Malaysian Journal of Computer Science, Vol. 16 No. 1, June 2003, pp. 68-76

PERFORMANCE ANALYSIS ON SECURITY ASSOCIATION IN HIGH SPEED ATM NETWORKS

W. H. Cheong, T. C. Ling, Mashkuri Hj. Yaacob and K. K. Phang
Faculty of Computer Science and Information Technology
University of Malaya, Kuala Lumpur, Malaysia
email: hon@pc.jaring.my
tchaw@um.edu.my
mashkuri@um.edu.my
kkphang@.um.edu.my

ABSTRACT

The ATM Forum has released an ATM Security Specification that contains the requirements and specifications of security support services. The ATM Security Specification suggests placing all the security features in the user plane, control plane, management plane, ATM adaptation layer and ATM layer of ATM network architecture. Implementing security features in these planes and network layers will introduce extra overhead on data transmission. The key reason is that security options, algorithms, and key lengths have to be negotiated via Security Message Exchange (SME) before any security services can be provided. This paper aims to carry out performance analysis to determine the cell throughput and SME setup time for different sets of security association topologies. For this purpose, security support services are implemented and integrated with the NIST ATM/HFC Network Simulator. From this performance testing, the specific security association topology that provides the best performance could be selected.

Keywords: Security Association, ATM Networks, Security Message Exchange (SME)

1.0 INTRODUCTION

The ATM Security Specification [1] has specified that the features needed for the security support services are as follow:

- Security message exchange protocols and basic negotiation
- Security messaging in the control plane
- Security messaging in the user plane
- Key exchange
- Session key update
- Certification infrastructure

Messages must be exchanged between the involved security agents (SAs) in order to perform many of the security services as described in the previous section. A mechanism for negotiation of security options is also provided by the security message exchange (SME). It is important to provide a variety of security services, algorithms, and key lengths, which meet a wide range of security needs since security requirements vary among organisations. Therefore, the ATM security mechanisms should support multiple security services, algorithms, and key lengths. SME provide negotiation of common security parameters such as algorithms and key lengths as part of the security establishment procedure for the VC so that SA could agree on these parameters to be used for the security services. There are two methods for security message exchange. They are message exchange within UNI 4.0 signaling and in-band message exchange.

The security message exchange and basic negotiations form security associations among security agents. A security association is the distributed contextual information (e.g. cryptographic algorithm, mode of operation, optional features enabled, etc.) controlling the nature of the security service to be provided for a given VC.

Key exchange is the mechanism by which two security agents exchange secret keys for use by the confidentiality and integrity services. Authentication service is often tied with the key exchange in order to protect against "man in the middle" attacks. For these to be accomplished, "confidential" key exchange parameters are included within the authentication flows. There are many optional methods to perform key exchange. It could be performed with

either symmetric (secret key) or asymmetric (public key) algorithms. It could also be either be bi-directional (two-way), or uni-directional (one-way).

User plane confidentiality and integrity services over an ATM virtual circuit uses session key directly for encryption and decryption. It is critical that keys be periodically changed to avoid "key stream re-use" due to the potentially high data rate of the virtual circuit.

In public key cryptography, a public and private key are created simultaneously using the same algorithm (a popular one is known as RSA) by a certificate authority (CA). The private key is given only to the requesting party and the public key is made publicly available as part of a digital certificate in a directory that all parties can access. The private key is never shared with anyone or sent across the Internet. A person's private key is used to decrypt text that has been encrypted with the same person's public key by someone else who can find out the person's public key from a public directory. Thus, if A send B a message, A can find out B's public key (but not B's private key) from a central administrator and encrypt a message to B using B's public key. When B receives it, B decrypts it with B's private key. In addition to encrypting messages which ensures privacy, B can authenticate A so B know that it is really A who sent the message by using A's private key to encrypt a digital certificate. When B receives it, B can use A's public key to decrypt it.

This paper aims to carry out performance analysis to determine the cell throughput and SME setup time for different sets of security association topologies. For this purpose, security support services are implemented and integrated with the NIST ATM/HFC Network Simulator.

2.0 EMPIRICAL STUDY

The performance tests would emphasize on the throughput (number of cells received within a certain period) and the SME setup time of Constant Bit Rate (CBR) data from one end system to another end system. CBR data is chosen because this would make sure that there is no other priority data, which could affect the cell throughput.

