ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Computer Communications 28 (2005) 1317–1336

computer communications

www.elsevier.com/locate/comcom

A modeling and simulation methodology for analyzing ATM network vulnerabilities

Aparna Adhav[a], Tony S. Lee[b], Sumit Ghosh[c,*]

[a]Cisco Systems, 225 East Tasman Drive, San Jose, CA 95134, USA
[b]Yahoo! Inc., 701 First Avenue, Sunnyvale, CA 94089, USA
[c]SENDLAB, Department of ECE, Stevens Institute of Technology, Hoboken, NJ 07030, USA

Received 25 August 2004; revised 29 January 2005; accepted 31 January 2005
Available online 3 March 2005

Abstract

The design of complex asynchronous distributed systems including ATM networks is in itself quite challenging and designers rarely expend either the time or energy to consider how unexpected changes in the operating environment may affect the reliability of the system, let alone take into consideration imaginative ways in which a clever perpetrator may maliciously cause the system to fail, often catastrophically. While the occurrence and impact of attacks launched against telephone networks, store-and-forward networks such as the Internet, and the power grid, are widely reported in the news media, a systematic analysis of these attacks in the scientific literature is lacking. This paper is the first to propose the use of modeling and asynchronous distributed simulation as a systematic methodology to uncover vulnerabilities in complex ATM networks. The approach is demonstrated in two steps. In step 1, a few complex attacks are identified, which while based on the principles of ATM networking, are representative of those that would be construed by intelligent enemy agents. An attack is viewed as a perturbation of an operationally correct ATM network and may be classified under two broad categories. The first attack type focuses on failing specific, standard functions in ATM networks while the second category of attacks refers to the prescription of a malicious intent or objective. Under step 2, the attacks are modeled utilizing a representative ATM network and analyzed through a simulation utilizing an asynchronous, distributed, and accurate ATM simulator, that executes on a network of Pentium workstations under Linux, configured as a loosely-coupled parallel processor. Thus, the environment underlying the evaluation of the vulnerabilities reflect reality, implying, in turn, realistic results. In addition to revealing the weaknesses, the findings of this methodology may serve as a guide to either redesigning the ATM network and eliminating the vulnerabilities or synthesizing a sentinel that conceptually surrounds and protects from network from attacks. While the methodology is generalizable to ATM-like MPLS network and future network designs, it is beyond the scope of this paper.

Keywords: ATM network; Vulnerabilities; Security breaches; Threat scenarios; Catastrophic failures

1. Introduction

While fault simulation and test generation tools [1] have been in practice for over two decades in the field of computer-aided design of VLSI and digital systems to identify design and manufacturing errors in hardware systems, they were primarily confined to synchronous system designs subject to a centralized clock. In contrast, the approach proposed in this paper applies to complex asynchronous distributed systems where individual entities are driven by their own independent clocks and interact asynchronously with one another.

As complex systems, networks consist of a number of constituent elements that are geographically dispersed, are semi-autonomous in nature, and interact with one another and with users, asynchronously. Given that the network design task is already intrinsically complex, it is natural for the traditional network designer to focus, in order to save time and effort, only on those principles and interactions, say D, that help accomplish the key design objectives of the network. The remainder of the interactions, say U, are viewed as “don’t cares” or passive, bearing no adverse impact under normal operating conditions. In reality, however, both internal and external stress may introduce

[*] Corresponding author. Tel.: +1 201 216 5658; fax: +1 201 216 8246.
E-mail addresses: tlee@yahoo-inc.com (T.S. Lee), sghosh2@stevens.edu (S. Ghosh).

0140-3664/$ - see front matter © 2005 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2005.01.018

abnormal operating conditions into the network under which the set U may begin to induce any number of unintended effects, even catastrophic failure. A secure network design must not only protect its internal components from obvious attacks from the external world, but, and this is equally important, resist internal attacks from two sources, foreign elements that successfully penetrate into the network and attack from within and one or more of the internal components that spin out of control and become potentially destructive. This section introduces the notion of network vulnerability analysis, conceptually organized into three phases. Phase I focuses on systematically examining every possible interaction from the perspective of its impact on the key design objectives of the network, and constitutes an indispensable element of secure network design. Given that the number of interactions in a typical real-world network is large, to render the effort tractable, phase I must be driven from a comprehensive and total understanding of the fundamental principles that define the network. Phase I is likely to yield a nonempty set of potential scenarios under which the network may become vulnerable. In phase II, each of these weaknesses is selected, one at a time, and where, possible, a corresponding attack model is synthesized. The purpose of the attack model is to manifest the vulnerability through an induced excitement and guide its effect at an observable output. The attack model assumes the form of a distinct executable code description, encapsulating the abnormal behavior of the network, and assumes an underlying executable code description that emulates the normal network behavior. In phase III, the attack models are simulated, one at a time, on an appropriate testbed, with two objectives. First, the simulation verifies the thinking underlying the attack model, i.e. whether the attack model succeeds in triggering the vulnerability and forcing its manifestation to be detected at an observable output. When the first objective is met, the simulation often reveals the impact of the attack model on network performance. Under the second objective, the extent of the impact is captured through an innovative metric design.

The remainder of the paper is organized as follows. Section 2 is a brief review of the current literature on attack models. Section 3 presents the fundamental ATM network principles that form the basis for launching the vulnerability analysis. Section 4 focuses on vulnerability analysis and synthesis of the attack models intended to expose the vulnerabilities. Section 5 presents details on the assessment of the attacks through modeling and asynchronous distributed simulation on ATMSIM 1.0 [2] and the lessons learned for hardening ATM networks in the future.

