Key Distribution Scheme for Multinode Network

Ajay Kakkar
Thapar University, Patiala

Dr. M. L. Singh
G.N.D.U, Amritsar

Dr. P. K. Bansal
Ex- Principal M.I.M.I.T, Malout

ABSTRACT
In order to protect the data from the intruders powerful encryption algorithms with multiple keys has been used over the recent years. Once the encryption process has been done then there is a need to transmit it over the channel. The secured model has been examined on the basis of its design, mode of transmission of data and number of nodes. With increase in number of nodes, key length, number of keys and data length the model consume more power and takes more time to generate keys from the available data. Therefore in this paper a new approach has been proposed in which keys are generated, processed and distributed in the model by the help of S- Boxes in order to reduce the processing time. MATLAB 7.3 has been used to determine the processing and failure rate of various keys in multinode network.

1. INTRODUCTION
The model is designed in such a way that it should makes comprise between multiple keys and S-Boxes and it enables the higher class to retrieve the encrypted data related with lower classes. In the same case it is expected that the lower classes does not have the power to access the data concerned with higher classes. A key management system is used to provide such kind of facility. Once a key has been exchanged then the bit string of the key might becomes known to the hacker. In such cases it is highly required to re-encrypt the same data with different key. This has been done only such cases when the failure rate of the previous key exceeds from a predefined value. The behaviors of the keys are unpredictable in real environment, there is always a difference between ideal and real key. In order to achieve this, we determine to what extent several security patterns are robust to known categories of attacks. Various classes are created for represent the numbers of attacks in a given interval of time. The need for risk analysis at design level has been particularly suggested by McGraw [1]. If analysis of the attack has been done in the initial stage then it will provide easiness to select the proper security patterns. Several specialized encryption techniques have been proposed to the security patterns by R. Agrawal [2]. In 1977, R.M. Davis provides a hardware based algorithm for enciphering data, which has been adopted as a Federal standard to provide a high level of cryptographic protection [3]. In 1999, W. Stallings presents key distribution techniques based upon the polynomials. It also provides the way to use various cipher design procedure for the sensor networks. Different encryption methods to secure the transmission or storage of the data are proposed and evaluated that allows high encryption and decryption rates [4]. In 2002, Subbarao V. Wunnava describes the data encryption performance and evaluation schemes [5]. In 2002, L. Eschenauer suggests random key management scheme for distributed sensor networks [6]. In 2003, D. Liu [7] provides an efficient way to establish pairwise keys in a Wireless Sensor Network (WSN). It also provides the technique to determine the faulty nodes in a given network. Multiple failure rates of single key can also be determined in the approach. In the same year, C. Karlof [8] suggests the routing techniques in WSN. They also show how the keys are protected from the various attacks and what the counter measures are. In 2004, Xun Yi describes an approach based on identity based fault tolerant conference used for multiple key agreements between the users [9]. In 2008, Park Et. Al. provides dynamic path management with resilience constraints under multiple link failures in multi protocol label switching. The work also highlights the recovery mechanisms for the faculty nodes [10]. In 2010 S. Pradheep kumar et. Al. proposed a secured grid based route driven PKC scheme for heterogeneous sensor networks. They also compare the energy and throughput efficiency for the dynamic position of sensor nodes. They tested their route driven scheme for the scalability by varying the node density from 100 nodes 1000 nodes in the network. The main limitation of their work is that in case of node failure only neighboring nodes were used to hold the data of faulty node. Practically it is not possible to provide additional buffers to all the nodes to cope the problem. In 2011 Lepakshi Goud T [17] proposed a routing driven public key crypto system based key management scheme for a sensor network. The work was focused to integrate the advantages of classical cryptography and RSA public key algorithm along with Quantum Key Distribution Protocols (QKDPs) in order to detect the eavesdroppers. The work not includes any simulation and practical implementation of keys on FPGA boards.

