A NEW APPROACH TO ENHANCE SECURITY IN MPLS NETWORK

S.Veni[1] and Dr.G.M.Kadhar Nawaz[2]

[1]Research Scholar, Barathiar University, Coimbatore, India
venii_k@yahoo.com
[2]Director, Dept. of MCA, Sona College of Technology, Salem, India
nawazse@yahoo.com

ABSTRACT

As Multiprotocol Label Switching (MPLS) is becoming a more widespread technology For providing virtual private network (VPN) services, MPLS architecture security is of increasing concern to service providers (SPs) and VPN customers. MPLS suffers from a number of security issues as soon as an attacker successfully penetrates the core. This paper provides an approach to enhance security in MPLS network by integrating a new (k,n) Threshold Secret Sharing scheme with MPLS in which shares obtained are send over multiple disjoint paths. Our approach is implemented to measure time overhead on secrets packet transmission.

KEYWORDS

MPLS, Security, Threshold Secret sharing, LSP.

1. INTRODUCTION

Multi-Protocol Label Switching (MPLS) is a multiservice internet technology based on forwarding the packets using a specific packet label switching technique. The premise of MPLS is to attach a short fixed-length label to the packets at the ingress router of the MPLS domain. The edge routers are called Label Edge Routers (LERs), while routers capable of forwarding both MPLS and IP packets are called Label Switching Routers (LSRs). Packets are forwarded along a Label Switch Path (LSP) where each Label Switch Router (LSR) makes forwarding decisions. Each LSR re-labels and switches incoming packets according to its forwarding table. Label Switching speeds up the packet forwarding and offers new efficient and quick resilience mechanisms. Figure 1 illustrates an MPLS domain. he Label Distribution Protocol (LDP) and an extension to the Resource ReSerVation Protocol (RSVP) are used to establish, maintain, and teardown LSPs [1]. MPLS network architecture does not provide header or payload encryption [2].

MPLS technology has emerged mainly to provide high speed packet delivery. As a result security considerations have not been discussed thoroughly until recent demands for security have emerged by most providers and researchers.

The reason why MPLS does not provide encryption mechanisms is related to the purpose it was built for. In conventional IP networks, every router in the network has a role in analyzing IP packets headers, to classify, and to process every packet passing through it. This of course will add more overhead and delay in the network [3 and 4]. In MPLS network, only two routers (the ingress and egress routers) are responsible for this task. Core or LSR routers in MPLS network will only forward packets based on labels transmitted through a pre established LSP. The use of encryption to provide privacy of data requires the core MPLS routers to analyze and process packets' header, which will result in reducing the performance of MPLS network.

DOI : 10.5121/acij.2012.3308

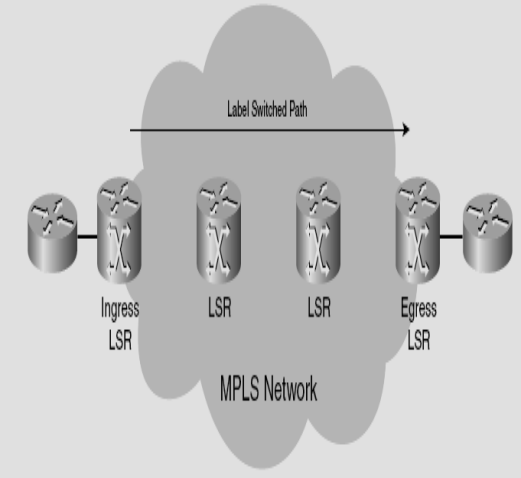

Figure.1 MPLS Domain

This paper considers security based on new Threshold Secret Sharing (TSS) scheme where the shares obtained are send over multiple disjoint paths. The main security issues in MPLS are Confidentiality, Integrity, Modification and fabrication of packet. In this paper we focus on packet confidentiality so that an attacker cannot collect and analyze traffic data or understand routing configuration. Our consideration includes reducing overhead and saving bandwidth of operations.