2. Brief review of the current literature on attack models

A careful examination of the literature on attack models for networking reveals that nearly all efforts focus on store-and-forward networks [3]. The literature also reveals the lack of a systematic analysis of the vulnerability of data networks from basic principles. As a result, both a set of basic attacks derived from the vulnerability analysis and an approach to validate such attacks are missing in the literature. Virtually all of the reported efforts, except for [4], are ad hoc, lack systematic modeling and analysis, and do not support efforts to use them to harden networks. Since, the Internet, the most well-known store-and-forward network has been around the longest, the literature contains a rich set of documented methods to launch attacks on the Internet as well as a collection of clever techniques to defeat them. These include:

- Denial of service attack via PING: a denial of service attack via PING occurs when oversized IP packets are transmitted inadvertently or intentionally via PING. Given that the maximum packet size in TCP/IP is set at 65,536 bytes, when confronted with oversized IP packets, networks may react in unpredictable ways including crashing, freezing, or rebooting of the system.
- Password breaking: though crucial to system security, system files such as/etc/passwd are normally readable by all users, tempting perpetrators to attempt to break the encrypted information stored in these files.
- TCP Wrapper: the proposed enhancement permits the system administrator to selectively reject requests for services such as ftp, rsh, and rlogin from suspicious sources.
- Data encryption: as a logical step, sensitive data may be encrypted to defeat unauthorized tapping and access by intruders.
- Firewalls: the philosophy underlying firewalls is to shield the network from the external world and concentrate attacks at a single point that can be effectively monitored by the network management.
- Trojan horse: the concept of Trojan horse attacks refers to the technique of secretly implanting hostile entities in a network. Thus, in theory, unless a system is designed and implemented completely by one trusted individual, the system does not and should not lend itself to 100% trust. Thompson [4] warns of the danger of compiling malicious code, deliberately or accidentally, into the operating system, labeling them Trojan horses. A careful analysis reveals that all networks are fundamentally vulnerable to the metastability problem [2,5] that affects every sequential digital design when a flip–flop encounters an asynchronous input signal from the external world.
- Classification of attacks on networks: potential security violations may be organized under three categories: (1) unauthorized release of information, (2) unauthorized modification of information, and (3) unauthorized denial of resources. All of these attacks may be further classified into two types, active and passive. While active attacks are capable of modifying information or causing denial of resources and services, under passive

attacks, the intruder merely observes the passage of the PDUs on the network without interfering with their flow. Thus, passive attacks simply cause information release in that the intruder may examine the protocol control information portion of a PDU, recording the location and identities of the communicating protocol entities.

- Proposed approaches to communications security: to provide communications security, two basic techniques are recommended in the literature: link-oriented and end-to-end security measures. Under the rubric of 'link-oriented', the thinking is to provide security to the information being transmitted over an individual communication link between two nodes, regardless of the ultimate source and destination of the information. Since, the information is encrypted only on the link, the nodes at either end of the link must necessarily be secure. Under 'end-to-end', the thinking is to provide uniform protection to every message propagated from the source to the destination, regardless of whether the intermediate nodes and links are secure.

3. Fundamental characteristics of ATM networks

The ATM networking technology was designed by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T), intended as a standard for the high-speed transfer of voice, video, and data through public and private networks. Current standardization efforts for ATM are led primarily by the ATM Forum [6].

3.1. Key characteristics

ATM differs from all other networking strategies through the combination of the following three characteristics:

- Fixed-size cells: all traffic-audio, video, or data-is organized into fixed-length packets to permit greater efficiency in switching, from the hardware perspective, than for variable-length packets.
- Connection-oriented service: all of the cells of a given message are propagated along the same route that is established following a connection request and prior to launching the first traffic cell.
- Asynchronous multiplexing: To ensure fairness and efficient use of bandwidth resources, cells arriving at the input of any ATM switch, possibly from different users, are selected through statistical multiplexing, subject to priority considerations, and processed by the switch.

By combining these characteristics, ATM can provide a number of different categories of service for users with a wide range of data requirements. Following a user's request, a service contract is established and a virtual connection is set up from the source all the way to the destination. As a consequence of the contract, the connection guarantees a specific bandwidth and other QoS parameter values throughout the life of the connection.

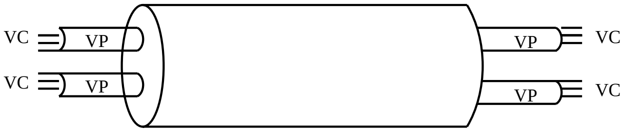

Fig. 1. Virtual paths and virtual channel connections.

3.2. Virtual paths and virtual channels

In ATM networks, virtual connections come in two forms:

- Virtual path connections, identified by virtual path identifiers (VPIs).
- Virtual channel connections, identified by the combination of a VPI and a virtual channel identifier (VCI). A virtual channel approximates a classic virtual circuit.

As seen in Fig. 1, a virtual path is a bundle of virtual channels, all of which are switched transparently across the ATM network on the basis that they share a common VPI. A virtual path connection is a collection of virtual channels.

3.3. ATM switch

Conceptually, an ATM switch is organized into two elements: a switch fabric and a call processor. Fig. 2 elaborates on the functions of the ATM switch. The organization for establishing standards, ATM Forum, has proposed two protocols: PNNI [6,7], the private network-to-network protocol, and UNI [7], the user-network interface protocol. While PNNI is for use between private ATM switches and between groups of private ATM switches, UNI lays the communications groundwork between a user and the interfacing ATM switch of the ATM network.

- Under PNNI, continuously updated topology information is distributed between switches and clusters of switches, which is used to dynamically compute paths through the network. A hierarchical organization attempts to ensure that the protocol is scalable for large worldwide ATM networks. PNNI topology update and routing are based on the well-known link-state routing technique.
- Included in UNI is a signaling protocol that is used to establish point-to-point and point-to-multipoint connections across an ATM network. This protocol has added mechanisms to support source routing, crankback, and alternative routing of call setup requests in case of connection setup failure.