On the basis of previous work, we are focused to design a network which consists of n nodes, where each node has the ability to re-encrypt the data under critical situation. Multiple keys are used to protect the individual node. The failure rate of all the keys is simultaneous checked by using MATLAB 7.3. The objectives of the work is to deign a network having (i) re routing ability, (ii) re-encryption of keys and (iii) determination of failure rate of keys.

2. FORMATION AND ANALYSIS OF MODEL
This section deals with the analysis of failure rate of various keys used by different S- Boxes in MN. On the basis of number of attacks, hacking levels and security levels are determined for the model (Table 2.1). Multiple keys $k_1 \& k_2$ having different failure rate a, b , are used for different stations $S_i, S_i^{'}$ *where* $1 \le i \le N$,
$T_1, T_2 = active\ time\ of\ k_1, k_2\ resp.$

Table 2.1. Various security levels for the multinode network

S. No.	Hacking Level	Total number of attacks in one minute	Level of Security	Remarks
1	Low	0-50	Very Good	Used for both short and long data sequences
2	Medium	51-100	Good	Normally used for long data sequences with multiple keys
3	Average	101-150	Average	Prefer short sequences
4	Marginally acceptable, provided that 2nd key (low failure rate take the charge immediately in case of failure of 1st key)	151-200	Weak	Only short data length sequences
5	High	Above 200	Very weak	Not used

There are many approaches suggested by Jong Park [10] for dynamic path management. These approaches also take care of link failures, moreover they also provide the effective approach to re-route the data in case of hazards.

(a) End to end mode

The figure 2.1a shows that how the data is transmitted between the two parties. Here end to end protection mode has been used. Source (S) and destination (D) are linked with each other by multiple nodes.

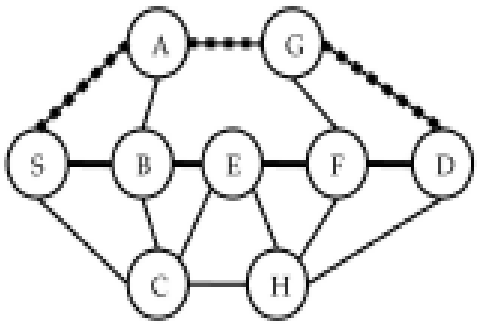

Figure 2.1a: node structure in end to end network

The nodes of entire network comprise S-boxes and multiple keys to encrypt the data. The intermediate nodes such as A,G,B…..(see figure 2.1a) has the power re-encrypt the data by taking permission from master node (S). Here we select the path $P_1 = S \to A \to G \to D$; we assume that the ideal keys are used for encryption process. If the failure rate of the used key falls below a certain level than alternate paths can be used [15-16]. Let us take that A is the weak station that means the encrypted data has been accessed by the hacker at A node. At the same time the node A takes much time re-encrypt the data. In such case it is advisable to use the alternate paths by leaving the node A;

$$P_2 = S \to B \to E \to F \to D$$
$$P_3 = S \to C \to H \to D$$
$$P_4 = S \to B \to C \to H \to D$$
$$P_5 = S \to B \to E \to C \to H \to D$$

Let us start from the path P_2; it includes one additional node therefore it is more time consuming as compared to the path P_1. This will provides more time to the hacker to hack the data. The same problem also exits in paths P_4 & P_5. The only alternate is P_3 has been used in this case; it provides approximately same security level as we achieved in P_1. If alternates paths are selected then they require additional buffer in order to accommodate the incoming stream from node A

From the above factors it has been observed that instead of using alternate path it is more beneficial to provide support to weak station A.

Step 1: To analyze the model; it contains the information about the number of nodes including source and destination.
Step 2: determine the number of S-Boxes and Keys used by individual nodes.
Step 3: determine the failure rate of individual key for each node.
Step 4: if failure rate is high then the re-encrypt the data by using second key.
Step 5: generate the second key from the available data. At the same time support the weak node by arbitrary key in the absence of original key.

In the step 4 it is suggested that the key should generated from the available data. If this has been not done than there is a need to send the key over the secure channel which does not exists in real environment.