2. A NEW (K,N) THRESHOLD SECRET SHARING SCHEME

In Shamir's threshold secret sharing scheme a heavy computational cost is required to make shares and recover the secret. A new threshold scheme is proposed by Jun Kurihara[5] et al . For the purpose to realize high performance, the proposed scheme uses just EXCLUSIVE-OR (XOR) operations to make shares and recover the secret. The proposed scheme is a perfect secret sharing scheme, every combination of one or more participants can recover the secret, but every group of less than participants cannot obtain any information about the secret. Moreover, the proposed scheme is an ideal secret sharing scheme similar to Shamir's scheme, which is a perfect scheme such that every bit-size of shares equals that of the secret.

Let $P = \{Pi \mid 0 \leq i \leq n-1, i \in N_0\}$ be a set of n participants. Let $D(\notin P)$ denote a dealer who selects a secret $s \in S$ and gives a share $w_i \in W_i$ to every participant $Pi \in P$, where S denotes the set of secrets, and W_i denotes the set of possible shares that P_i might receive. The access structure $\Gamma(\subset 2P)$ is a family of subsets of P which contains the sets of participants qualified to recover the secret. Especially, Γ of a (k, n)- threshold scheme is defined by $\Gamma = \{A \in 2^P \mid |A| \geq k\}$.

Let S and W_i be the random variables induced by s and w_i, respectively. A secret sharing scheme is perfect if

$$H(S|V_A) = \begin{cases} -0, & A \in \Gamma \\ H(S), & A \notin \Gamma \end{cases} \qquad (1)$$

where $A \subset P$ denotes a subset, and $V_A = \{W_i \mid P_i \in A\}$ denotes the set of random variables of shares that are given to every participant $P_i \in A$. For any perfect secret sharing scheme, the equation $H(S) \leq H(Wi)$ is satisfied [7, 8].Let p(s) and $p(w_i)$ be the probability mass functions of

S and W_i defined as $p(s) = Pr\{S = s\}$ and $p(w_i) = Pr\{W_i = w_i\}$, respectively. In general, the efficiency of a secret sharing scheme is measured by the information rate ρ [6] defined by

$$\rho = \frac{H(S)}{\underset{P_i \in P}{MAX} \; H(W_i)}$$

The maximum possible value of ρ equals one for perfect secret sharing schemes. When the probability distributions on S and W_i are uniform, i.e. $p(s) = 1/|S|$ and $p(w_i) = 1/|W_i|$, the information rate is

$$\rho = \frac{\log_2 |S|}{\underset{P_i \in P}{\max} \; \log_2 W_i}$$

that is, the ratio between the length (bit-size) of the secret and the maximum length of the shares given to participants. A secret sharing scheme is said to be ideal if it is perfect and ρ = 1 [9–11]. Shamir's scheme[12] is recognized as being a typical ideal secret sharing scheme.

This scheme enables to make n shares (distribution) and recover the secret from k or more shares (recovery) using just XOR operations, for arbitrary threshold k and the number of participants n. In this scheme, the secret $s \in \{0, 1\}^{d(n_p - 1)}$ needs to be divided equally into $n_p - 1$ blocks $s_1, s_2, \ldots s_{np-1} \in \{0, 1\}d$, where n_p is a prime number such that $n_p \geq n$, and $d > 0$ denotes the bit-size of every divided piece of the secret.Also, D uses n shares, $w_0, \cdots, w_{n-1}$, of a (k, n_p)-threshold scheme to construct a (k, n)-threshold scheme if the desired number of participants n is a composite number.

Distribution Algorithm

INPUT : $s \in \{0, 1\}^{d(n_p - 1)}$

OUTPUT : $(w_0, \ldots, w_{n-1})$

1: $s_0 \leftarrow 0^d, s_1 \| \ldots. \| s_{n_p - 1} \leftarrow s$

2: for i ← 0 to k – 2 do

3: for j ← 0 to n_p – 1 do

4: $r_j^i \leftarrow GEN(\{0, 1\}^d)$

5: end for

6: end for (discard $r_{n_p - 1}^0$)

7: for i ← 0 to n – 1 do

8: for j ← 0 to n_p – 2 do

9: $w(i,j) \leftarrow \left(\bigoplus_{h=0}^{k-2} r_{h,i+j}^h \right) \oplus s_{j-1}$