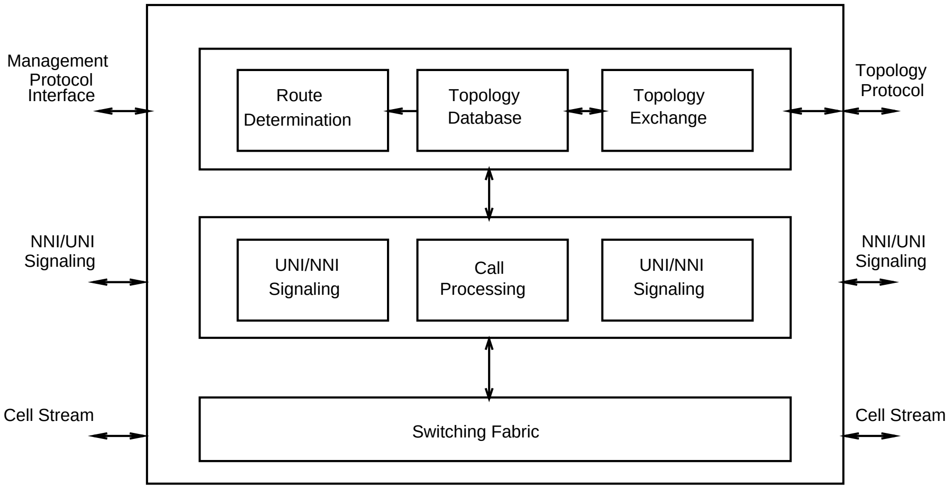

Fig. 2. Reference model for an ATM switch.

4. Synthesis of security attack models for ATM networks

An attack may be viewed as a perturbation of an operationally correct ATM network. Given the complex nature of ATM networks, conceivably, a rare combination of user traffic and system parameters may automatically lead to an adverse interaction between the different ATM principles, reflecting the lack of comprehensive thinking during design. This section, however, will be confined to attacks that are deliberately planned by intelligent enemy agents, starting from a thorough analysis of the ATM vulnerabilities. The vulnerability analysis effort will build on the fundamental framework for network security presented in [8], and focus on the four key components of ATM networks: switch fabric, call processor, ATM links, and the basic ATM operating principles including PNNI and UNI [6,7]. Once a vulnerability has been identified, the goal is to synthesize an attack that will stimulate the vulnerability and cause it to manifest itself in the form of perceptible performance impacts. The attack may consist of a contrived set of user interactions with the network, user traffic, and system parameters that are generated synthetically. In this section, the focus is to identify complex attacks that while based on the ATM fundamentals are representative of those that would be constructed by thoughtful enemy agents. Attacks are organized into two broad categories. The first attack type, basic, focuses on the failure of specific standard functions in ATM networks, while the second attack type is labeled complex, and it refers to the prescription of a malicious intent or objective. The approach presented here may be generalized to other networks including the ATM-like MPLS network [9] and the recently proposed broadband convergence network (BCN) [10,11]. Highly sophisticated attacks including timing attacks and those coordinated across different geographical points are conceivable. These may be extremely difficult to detect and defeat and are beyond the scope of this paper.

4.1. Vulnerabilities

4.1.1. Unrestricted user interactions with UNI

A significant strength of ATM networks, as stated earlier in the paper, is the lack of restrictions imposed on the users in their different interactions with the network. First, a single user may request any number of different call requests at the UNI, either for a single destination node or different destination nodes. Second, a user may request any combination of the QoS traffic parameters. Although any call request is approved only when appropriate network resources are available, ATM's permissiveness may be successfully exploited by perpetrators.

4.1.2. In-band signaling and nonseparation of resources for traffic and signaling cells

Given the significant bandwidth of ATM links, 155 Mb/s and higher, and the relatively modest bandwidth requirements of the signaling network, ATM Forum's decision to use the switching fabric network to transport signaling cells, instead of constructing a separate signaling network, is logical and makes economic sense. However, under these circumstances, termed in-band signaling, both the signaling and traffic cells have access to a key resource within the ATM switch, namely buffers. This may construe a serious vulnerability, limited by the imagination of the perpetrator. The use of in-band signaling was popular in the early Bell System telephone networks, around the time of World War II, primarily for efficiency and economy. No additional bandwidth was required, and the signaling could easily be moved across available speech channels. However, clever users soon discovered mechanisms to gain access to the switch by sending special characters during a conversation session, and they could dial long-distance calls without being detected [12,13]. This cost Ma Bell untold dollars [14]. Other mischief is equally conceivable. Eventually, in-band signaling was disbanded in favor of out-of-band signaling, with the creation of a signaling network completely isolated from the voice network for reliability and security.

4.1.3. Unrestricted access to cell headers

By definition, every intermediate switch must possess at least complete read access to every cell header. The header contents must be analyzed to yield the subsequent path for the cell. This property of ATM switches may constitute a vulnerability.

4.1.4. Vulnerability of VPI/VCI-based switching

Following a successfully established connection between the source and destination nodes, corresponding to a user call request, user traffic is transported along the channel in the format of 53-byte ATM cells. Each cell contains a 5-byte header containing a VPI/VCI pair, which, coupled with the VPI/VCI translation table entry created at the intermediate ATM switches at the time of call establishment, ensure the correct switching of the cells along the predetermined channel from source to destination. ATM Forum's PNNI document does not clarify whether the call processors at the intermediate switches must retain the source node and destination node addresses, call reference number, etc. that are specified in the DTL and utilized while the call SETUP request is being processed. Thus, according to current standards, only the VPI/VCI values control the routing of user traffic cells, which renders the VPI/VCI pair sensitive and vulnerable.

4.1.5. Vulnerability of the call processor

The call processor plays a major role in determining whether a user's call request is to be accepted or rejected. The decision is based on the exact parameters requested by the user and the corresponding resources available in the network. Thus, should a perpetrator attack the call processor of an ATM switch and successfully take over the control, the normal functioning of the ATM network may be greatly jeopardized.

