD5 has messages is received from deciphered message, it proves that our message was not attacked and safe.

REFERENCES

[1] Neeraj Kumar, Manoj Kumar, and R. B. Patel," A Secure and Energy Efficient Data Dissemination Protocol for Wireless Sensor Networks" International Journal of Network Security, Vol.15, No.6, PP.490-500, Nov. 2013

[2] Mohammad Hamed Firooz, Student Member, IEEE, Sumit Roy Fellow, IEEE," Data Dissemination in Wireless Networks with Network Coding" arXiv:1203.5395v3 ,8 Dec 2013

[3] Jin Wang, Zhongqi Zhang , Feng Xia , Weiwei Yuan and Sungyoung Lee," An Energy Efficient Stable Election-Based Routing Algorithm for Wireless Sensor Networks" Sensors 2013 network coding in wireless sensor networks." ACM SIGBED Review 9.3 (2012).

[4] Voigt, Thiemo, et al. "On the applicability of network coding in wireless sensor networks." ACM SIGBED Review 9.3 (2012).

[5] Law, Yee Wei and Chatterjea, Supriyo and Jin, Jiong and Hanselmann, Thomas and alaniswami, Marimuthu (2009), "Energy-efficient data acquisition by adaptive sampling for wireless sensor networks. In: 2009 International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly, 21-24 June 2009, Leipzig, Germany (pp. pp. 1146-1151).

[6] Milan Simek, Patrik Moravek and Jorge sa Silva," Wireless Sensor Networking in Matlab:Step-by-Step" Eletrorevue, Vol. 2, No. 3, September 2011.

[7] Abdelrahman Elleithy and Gonhsin Liu," A Simulation Model For The Lifetime Of Wireless Sensor Networks" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.2, No.4, December 2011

[8] Mohammad H. Firooz, Student Member, IEEE, Sumit Roy Fellow, IEEE," Data Dissemination in Wireless Networks with Network Coding" *EURASIP Journal on Wireless Communications and Networking* 2010

[9] Stojanovic, I.; Sharif, M.; Starobinski, D., "Data Dissemination in Wireless Broadcast Channels: Network Coding or Cooperation," Information Sciences and Systems, 2007. CISS '07. 41st Annual Conference on, vol., no., pp.265,270, 14-16 March 2007

[10] Sachin Katti, Hariharan Rahul, Wenjun Hu Dina Katabi, Muriel M´edard," XORs in The Air: Practical Wireless Network Coding" SIGCOMM'06, September 11–15, 2006, Pisa, Italy

[11] Fragouli, C., "Network Coding: Beyond Throughput Benefits," Proceedings of the IEEE , vol.99, no.3, pp.461,475, March 2011

[12] Jisha Mary Jose, Jomina John," Data Dissemination Protocols in Wireless Sensor Networks - a Survey" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 3, March 2014

[13] Rohit Kumar Vishwkarma, Arvind Kumar," Reliable and Efficient Data Dissemination Protocol for Wireless Sensor Networks" International Journal of Computer Applications (0975 – 8887) Volume 69– No.27, May 2013

[14] Lingzhi Li, Shukui Zhang, Zhe Yang, and Yanqin Zhu," Data Dissemination in Mobile Wireless Sensor Network Using Trajectory-Based Network Coding" International Journal of Distributed Sensor Networks Volume 2013.

[15] Manjunath Doddaven katappa, Mun Choon Chan, Ben Leong," Splash: Fast Data Dissemination with Constructive Interference in Wireless Sensor Networks" 10th USENIX Symposium on Networked Systems Design and Implementation (NSDI '13)

[16] Christina Fragouli, JeanYves Le Boudec, J¨org Widmer," Network Coding: An Instant Primer" CM SIGCOMM Computer Communication Review Volume 36, Number 1, January 2006Voigt, Thiemo, et al. "On the application.