10: end for

11: $wi \leftarrow w_{(i,0)} \| \ldots\ldots \| w_{(i,n_p - 2)}$

12: end for

13: return $(w_0, \ldots, w_{n-1})$

To make shares, our (k, n)- threshold scheme requires 3 steps, where line 1, lines 2-6 and lines 6-13 in denote the first, second and third step, respectively: First, D divides the secret s ∈ $\{0, 1\}^{d(np-1)}$ into $n_p - 1$ pieces of d-bit sequence s1, . . . , $s_{np-1} \in \{0, 1\}^d$ equally at line 1, where s_0 denotes a d-bit zero sequence, i.e. $s_0 = 0^d$ and $s_0 \oplus a = a$. We call this d-bit zero sequence a singular point' of divided pieces of the secret.1 Next, at lines 2–6, $(k - 1) n_p - 1$ pieces of d-bit random number r_0^0, r_{np}^0 -2, r_0^1, r_{np-1}^1 , ……., r_0^{k-2}, …..r_{np-1}^{k-2} are chosen from $\{0, 1\}^d$ independently from each other with uniform probability $1/2^d$, where GEN(X) denotes a function to generate an ($\log_2 |X|$)-bit random number from a finite set X. Finally, D concatenates these pieces and constructs shares $w_i = w(i,0) \| \ldots \| w(i,n_p-2)$, and sends shares to each participant through a secure channel. If $n < n_p$, lines 7–12 does not work for $0 \le i \le np - 1$ but it does for $0 \le i \le n - 1$, and hence D does not generate $n_p - n$ shares $w_n, \cdots, w_{np-1}$. Thus, it is possible to add new participants $P_n, \cdots, P_{np-1}$ after distribution by generating wn, · · · ,wnp−1 anew as necessary. However, to generate new shares, k existing shares should be gathered, and all random numbers and the secret should be stored.

Recovery Algorithm

INPUT : (w_{t_0} , w_{t_1} , ……..$w_{t_{k-1}}$)

OUTPUT : s

1: for i ← 0 to k – 1 do

2: $w_{(t_{i,0})} \| \ldots\ldots \| w_{(t_{i,n_{p-2}})} \leftarrow w_{t_i}$

3: end for

4: w ← $(w_{(t_{0,0}} \ldots\ldots w_{(t_{0,n_p-2})} \ldots\ldots w_{(t_{k-1,0})} \ldots\ldots w_{(t_{k-1,n_p-2})})^T$

5: M ← MAT($t_0, \ldots, t_{k-1}$)

6: $(s_{1,\ldots} s_{n_p-1})^T \leftarrow$ M.w

7: s ← $s_1 \| \ldots\ldots\ldots \| s_{n_p-1}$

8: return s

First, each share is divided into d-bit pieces at lines 1–3. Next, at line 4, $k(n_p-1)$ dimensional vector w is generated, which is a vector of divided pieces of shares. At line 5, $k(n_p - 1) \times k(n_p - 1)$ binary matrix M is obtained by the function MAT(). All divided pieces of the secret, s_1 , ……..$s_{n_p\ 1}$ are recovered by calculating M·w at line 6. Finally, the secret s is recovered by concatenating s_1 , ……..s_{n_p-1} at line 7.

3. SIMULATION AND PERFORMANCE ANALYSIS

In this section, we evaluate the efficiency of new scheme by comparing it with Shamir's scheme. First, we show the result of computer simulation by implementing both new scheme and Shamir's. We compared the proposed scheme with that of Shamir's for (k, n) = (3, 11), (3, 59), (3, 109), (5, 11), (10, 11) and (10, 23) by implementation on a PC, where every scheme is implemented for n = np. Fig.1 denotes the processing time required to make n(= n_p) shares from 4.5 MB data (secret) and recover the 4.5 MB secret from k shares, $w_0, \cdots, w_{k-1}$ by using new scheme and Shamir's scheme. For the implementation of Shamir's scheme, SSSS Version 0.5[19] is used ,which is a free software licensed under the GNU GPL. In Fig.1, the horizontal axis and vertical axis denote pairs of threshold and the number of participants, i.e. (k, n), and the processing

time, respectively. This graph shows that new scheme performed processing much faster than Shamir's. In (3, 11)-threshold schemes, new scheme was more than 900-fold faster than Shamir's in terms of both distribution and recovery. Similarly, in (3, 59), (3, 109), (5, 11), (10, 11) and (10, 23)-threshold schemes, Fig.2 shows that new scheme achieved far more rapid processing than Shamir's.