4.1.6. Trusting traffic controls at the UNI

Following successful call establishment and negotiation of the traffic parameters between the user and the UNI, only the UNI checks the user traffic for compliance. In general, where user traffic exceeds the agreement, determined through a sliding window or other mechanisms, the excess cells are marked with one in their cell loss priority (CLP) field so that they may be dropped in the event of severe congestion within the network. The thinking is that the combination of the bandwidth allocation along the links and the traffic controls at the UNI will ensure the absence of congestion and undue cell loss. A key difficulty with the thinking is that ATM traffic is highly bursty, leading to uncertainty in the measurements of sustained cell rate and peak cell rates that are utilized in the negotiations. As a result, traffic control at the UNI is imprecise, permitting excess cells to slip into the network. This characteristic may be successfully exploited by a perpetrator, especially if access is gained to one of the intermediate ATM nodes. The problem is real, since, for obvious performance reasons, compliance is not verified at the intermediate nodes, deep in the network.

4.1.7. Access to knowledge of the state of the network

A key ATM principle is that a node within a peer group possesses knowledge of the complete topology of the group, i.e. the location of the peer nodes and the links, plus the gateway node identifiers of other groups to which this peer group is connected. In addition, a node may contain updated information on the bandwidth utilization of links other than the ones to which it is directly connected, node processing delays at peer ATM switches, etc. which it utilizes to compute superior routes dynamically. The complete knowledge represents the current 'state' of the network at the peer group level, from the perspective of the node in question. Clearly, where a perpetrator gains unauthorized access to an ATM switch, knowledge of the 'state' may constitute a vulnerability.

4.2. A methodology for attack modeling

Given the absence in the literature of a scientific methodology to derive attack models from analyzing network vulnerabilities, this section presents a new approach that has been developed and experimentally validated for ATM networks. The approach consists of three phases: designing an attack, modeling the attack and simulating it under realistic conditions, and assessing the performance impact of the attack model through appropriate metrics. The attack design phase, in turn, relies on two mechanisms. Under the first mechanism, a careful analysis of the key ATM principles and the modes in which the normal ATM functioning may be disrupted will most likely yield the straightforward vulnerabilities and the corresponding attacks. To uncover highly complex and subtle vulnerabilities with far-reaching impacts and sophisticated attacks, the second mechanism suggests that one or more individuals explicitly engage in intense reflection on the basic and fundamental nature of ATM networking and its constituent subprocesses. Reflection is defined as introspective contemplation or meditation on a thought or idea, quietly or calmly, with a view to understanding it in its right relation to all other concepts. Only after a thorough and deep analysis of all of the fundamental ATM issues has been completed, based on all that is known, and following an exhaustive and meticulous exploration of every available approach and reasoning technique, does the focus of the reflection converge. Given that networks will be progressively powerful, encompassing, useful, and complex, the second mechanism is likely to become indispensable to ensure their security. This technique is beyond the scope of this paper.

To enhance the effectiveness of an attack model, the following guidelines may be employed:

- How to strengthen an attack's disruptive influence on normal ATM operation.
- How to combine the essence of different individual attacks into a complex attack.
- How to render an attack more difficult to detect.

The arguments underlying the use of an accurate, asynchronous, distributed simulator to emulate the attacks and study their performance behavior are as follows. First, a simulator is highly flexible and permits the testing of complex attacks that may be very difficult to realize in an actual ATM network. Second, the incorporation of hardware and timing parameters of the ATM switches into the simulator renders it highly realistic and implies accurate results. Third, modeling attacks on an actual ATM network may require extensive hardware and software modifications to the ATM switches, which may be prohibitively expensive.

To assess the effectiveness of the attacks, especially sophisticated attacks, existing metrics may require reexamination, or completely new metrics may need to be designed. The following guidelines have been employed in metric design:

- Specify the exact function of the attack.
- Identify network parameters upon which the impact of the attack may be observed.
- Quantify the extent of the adverse impact, relative to the normal operation.
- Develop reasoning about how the metric may be utilized to detect an attack.

5. Modeling, simulation, and behavior analysis of security attack models

The objectives of modeling and simulation of an attack model are two-fold. First, they serve to verify that the attack model design successfully forces the corresponding vulnerability to be manifested at an observable output, under realistic input traffic conditions. Second, they are expected to yield an accurate picture of an attack's qualitative or quantitative impact on one or more of the network's performance metrics. To achieve these objectives, three requirements are in order. The choice of a representative ATM network topology satisfies the first requirement. The second requirement is the development of an input traffic stimulus that is representative of the real world. The third requirement is the development of ATMSIM 1.0 [2], an accurate, distributed ATM simulator that utilizes an asynchronous distributed simulation algorithm to execute the computationally intensive behavior models of the ATM switches as well as emulate the complex asynchronous interactions between them. In this section, five attack models, representative of the types of attacks described earlier are modeled and simulated. The design of attack models starting from vulnerability analysis, coupled with their modeling, simulation, and behavior analysis, constitutes a scientific approach to studying security attacks in ATM networks.

5.1. Choice and justification of the network topology

A 9-node representative ATM network topology is synthesized for this study and shown in Fig. 3. Given that hundreds of simulation runs are required for debugging and performance analysis, simulation is computationally intensive, and since only finite computational resources are available, the choice of a reasonably sized network topology with a modest number of nodes is necessary to complete the study in a reasonable time. To exercise the key elements of the PNNI protocol and to achieve acceptable accuracy in the overall performance analysis, the network must consist of multiple peer groups. In this study, a total of nine nodes are organized into three peer groups, arranged in a two-level hierarchy. The groups are labeled A, B, and C. Of these peer groups, one in particular, group B, is designed to consist of five nodes, more than in groups A and C. This enables peer group B to offer greater flexibility in the placement of the attacker node versus the target nodes and also to model the more complex attack 5. Peer groups A and C consist of two nodes each and while both nodes of C are of gateway type, i.e. they interface with other peer groups, only one node of A is of gateway type. The aim underlying the node placements and their connectivity is to yield insights into the overall network behavior under attack.