(b) Shared segment protection mode

In this mode the shared segmentation method has been used. It includes one additional path between the weak and receiving node. The next node has the power to accommodate the additional data and capable to encrypt the same data with different keys.

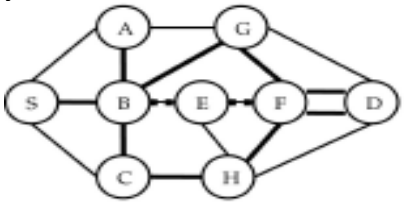

Figure 2.1b: node structure in shared protection mode

The effective nodes are determined by given formula

$$N_{eff} = \frac{number\ of\ \ protected\ \ components}{Total\ \ number\ of\ \ components}$$

In the above model; we will take the polynomial pool based key pre-distribution techniques [3] due to the given advantages: It ensures that the two wireless sensors can establish pair wise keys in order to communicate each other. Secondly, comprised nodes are also accommodated by the techniques. Thirdly, the probability of node failure is directly determined in this scheme. Protection mechanisms for the scheme are classified as $1+1$ *and* $1:1$,$1:N$ *and* $M:N$. Failures can be localized and detected by a notification message to the master node A. For intermediate node failure Key Distribution Centre (KDC) [3] has been used. It is based upon path key management scheme. For n nodes, there are $n-1$ links has been used. The failure rate of each node has been determined on the basis of number of keys, S-Boxes and length of key. We can test the products and audit the procedures to find out misbehavior but we cannot certain to prove that something is secure [11-14]. Therefore efforts are required to upgrade the keys generation mechanism. Detection probability should be kept as minimum as possible, keys generation should be done in a manner that they show high resistance to the hacker [15]. The output distribution of a stage having encrypted data length N with multiple inputs is:

$$F_Y(y)=\sum_{i=1}^{N}\sum_{j=1}^{i}\sum_{k=1}^{i}P(Y=X_{(j)})\times\binom{N}{k}\binom{N-k}{i-k}(-1)^{i-k}F_X^{i}(y)$$

Proof: By using

$$F_j(y)=\sum_{k=1}^{N}\binom{N}{k}F_X^{k}(y)(1-F_X(y))^{N-k}$$

We can write

$$F_Y(y)=\sum_{j=1}^{N}\sum_{k=1}^{N}P(Y=X_{(j)})\times\binom{N}{k}F_X^{k}(y)(1-F_X(y))^{N-k}$$

$$F_Y(y)=\sum_{j=1}^{N}\sum_{k=j}^{N}\sum_{n=0}^{N-k}P(Y=X_{(j)})\binom{N}{k}\times\binom{N-k}{n}(-1)^{N-k-n}F_X^{N-n}(y)$$

$$F_Y(y)=\sum_{j=1}^{N}\sum_{k=j}^{N}\sum_{i=k}^{N}P(Y=X_{(j)})\binom{N}{k}\times\binom{N-k}{i-k}(-1)^{i-k}F_X^{i}(y)$$

Re-arranging the equation, also $N-n=i$

$$F_Y(y)=\sum_{i=1}^{N}\sum_{j=1}^{i}\sum_{k=1}^{i}P(Y=X_{(j)})\times\binom{N}{k}\binom{N-k}{i-k}(-1)^{i-k}F_X^{i}(y)$$

$F_Y(y)$ is the weighted sum of the distribution of the largest order statistics of all the keys whose sizes is less than or equal to N

Table 2.2. latency time and energy consumption for different key and S-Boxes

Operation		Latency(μs)	Energy Consumption (μJ)
Encryption			
Key Size	S-Boxes		
8	8	20.12	21.89
8	16	31.23	29.42
16	8	14.73	22.53
16	16	19.15	39.21
Decryption			
Key Size(Bits)	S-Boxes		
8	8	21.62	21.81
8	16	31.09	22.45
16	8	16.34	15.01
16	16	20.74	39.01

We know that keys are the based upon the mathematical function, there is always a correlation between the various keys. Therefore it is essential to know the dependence of keys with each other.