Besides the type of data and the security association topology, there are other variables, which could affect the cell throughput. These include:

- Encryption time
- Security Algorithms
- Switches configuration
- Data congestion
- Distances between every nodes
- Rate of CBR data
- Virtual connection route

Thus, it is important to make sure that all these configurations are the same for every test so that the only variable, which could affect the cell throughput and SME setup time, is the security association topology chosen.

For the encryption time, the Rijndael algorithm's encryption time is used. Although Rinjndael is not supported by the ATM Forum's security specification [1], the encryption time is used for the reason that this algorithm has been chosen as the new proposed US government Advance Encryption Standard (AES) for protecting sensitive, unclassified US government data [2]. The Rinjndael algorithm has the best combination of security, performance, efficiency, ease of implementation and flexibility [2, 3]. It is set to replace the aging Data Encryption Standard (DES) adopted in 1977. The time needed for encryption with 128-bit keys on Pentium-Class CPU is 58 clocks per Byte [3, 4]. Therefore encryption time for 48 bytes ATM cell payload on a machine running at 400 MHz would take:

$$\frac{53 \times 48 \text{ clocks cycle}}{400 \text{ MHz}} = 6.36 \text{ micro seconds}$$

A 128-bit key encryption is used, as this is the fastest and will provide adequate security for virtually any application for the next several decades at least [5].

There are multiple ways to setup security associations for a virtual connection, which has three SAs. These are all depicted in Fig. 1. Table 1 and Fig. 2 show the throughput result and chart respectively for each of the topologies that has three SAs. Table 2 lists the SME setup time for these topologies.

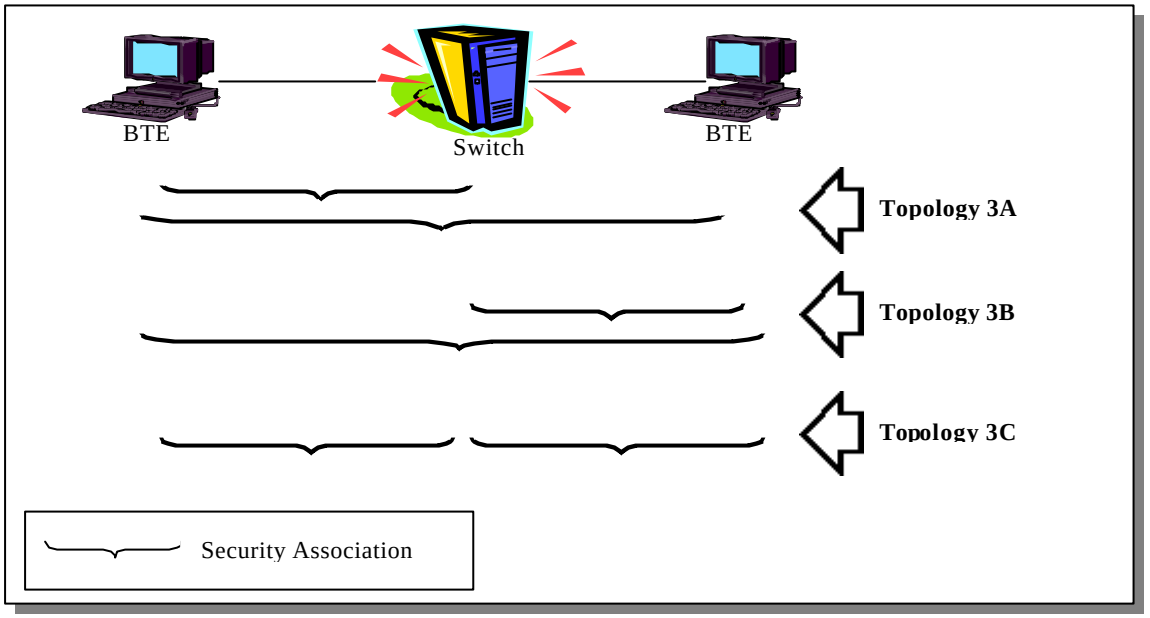

Fig. 1: Security Association Topologies for Three SAs

Table 1: Throughput Result for Security Associations with Three SAs

Topology	**Cell Throughput**									
	0.1s	**0.2s**	**0.3s**	**0.4s**	**0.5s**	**0.6s**	**0.7s**	**0.8s**	**0.9s**	**1.0s**
Topology 3A	707	1887	3067	4247	5427	6607	7787	8967	10147	11327
Topology 3B	707	1887	3067	4247	5427	6607	7787	8967	10147	11327
Topology 3C	802	1982	3162	4342	5522	6702	7882	9062	10242	11422