The two nodes in peer group A are labeled A.1 or 1 or 100 and A.2 or 2 or 101. In peer group C, the nodes are labeled C.1 or 8 or 120 and C.1 or 9 or 121. In peer group B, the nodes are labeled B.1 or 3 or 110, B.2 or 4 or 111, B.3 or 5 or 112, B.4 or 6 or 113, and B.5 or 7 or 114. The multiple labels underlie different naming conventions used by ATMSIM 1.0 and other associated programs. The network topology is conceived from the following interconnected cities in the US. Nodes A.1, A.2, B.1, B.2, B.3, B.4, B.5, C.1, and C.2 correspond to Olympia, Carson City, Pierre, Jefferson City, Baton Rouge, Topeka, Santa Fe, Rayleigh, and Albany. Links are bidirectional, and separate identifiers are used to label each direction. Thus, 4 → 9 represents a link from node four to node nine. Table 1 presents the identifiers for each of the links in the network and Table 2 presents their key characteristics, namely, their distances and physical propagation delays in absolute seconds and in terms of timesteps, the basic unit of time in the simulation. Assuming OC-3 links, rated at 155.52 Mb/s, and an ATM packet size of 53 bytes, or 424 bits, the transmission time for an ATM packet is (424 b)/(155.52 Mb/s) = 2.73 μs.

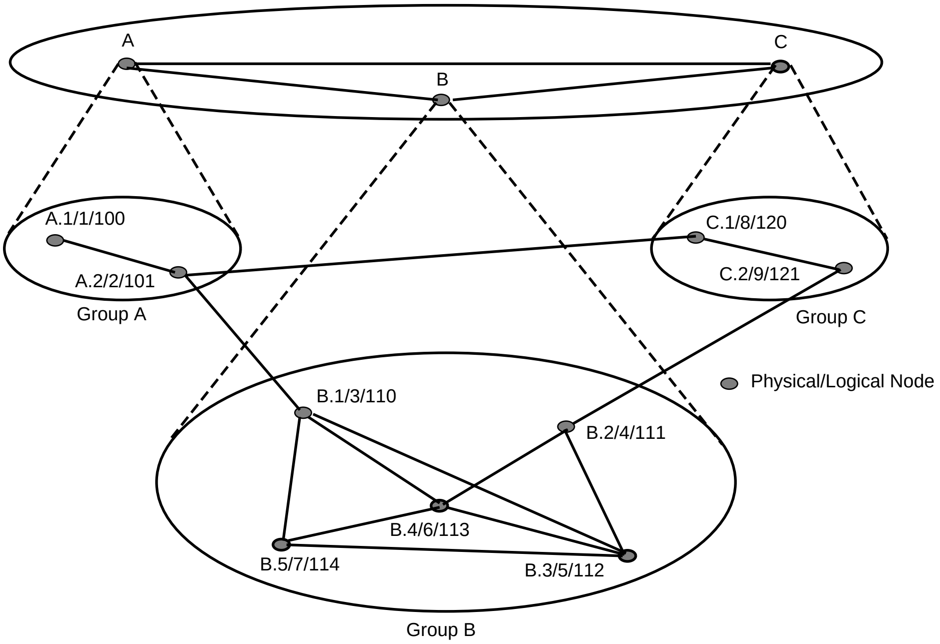

Fig. 3. Nine-node representative ATM network topology.

5.2. Utilizing an accurate ATM simulator: ATMSIM 1.0

ATMSIM 1.0 [2] is an asynchronous distributed ATM simulator that encapsulates the key elements of ATM Forum's PNNI 1.0 and UNI 3.0. Later versions of PNNI and UNI do not differ appreciably from PNNI 1.0 and UNI 3.0. The simulator utilizes the principles of asynchronous distributed simulation outlined in [15]. In this study, ATMSIM 1.0 is executed on a testbed of Pentium laptops, configured under the Linux operating system and interconnected through a 100 Mb/s Fast Ethernet. While ATMSIM 1.0 incorporates input traffic [16,17], designed to emulate a representative ATM network, it permits users to generate call SETUP requests externally and insert them into the network. Traffic consists of audio, video, and data. While call SETUP requests are assumed to obey a Poisson distribution, the traffic volume is set based on the 'stability criterion' [15]. The bandwidth requests are assumed to be stochastic, varying between 4 and 6 Mb/s for normal calls. For bogus calls, the bandwidth requests are defined by the specific attack and are discussed subsequently. In the course of its execution, the simulator writes intermediate data onto specific files, from which the progress of an attack may be inferred. For performance analysis, a total of 150 simulation runs are executed on the testbed, each run requiring approximately 10–12 h of wall clock time, and cumulatively generating a total of 175 Mb of simulation data.

Table 1
Identifiers for each of the bidirectional links in the network

Link x↔y	Link ID x→y	Link ID x←y
A1↔A2	1	14
A2↔B1	2	15
B1↔B3	3	16
B1↔B4	4	17
B1↔B5	5	18
B2↔B3	6	19
B2↔B4	7	20
B3↔B4	8	21
B3↔B5	9	22
B4↔B5	10	23
B2↔C2	11	24
C1↔C2	12	25
A2↔C1	13	26

5.2.1. Input files

ATMSIM 1.0 permits the simulation to be controlled through a number of input files, the names and contents of which are described subsequently.