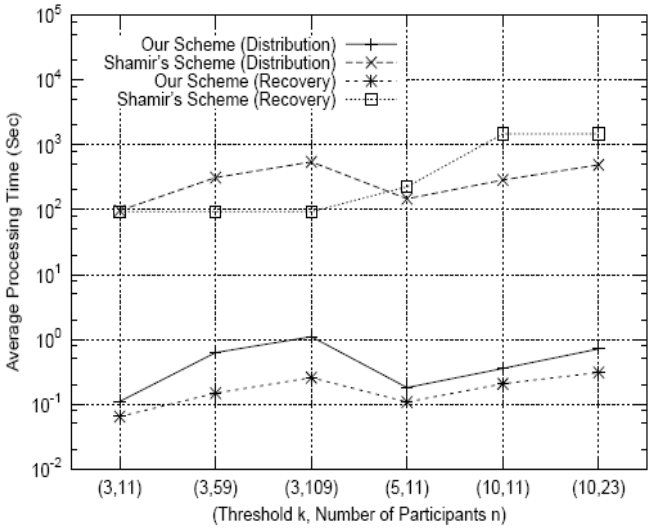

Fig: 2 Distribution and Recovery Processing Time for n=n p

4. CONCLUSIONS

In this paper, we integrated new (k, n)-threshold secret sharing scheme in MPLS which uses just XOR operations to make shares and recover the secret, and we proved that the proposed scheme is an ideal secret sharing scheme. We estimated the computational cost in new scheme and Shamir's scheme for values of k and n.

REFERENCES

[1] E. C. Rosen, A. Viswanathan, and R. Callon, (2001), "Multiprotocol label witching architecture", RFC 3031.

[2] S. Alouneh, A. En-Nouaary, and A. Agarwal( ), MPLS security: an approach for unicast and multicast environments.

[3] J. Chung, "Multiple LSP Routing Network Security for MPLS Networking," IEEE-MWSCAS, 2002.

[4] T. Saad, B. Alawieh and H. Mouftah, (2006), "Tunneling Techniques for Endto- End VPNs: Generic Deployment in an Optical Testbed Environment", IEEE Communication Magazine.

[5] Jun Kurihara, Shinsaku Kiyomoto, Kazuhide Fukushima and Toshiaki Tanaka(2008), "A New (k,n)-Threshold Secret Sharing Scheme and Its Extension", ISC '08 Proceedings of the 11th international conference on Information Security.

[6] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, (1993), "On the information rate of secret sharing schemes," Proc. CRYPTO '92, LNCS 740, Springer-Verlag, pp.149– 169.

[7] E. D. Karnin, J. W. Greene, and M. E. Hellman, (1983), "On secret sharing systems," IEEE Trans. Inform. Theory, vol.29, no.1, pp35–41.

[8] R. M. Capocelli, A. De Santis, L. Gargano, and U. Vaccaro, (1983), "On the size of shares for secret sharing schemes," J. Cryptology, vol.6, pp.35–41.
[9] C. Blundo, A. De Santis, L. Gargano, and U. Vaccaro, (1993), "On the information rate of secret sharing schemes," Proc. CRYPTO '92, LNCS 740, Springer-Verlag, pp.149– 169.

[10] D. R. Stinson, (1994), "Decomposition constructions for secret sharing schemes", IEEE Trans. Inform. Theory, vol.40, no.1, pp.118–125.

[11] D. R. Stinson, (1995), Cryptography: Theory and Practice, CRC Press, Florida.

[12] A. Shamir, (1979), "How to share a secret," Commun. ACM, vol.22, no.11, pp.612–613, 1979.

Authors

S.Veni is presently working as a Assistant Professor in the Department of MCA, Karpagam University, Coimbatore. She has eight years of teaching experience. She has participated and presented ten papers in national conferences and two papers in International conferences. Her area of research includes network architecture and network protocols.

Dr.G.M.Kadhar Nawaz is presently working as Director in the Department of Computer Applications, Sona College of Technology, Salem. He has presented and published papers in various national and international Conferences and journals. He has also organized national conferences. He completed Ph.D in Computer Science from Periyar University and his area of research includes Digital image Processing and Stegnography.