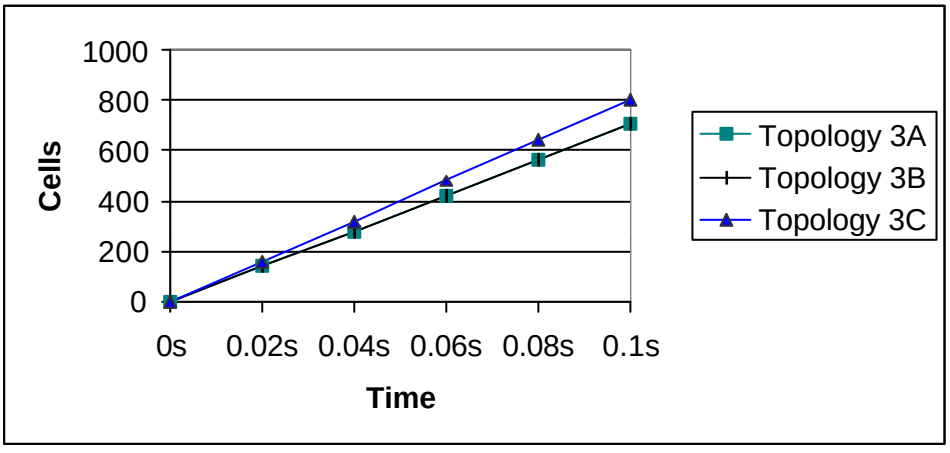

Fig. 2: Throughput Chart for Security Associations with Three SAs

Table 2: SME Setup Time for Security Associations with Three SAs

Topology	SME Setup Time (micro seconds)
Topology 3A	40062
Topology 3B	40062
Topology 3C	32031

It is clearly noticeable that each test value is recorded only once in all tables shown in this section. This is because repeated tests for each topology produces exactly the same results.

The same performance tests are then carried out on network configuration with four SAs followed by five SAs. Fig. 3 depicts the possible security association topologies for a virtual connection with four SAs. The performance test results for all these topologies are recorded in Table 3, Table 4 and Fig. 4. Fig. 5 depicts the possible security association topologies for a virtual connection with five SAs and their test results are shown in Table 5, Table 6 and Fig. 6.