Table 2
Distances and physical propagation delays of the links

Link	Distance (D) in km	D km/(fiber optic speed=200,000 km/s) in seconds	Link delay in timesteps
A1–A2	1158.16	5.79	2121
A2–C1	4420.08	22.1	8095
A2–B1	2369.90	11.84	4337
C1–C2	1022.04	5.11	1872
C2–B2	1546.73	7.73	2832
B1–B3	2405.78	12.03	4407
B1–B4	927.91	4.64	1700
B1–B5	1486.07	7.43	2722
B2–B3	1268.37	6.34	2322
B2–B4	356.23	1.78	652
B3–B4	1505.06	7.5	2747
B3–B5	1916.00	9.58	3509
B4–B5	1347.38	6.74	2469

5.2.1.1. Files with name 'atm_input_#'. There are nine files, one for each node, represented by #, through which externally generated call SETUP requests may be inserted into the simulation. In addition, for successfully established external calls, these files serve as conduits for externally generated traffic cells to be inserted into the simulation. Information in these files is organized as lines with following fields: 'timestep,' 'call_id,' 'action-character'.

The 'timestep' field specifies when this input line should be called into effect, the 'call_id' field specifies a unique call identifier, and the 'action-character' field contains one of two symbols, C or T. The symbol C represents a call SETUP request, and the data in subsequent lines are interpreted according to the following fields: 'dest_id,' 'qos_class,' 'cpr,' 'ctd,' where, 'dest_id' implies the destination node identifier, 'qos_class' represents the quality of service (QoS) class, not currently used, 'cpr' refers to the peak cell rate, and 'ctd' represents the cell transfer delay, also currently unused.

The symbol T represents a request to send user traffic, and the data in subsequent lines consist of a single field, '# cells,' which refers to the number of cells to be inserted at 'timestep' on behalf of the call 'call_id,' where, it is successfully established. In the event the call fails, the information in the '# cells' field is ignored.

5.2.1.2. File with name 'attack.in'. Through this file the user specifies the attack to be activated. The information in the file is organized through lines with the fields: 'attack#,' 'attacker,' 'target,' where, the first field, 'attack#', identifies the specific attack by number; the second field, 'attacker', specifies the node identifier that is controlled by the perpetrator; and the third field, 'target', specifies the target node identifier, i.e. the node to be attacked. The node identifiers are specified utilizing the three-digit naming convention explained earlier in Section 5.1.

5.2.1.3. File with name 'ATM_PARAMS'. The information in this file is organized through three lines, shown subsequently. The first and second lines specify the input and output buffer sizes at each node, in terms of ATM cells. The information in the third line is relevant to attack 2, elaborated subsequently in Section 5.4, and it specifies the time period, i.e. inverse of the frequency, with which different erroneous destination nodes must be selected.

```
IN_BUF_SIZE 30000
OUT_BUF_SIZE 30000
ATTACK_2_FREQ 25000
```

5.2.2. Output files

The simulator logs data into the output files, which, in turn, serve as a window into the internal functioning of the simulation, under normal and attack scenarios.

5.2.2.1. Files with name 'atm_log_file_#'. There are nine such files, one per node, represented by #, wherein each node dynamically logs key information. The information contained is of three types:

- [110000] CALL ID:1 SETUP:UNI SETUP: calling party: UNIie_CGP_NUM:113:0:0
  called party: UNIie_CP_NUM:101:0
  ATD:ATM_TRAF_DESC: for_pcr_0 (130/1000)
  conn id: flags:0 vpci:0 vci:0
  The implication here is that at a time instant specified by 110000 timesteps, the call SETUP request with identifier 1 was initiated at this node, with the destination node 101. The quality of service (QoS) parameters requested are identified in the field 'ATM_TRAF_DESC for_pcr_0 (130/1000)' consisting of a bandwidth request of 1000.
- [110217] CTIME CALL ID:1
  [110217] CALL SETUP SUCCESSFUL:DTL-[*trans*_0][101|0][110|0]
  The information contained here is that a call request with identifier 1 was successfully established at a time instant given by 110217 timesteps. The DTL for this call is contained at the end of the line.
- [110000] BW_AVAIL: link [3|8]:155000This indicates at the time instant given by 110,000 timesteps, the available bandwidth on the link between nodes three and six is 155,000. This is reserved bandwidth, not actual, and appears in the log file only when there is a change.

5.2.2.2. Files with name 'atm_output_#'. These files, one for each node, contain the summary statistics for the corresponding node. The summary includes the number of ATM cells processed, number of cells dropped, etc.

5.3. Attack 1

Under this attack, if a call setup request that originates at a 'node to be attacked' arrives at an intermediate node (which is already under attacker's control), under the attack condition, accept the connection at this intermediate node without letting the destination know about it and then drop all the cells on that channel.

Assume that the perpetrator controls node B.2 and its target is node B.5. Ideally, the perpetrator should occupy a node from where it may intercept the maximal number of target calls. In the network in Fig. 3, nearly all of the nodes are connected to each other, and no node has any significant advantage over another. Since the gateway nodes B.1 and B.2 are connected to other groups, they offer an ideal location to a perpetrator to inflict maximal damage to the overall network. Both B.1 and B.2 offer similar connectivity, and the latter is chosen arbitrarily. As a challenge to the attacker, the target node is located as far away from B.2 as possible. Both nodes B.1 and B.5 are strong candidates, and B.5 is selected arbitrarily. Thus, all call SETUP requests originating at B.5 and routed through B.2 such as to destination nodes C.1 or C.2 are likely to be intercepted by

Table 3
Call success rates under attack 1 for 8 target calls

Node	A.1	A.2	B.1	B.2	B.3	B.4	B.5	C.1	C.2
Call success rate (normal) (%)	35	53	59	40	63	63	62	43	38
Call success rate (attack) (%)	35	53	59	42	65	62	55	43	40

the attacker. Thus, the input file ‘attack.in’ will contain the line: ‘1 111 114.’