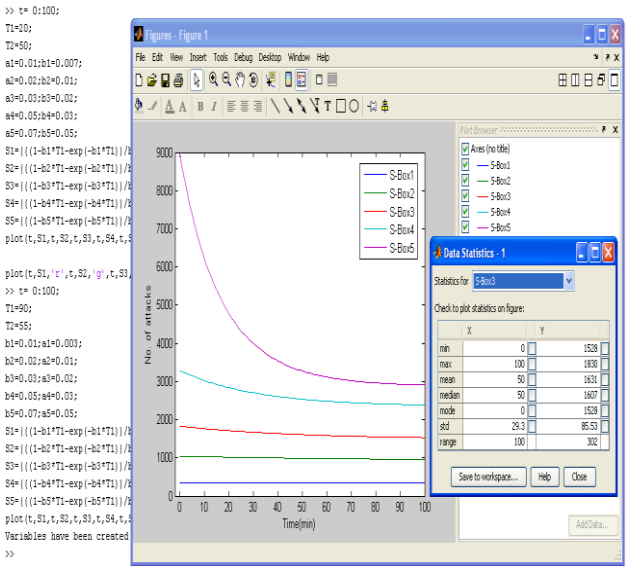

Figure 2.3: determination of failure rate of S-Boxes with 2 keys

The failure rate and data statistics for each S-Box has been determined by using MATLAB 7.3. From the graph it is clear that if the failure rate of the 1st key is less than as compared to the second key then the time available to the hacker will be more to break the model. The strength of all key permutation decreases w.r.t time.

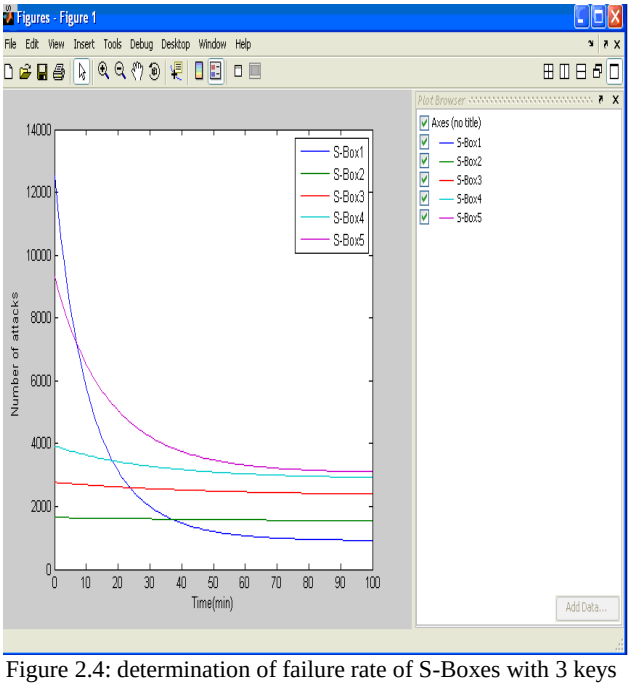

Figure 2.4: determination of failure rate of S-Boxes with 3 keys

Similarly we can able to calculate the failure rate of the other S-Boxes. The failure rates for the same are shown in the tables 2.3-2.7.

Case-1

There are 8 S- Boxes are used which are capable of encrypt the data with dual keys. They keys are based upon mathematical model and all are generated from the available data. Once keys are generated then they are tested by using permutation techniques in order to determine the failure rate of the keys.