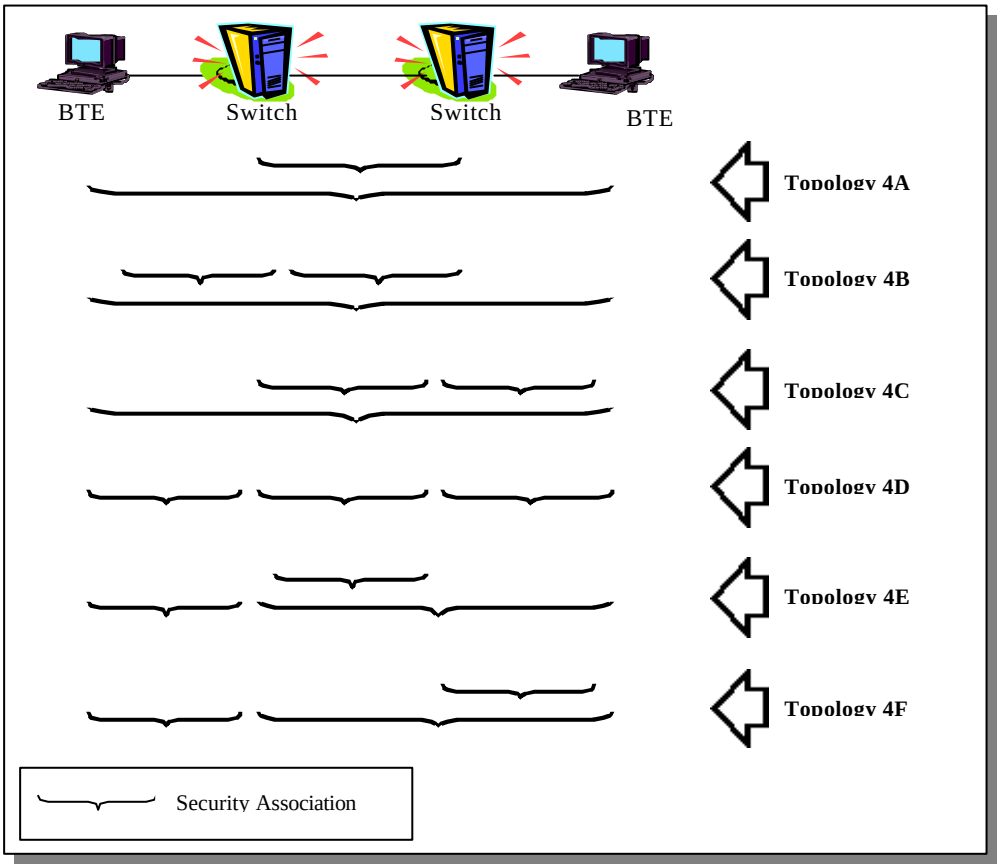

Fig. 3: Security Association Topologies for Four SAs

Table 3: Throughput Result for Security Associations with Four SAs

Topology	Cell Throughput									
	0.1s	0.2s	0.3s	0.4s	0.5s	0.6s	0.7s	0.8s	0.9s	1.0s
Topology 4A	707	1887	3067	4247	5427	6607	7787	8967	10147	11327
Topology 4B	707	1887	3067	4247	5427	6607	7787	8967	10147	11327
Topology 4C	707	1887	3067	4247	5427	6607	7787	8967	10147	11327
Topology 4D	802	1982	3162	4342	5522	6702	7882	9062	10242	11422
Topology 4E	801	1981	3161	4341	5521	6701	7881	9061	10241	11421
Topology 4F	801	1981	3161	4341	5521	6701	7881	9061	10241	11421

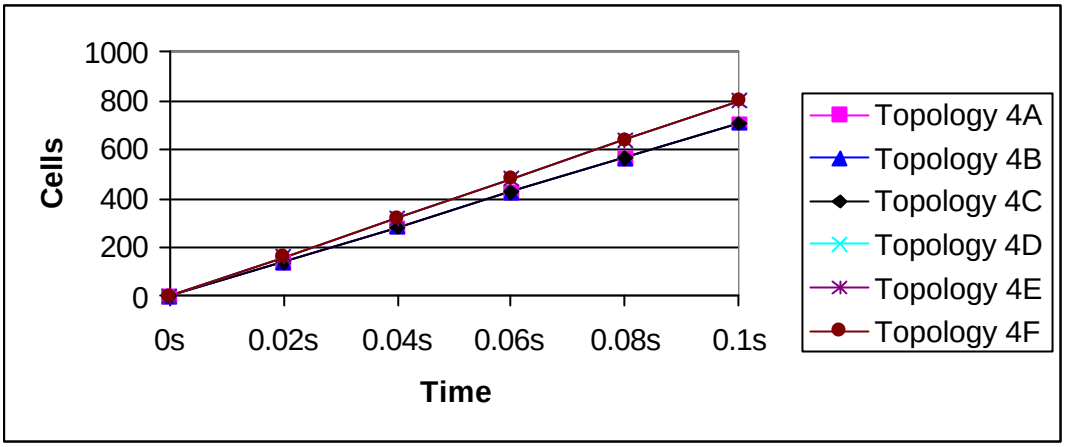

Fig. 4: Throughput Chart for Security Associations with Four SAs

Table 4: SME Setup Time for Security Associations with Four SAs

Topology	SME Setup Time (micro seconds)
Topology 4A	40093
Topology 4B	40093
Topology 4C	40093
Topology 4D	32031
Topology 4E	32062
Topology 4F	32062

Table 5: Throughput Result for Security Associations with Five SAs

Topology	Cell Throughput									
	0.1s	0.2s	0.3s	0.4s	0.5s	0.6s	0.7s	0.8s	0.9s	1.0s
Topology 5A	706	1886	3066	4246	5426	6606	7786	8966	10146	11326
Topology 5B	706	1886	3066	4246	5426	6606	7786	8966	10146	11326
Topology 5C	801	1981	3161	4341	5521	6701	7881	9061	10241	11421
Topology 5D	801	1981	3161	4341	5521	6701	7881	9061	10241	11421
Topology 5E	801	1981	3161	4341	5521	6701	7881	9061	10241	11421
Topology 5F	801	1981	3161	4341	5521	6701	7881	9061	10241	11421
Topology 5G	801	1981	3161	4341	5521	6701	7881	9061	10241	11421
Topology 5H	802	1982	3162	4342	5522	6702	7882	9062	10242	11422
Topology 5I	802	1982	3162	4342	5522	6702	7882	9062	10242	11422