5.3.1. Experiments

Observations indicate that of the approximately 550 call SETUP requests generated by the traffic generator incorporated within ATMSIM 1.0, only a handful, namely 6, originate at B.5 and include B.2 in their route. Thus, a number of trial experiments were designed, executed, and critically analyzed with the intent of identifying a scenario, where possible, that clearly reveals the impact of the attack. The initial experiments indicate that for externally generated calls, orignating at B.5 and destined for a node in peer group C, the route is more than likely to include the gateway node B.2 as an intermediate node. These calls are termed target calls.

To understand the relationship between the increasing intensity of attack and network performance, an experiment was designed where, the number of externally generated target calls is gradually increased in steps from 8, to 17, 25 and 60. Thus, the input file ‘atm_input_7’ is modified to include more calls with a node in peer group C as the destination.

5.3.2. Analysis of the simulation results

For every experiment a number of simulation runs are executed, and the data obtained from the output log files ‘atm_log_file_#’ are processed to yield statistics on the available bandwidth at each link at different timesteps, number of successful calls at each node, and number of call failures. Table 3 presents the call success rates under normal and attack scenarios for eight externally inserted target calls. For the network, refer to Fig. 3.

In Table 3, the call success rates at nodes A.1 and A.2 are unchanged under the attack scenario. This is logical, since, they do not constitute target nodes. For node B.5, the call success rate is appreciably lower in the attack scenario, implying that the perpetrator at B.2 is successfully intercepting calls originating at B.5. However, while the cause of the very slight decrease in the call success rate at node B.4, from 63 to 62%, is unclear, since, B.4 is not a target node, the increase in the call success rates at nodes B.2, B.3, and C.2 is unexpected.

To gain insights into the unexpected behavior of the network under attack, the bandwidth availability at all of the links, under normal and attack scenarios, is critically examined. Three distinct behaviors are observed, two of which are represented in Fig. 4 in the form of comparative analyses of the bandwidth availability at two links, 4→9 and 5→4, as a function of the progress of simulation. The third behavior is one where, a link’s available bandwidth is unaffected by the attack, implying that the link is beyond the sphere of influence of the attack. An example of the third behavior consists of the link 1→2. In Fig. 4, it is observed from the graphs corresponding to the link 4→9 that more bandwidth is available while the attack is in progress. This is logical, since when node four or B.2 intercepts the target calls destined for peer group C, either node C.1 or node C.2, it neither forwards the call requests nor allocates bandwidth for these calls along the link 4→9. Similar behavior is observed for the link 9→8, but that is not shown here graphically.

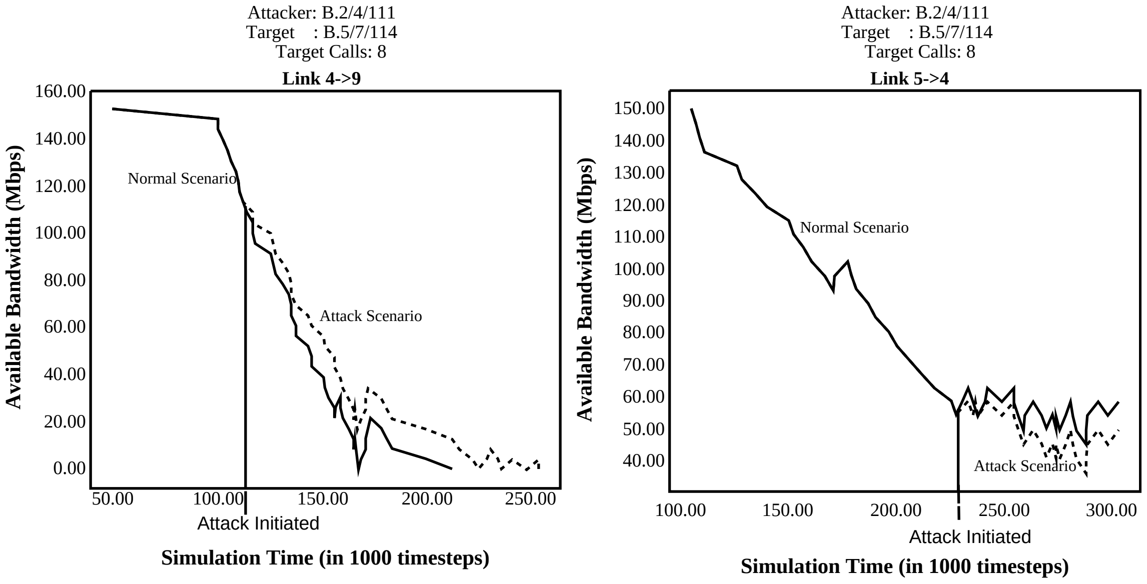

Fig. 4. Bandwidth analysis under attack 1 for eight target calls.

Table 4
Call success rates under attack 1 for 8, 17, 25, and 60 target calls

Target calls: 8									
Node	A.1	A.2	B.1	B.2	B.3	B.4	B.5	C.1	C.2
Call success rate (normal) (%)	35	53	59	40	63	63	62	43	38
Call success rate (attack) (%)	35	53	59	42	65	62	55	43	40
Target calls: 17									
Node	A.1	A.2	B.1	B.2	B.3	B.4	B.5	C.1	C.2
Call success rate (normal) (%)	35	53	58	40	61	62	60	43	37
Call success rate (attack) (%)	35	53	58	42	66	61	50	43	40
Target calls: 25									
Node	A.1	A.2	B.1	B.2	B.3	B.4	B.5	C.1	C.2
Call success rate (normal) (%)	35	53	58	39	60	60	57	43	36
Call success rate (attack) (%)	35	53	57	43	67	60	47	43	40
Target calls: 60									
Node	A.1	A.2	B.1	B.2	B.3	B.4	B.5	C.1	C.2
Call success rate (normal) (%)	35	53	57	39	59	59	45	43	34
Call success rate (attack) (%)	35	53	57	43	68	59	36	43	40

In Fig. 4, for the link 5→4, less bandwidth is available while the attack is in progress. A possible reason underlying this behavior is as follows. A number of calls originating at B.3 and destined for C.2 through B.2 may have failed under the normal scenario, due to lack of bandwidth availability along the link 4→9. This implies greater bandwidth availability along link 5→4. Under attack scenario, with less competition from the target calls, i.e. increased bandwidth availability along link 4→9, these previously failed calls are now successfully established, thereby reducing the bandwidth availability along link 5→4. Similar behavior is observed for the links 7→6 and 8→2.