Table 2.3. Failure Rate of 1st key is varied from (0.1-0.3); FR of 2nd key increases (0.1-0.8)

	a	b	a	b	a	b	T_1	T_2
S_1	0.1	0.1	0.2	0.1	0.3	0.1	10	50
S_2	0.1	0.2	0.2	0.2	0.3	0.2	10	50
S_3	0.1	0.3	0.2	0.3	0.3	0.3	10	50
S_4	0.1	0.4	0.2	0.4	0.3	0.4	10	50
S_5	0.1	0.5	0.2	0.5	0.3	0.5	10	50
S_6	0.1	0.6	0.2	0.6	0.3	0.6	10	50
S_7	0.1	0.7	0.2	0.7	0.3	0.7	10	50
S_8	0.1	0.8	0.2	0.8	0.3	0.8	10	50

Table 2.4. Failure Rate of 1st key is varied from (0.4-0.6); FR of 2nd key increases (0.1-0.8)

	a	b	a	b	a	b	T_1	T_2
S_1	0.4	0.1	0.5	0.1	0.6	0.1	10	50
S_2	0.4	0.2	0.5	0.2	0.6	0.2	10	50
S_3	0.4	0.3	0.5	0.3	0.6	0.3	10	50
S_4	0.4	0.4	0.5	0.4	0.6	0.4	10	50
S_5	0.4	0.5	0.5	0.5	0.6	0.5	10	50
S_6	0.4	0.6	0.5	0.6	0.6	0.6	10	50
S_7	0.4	0.7	0.5	0.7	0.6	0.7	10	50
S_8	0.4	0.8	0.5	0.8	0.6	0.8	10	50

Table 2.5. Failure Rate of 1st key is varied from (0.7-0.9); FR of 2nd key increases (0.1-0.8)

	a	b	a	b	a	b	T_1	T_2
S_1	0.7	0.1	0.8	0.1	0.9	0.1	10	50
S_2	0.7	0.2	0.8	0.2	0.9	0.2	10	50
S_3	0.7	0.3	0.8	0.3	0.9	0.3	10	50
S_4	0.7	0.4	0.8	0.4	0.9	0.4	10	50
S_5	0.7	0.5	0.8	0.5	0.9	0.5	10	50
S_6	0.7	0.6	0.8	0.6	0.9	0.6	10	50
S_7	0.7	0.7	0.8	0.7	0.9	0.7	10	50
S_8	0.7	0.8	0.8	0.8	0.9	0.8	10	50

In case-2; there failure rate of 2nd key is high for S-Box 1 and it goes on increases as we increases the number of S- Boxes.

Case-2

Here eight S-Boxes are used in which they strength of the keys are determined. The failure rate of 1st key high and the failure rate of second key is less. In the last attempt optimized and reliable combination is shown. In this combination the secured S-5 has been achieved.

Table 2.6. Failure Rate of 1st key is varied from (0.1-0.3); FR of 2nd key decreases (0.8-0.1)

	a	B	a	b	a	B	T_1	T_2
S_1	0.1	0.8	0.2	0.8	0.3	0.8	10	50
S_2	0.1	0.7	0.2	0.7	0.3	0.7	10	50
S_3	0.1	0.6	0.2	0.6	0.3	0.6	10	50
S_4	0.1	0.5	0.2	0.5	0.3	0.5	10	50
S_5	0.1	0.4	0.2	0.4	0.3	0.4	10	50
S_6	0.1	0.3	0.2	0.3	0.3	0.3	10	50
S_7	0.1	0.2	0.2	0.2	0.3	0.2	10	50
S_8	0.1	0.1	0.2	0.1	0.3	0.1	10	50

Table 2.7. Failure Rate of 1st key is varied from (0.1-0.3); FR of 2nd key decreases (0.8-0.1)

	a	B	a	b	a	B	T_1	T_2
S_1	0.4	0.8	0.5	0.8	0.1	0.5	10	50
S_2	0.4	0.7	0.5	0.7	0.1	0.4	10	50
S_3	0.4	0.6	0.5	0.6	0.1	0.3	10	50
S_4	0.4	0.5	0.5	0.5	0.1	0.4	10	50
S_5	0.4	0.4	0.5	0.4	0.1	0.2	10	50
S_6	0.4	0.3	0.5	0.3	0.1	0.4	10	50
S_7	0.4	0.2	0.5	0.2	0.1	0.3	10	50
S_8	0.4	0.1	0.5	0.1	0.1	0.4	10	50

3. CONCLUSION AND FUTURE SCOPE

The efficient selection of key size and number of keys and S-Boxes results in optimized and secured network. Re-routing of the data also provide the secured communication. The failure rate of the keys provides the information about the strength of node. The data statistics are used to make recovery mechanisms active. These are used to recover the data in faculty nodes. The work can be extended if number of keys is increases and the time shifting time is reduced from 0.1 to 0.01 ns.