Table 6: SME Setup Time for Security Associations with Five SAs

Topology	SME Setup Time (micro seconds)
Topology 5A	40125
Topology 5B	40125
Topology 5C	32093
Topology 5D	32093
Topology 5E	32093
Topology 5F	32062
Topology 5G	32062
Topology 5H	32031
Topology 5I	32031

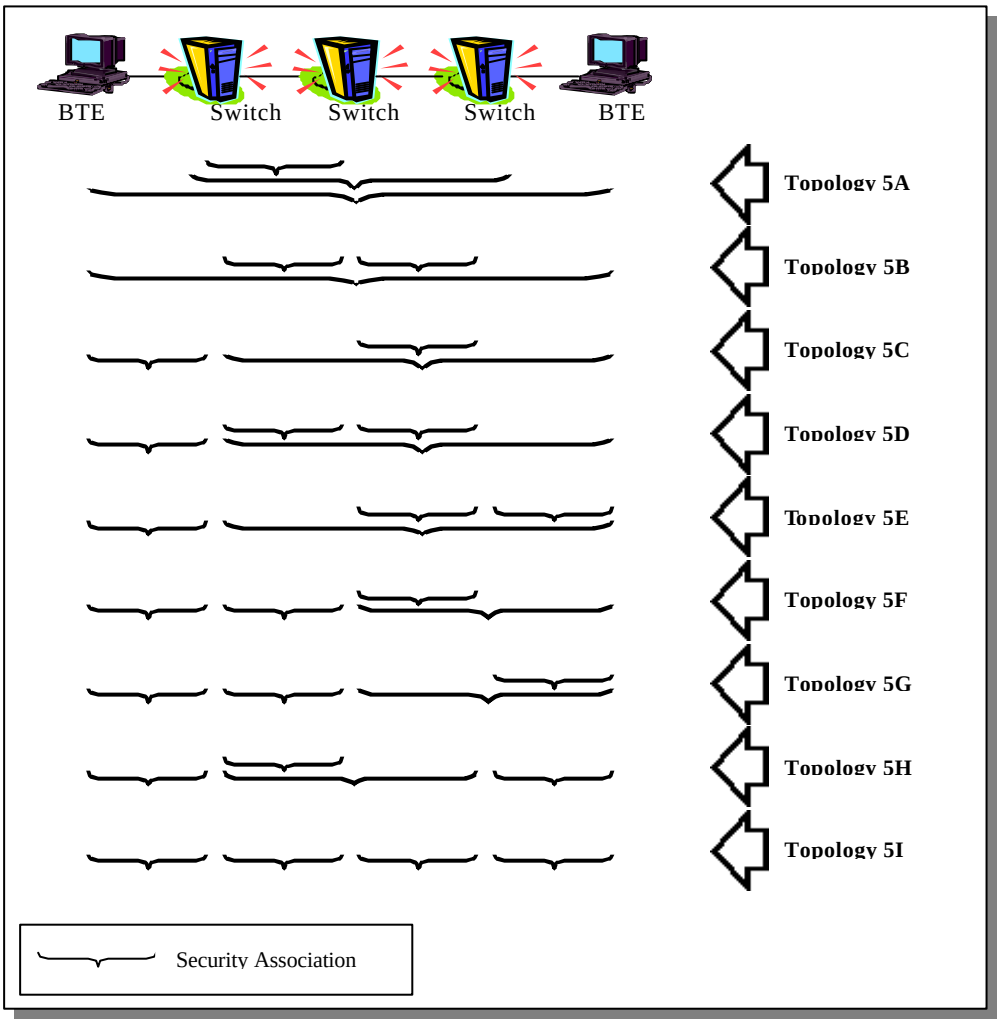

Fig. 5: Security Association Topologies for Five SAs

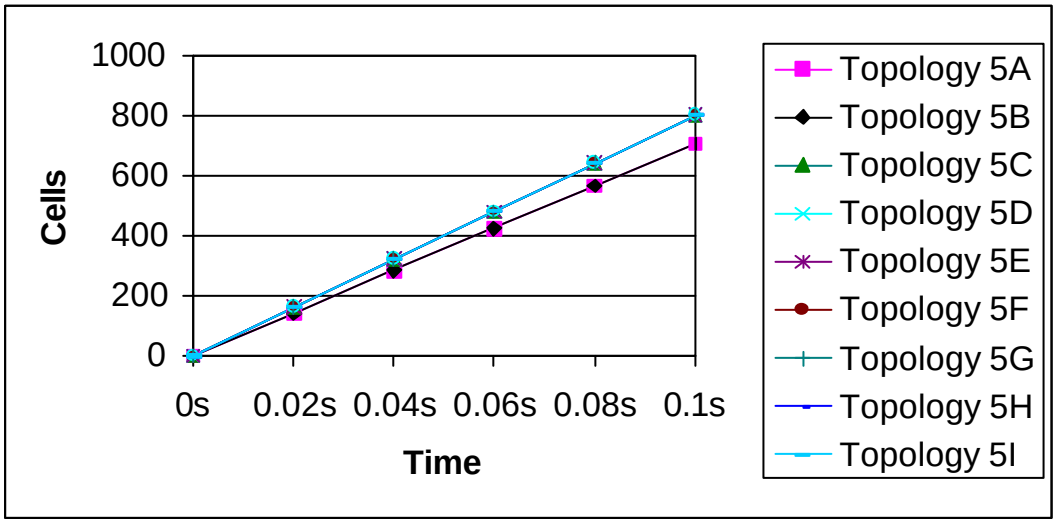

Fig. 6: Throughput Chart for Security Associations with Five SAs

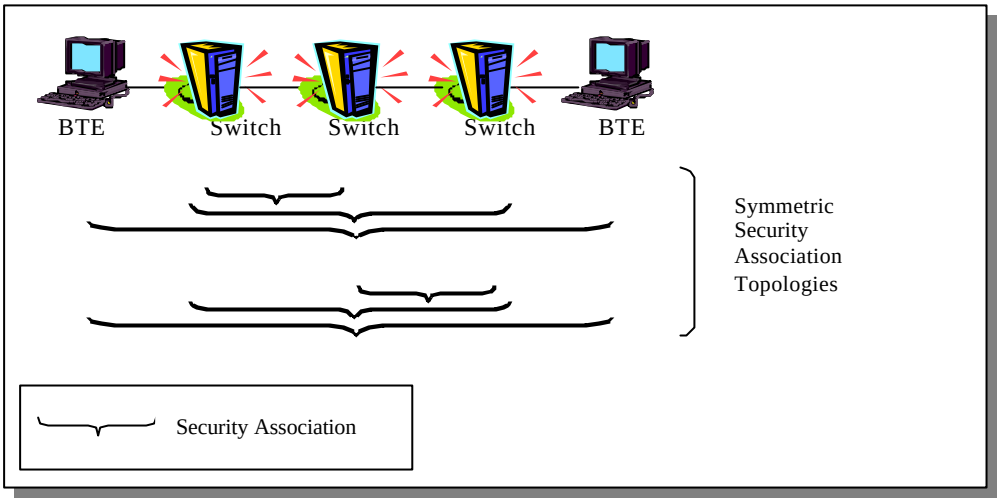

Fig. 7: Symmetric Security Association Topologies

For virtual connections which have five SAs, not all possible security association topologies are tested because there are many topologies that are symmetric to each other. An example of these symmetric security association topologies is shown in Fig. 7. If every node in the virtual connection has identical configurations, both topologies, which are symmetric to each other would produce the same result. Thus, only one of the topologies that are symmetric is tested.

3.0 ANALYSIS OF RESULT

The empirical study results show that the cell throughput of each topology decrease if the SME setup time increase. Cell throughputs are similar for every topology, which has the same SME setup time. Although the number of security associations are different for two different topologies, cell throughput for both the topologies would be the same if their SME setup time are the same. Examples are Topology 4A, Topology 4B and Topology 4C; Topology 5A and Topology 5B; as well as Topology 5C, Topology 5D and Topology 5E. These security association topologies could be referred from Fig. 2, Fig. 4 and Fig. 6. Even if the number of SAs for a few security association topologies are different, the same SME setup time would also produce the same cell throughput. Examples for these topologies are Topology 3C, Topology 4D and Topology 5I. There are 3 SAs, 4 SAs and 5 SAs in these topologies respectively, but their cell throughputs are the same.

This proved that cell throughput would not be affected by security services if the encryption time is shorter than the time needed to send the same amount of data with a fix CBR. The data rate for every performance tests that has been carried out is 5 Megabits per second. So, the time needed to send 48 bytes of data would be:

$$\left(\frac{48 \text{ bytes X } 8}{10^6} \text{ X } \frac{1}{5 \text{ Mbits/s}} \text{ X } 10^6 \right) = \textbf{76.8 micro seconds}$$

As stated in the previous section, encryption time for 48 bytes of data is 6.36 micro seconds, which is shorter than the time needed to send 48 bytes of data with data rate equals to 5 Megabits per second. Other dependencies that could affect the cell throughput are encryption time, security algorithms, switches configuration, data congestion, distances between every nodes, rate of CBR data and virtual connection route. All testing done on different topologies are setup using the same configurations for the listed dependencies.

Therefore, only SME setup time is taken into consideration to find the security association topology with the best performance. From the empirical study results, Topology 3C has the shortest SME setup time compared with all topologies that have three SAs. For security association topologies, which have four SAs and five SAs, Topology 4D and Topology 5I have the shortest SME setup time respectively. Topology 3C, Topology 4D and Topology 5I are security association topologies that have only non-overlapping security associations for all SAs.

Table 2 shows that topology 3A and topology 3B have the same SME setup time which are greater than the setup time for topology 3C. This is because topology 3A and topology 3B have a security association which passes through a network component, a switch in this case, while all security associations for topology 3C take the shortest route. The same trend is displayed for topologies that have three and four SAs. The longer the route taken for a security association, the longer it would take for SME setup. This revealed that all security associations in a network topology should select the shortest route in order to provide the best performance. In another words, topology that has non-overlapping security associations for every SAs would have the best performance.

4.0 CONCLUSION

The performance testing and analysis on security association in ATM network topologies have been successfully carried out. With the completion of this testing and analysis, the security association topology that provides the best performance was determined. This enables security associations that are required to be dynamically setup to select the best association in terms of performance.

REFERENCES

[1] The ATM Forum Technical Committee, "ATM Security Specification Version 1.0". *The ATM Forum/AF-SEC-0100.000*, Feb 1999.

[2] Philip Bulman, "Commerce Department Announces Winner of Global Information Security Competition". *NIST Press Release, G 2000-176*, 2 October 2000.

[3] B. Schneier and D. Whiting, "A Performance Comparison of the Five AES Finalists". *Third AES Candidate Conference*, 2000.

[4] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Performance Comparison of the AES Submissions". *Second AES Candidate Conference*, April 1999.

[5] The ATM Forum Technical Committee, "ATM Security Framework 1.0". *The ATM Forum/AF-SEC-0096.009*, 1998.

[6] G. N. Cohen, B. Kamenel, C. M. Kubic, Military Communications Conference, "Security for Integrated IP-ATM/Tactical-Strategy Network". *MILCOM '96, Conference Proceedings, IEEE Volume: 2*, 1996, pp. 456-460, Vol. 2.

[7] Donglin Liang, "A Survey on ATM Security". *Ohio State University Student Report*, 1999.

[8] Stevenson, N. Hillery and G. Byrd, "Secure Communications in ATM Networks Communications". *ACM, Volume 38, No. 2*, Feb, 1995, pp. 45-52.

[9] M. Peyravian and T. D. Tarman, "Asynchronous Transfer Mode Security". *IEEE Network Volume: 11 3*, May-June 1997, pp. 34-40.

BIOGRAPHY

W. H. Cheong obtained both his B.Comp Sc and M.Comp Sc from University of Malaya. He is currently a consultant for an IT company.

T. C. Ling obtained both his B.Sc and M.Comp Sc from University of Malaya. He is currently a lecturer at the Faculty of Computer Science and Information Technology, University of Malaya. His research interests is QoS in high speed network.

Mashkuri Hj. Yaacob is Professor of Computer Science of the Faculty of Computer Science and Information technology, University of Malaya. His research includes computer architecture and high speed networking.

K. K. Phang obtained both his B.Sc and M.Comp Sc from University of Malaya. He is currently a lecturer at the Faculty of Computer Science and Information Technology, University of Malaya. His research interests is QoS routing in high speed network.