4. REFERENCES

[1] G. McGraw 2006, Software Security: Building Security In. Addison Wesley.

[2] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu 2004, "Order-Preserving Encryption for Numeric Data," Proc. 2004 ACM Sigmod Conference.

[3] Ruth M. Davis 1997, "The Data Encryption Standard" Proceedings of Conference on Computer Security and the Data Encryption Standard, National Bureau of Standards, Gaithersburg, MD, Feb. 15, NBS Special Publication 500-27, pp 5-9.

[4] W. Stallings 1999, "Cryptography and Network Security: principles and practices, prentice Hall, 2nd edition.

[5] Subbarao V. Wunnava 2002, "Data Encryption Performance and Evaluation Schemes" Proceedings IEEE Southeastcon, pp 234-238.

[6] L. Eschenauer and V.D.Gligor 2002, "A key management scheme for distributed sensor networks" Proceedings of 9th ACM conference on computer and communications security, pp. 41-47

[7] Donggang Liu and Peng Ning 2003, "Establishing pair wise keys in Distributed Networks," CCS,s 03, USA, ACM, October 27-31.

[8] C. Karlof and D. Wagner 2003, "Secure routing in wireless sensor networks: attacks and countermeasures, 1st IEEE international workshop on sensor network protocols and applications.

[9] Xun Yi 2004, "Identity-Based Fault-Tolerant Conference Key Agreement", IEEE Transactions on Dependable and Secure Computing, Vol. 1, No. 3, pp 170-178

[10] Jong Tae Park, Jae Wook Nah, and Wee Hyuk Lee, 2008 "Dynamic Path Management with Resilience Constraints under Multiple Link Failures in MPLS/GMPLS Networks" IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp. 143-154.

[11] Fischlin, M. (2001) "A cost-effective pay-per-multiplication comparison method for millionaires", CT-RSA'01, Volume 2020 of Lecture Notes in Computer Science, Springer, pp.457–472.

[12] G. Ciardo, R.M. Marmorstein, and R. Siminiceanu (2003), "Saturation Unbound", Proceedings of International on Tools and Algorithms for the Construction and Analysis of Systems, pp. 379-393.

[13] H. Chan, A. Perrig, and D. Song (May, 2003), "Random Key Pre distribution Schemes for Sensor Networks," Proceedings of IEEE Symposium on Security and Privacy (S & P '03), pp. 197-213.

[14] J. Muppala, M. Malhotra, and K. Trivedi (1994), "Stiffness-Tolerant Methods for Transient Analysis of Stiff Markov Chains," Microelectronics and Reliability, Vol. 34, No.11, pp. 1825-1841.

[15] Jian Ren, and Lein Harn, (July 2008), "Generalized Ring Signatures", IEEE Transactions on Dependable and Secure Computing, Vol. 5, No. 3, pp153-164.

[16] S. Pradheepkumar, R. Fareedha, M. Jenieferkavetha, A. geanremona and R . Juliajoyce 2010," A Secured Grid Based Route Driven PKC Scheme for Heterogeneous Sensor Network" International Journal of Grid Computing & Applications (IJGCA) Vol.1, No.2, December 2010

[17] Lepakshi Goud. T 2011, "A Routing-Driven Public key Crypto system based key management scheme for a Sensor Network", International Journal of Advanced Engineering Sciences and Technologies, Vol. No. 6, Issue No. 2, 246 - 255