The insight thus gained may help in understanding the unexpected increase in the call success rates at nodes B.2, B.3, and C.2, noted in Table 3. The increased available bandwidth along link 4→9 under the attack scenario permits calls originating at B.2 and B.3 and destined for C.2 or C.1 to succeed that may have failed under the normal scenario due to lack of bandwidth. As a result, the call success rates at B.2 and B.3 are higher under the attack scenario. Similarly, the increased available bandwidth along link 9→8 contributes to a higher call success rate at node C.2.

A series of experiments was designed for an increased number of target calls, extending from 17 to 25 to 60. Preliminary experiments reveal that beyond 60 target calls, the general behavior of the network under attack remains unchanged, although the effects are amplified. Table 4 presents the call success rates for each of the nine nodes, under normal and attack scenarios, while Fig. 5 plots the difference in the available bandwidths between the normal and attack scenarios, averaged over all the nodes, as a function of the number of target calls, for the representative links 4→9 and 5→4.

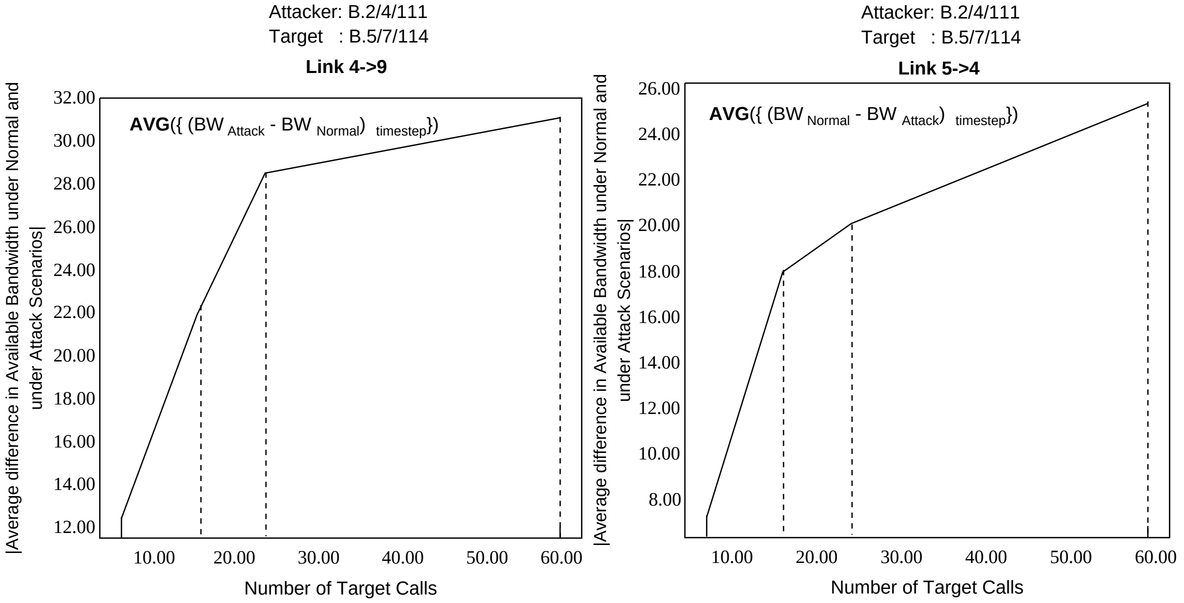

Fig. 5. Difference in available bandwidth under normal and attack scenarios, averaged over all nodes, as a function of the number of target calls.

Analysis of the information in Table 4 and Fig. 5 reveals that the behaviors previously observed for the eight target calls remain in effect and are amplified for higher numbers of target calls. Fig. 5 further shows that while the difference in the available bandwidths between the normal and attack scenarios, say ΔBW, increases with increasing number of target calls, the rate of increase of ΔBW slows down at higher numbers of target calls, possibly due to the links being saturated with successful calls.

In summary, insights into the behavior of the network under this attack may be expressed as follows. Under normal input traffic and stable network operation, call success rates at the nodes are generally held at uniform values, subject to minor variation. Any sharp variation in the call success rate at one or more of the nodes is more than likely to indicate the onset of this attack. In general, under attack, links leading away from the node under the perpetrator's control are likely to experience higher bandwidth availability. In contrast, links leading into the node under the attacker's control may experience, depending on the traffic, higher bandwidth usage, i.e. lower bandwidth availability. Although there are exceptions such as links 9→8, 8→2, and 7→6, the probability is high that the link bandwidth usage around the node under the attacker's control will reveal a change under the normal and attack scenarios. This may constitute a valuable tool in localizing the source of the attack.

5.4. Attack 2

Under this attack, if a call is already established between any two nodes in the network, routed through an intermediate node already under the attacker's control, and if the source (or destination) node is on the perpetrator's list of 'node(s) to be attacked,' redirect all the traffic cells arriving on this channel to a periodically selected arbitrary channel that is already established. The attack applies to a call that may already be established or is currently under consideration. The attack is launched when and after the call has been successfully established.

Assume that the perpetrator controls node B.2 and its target is node B.3. The choice of B.2 as the location of the attacker follows the same reasoning as in the previous Section 5.3. To maximize interception by the attacker, a node that is connected directly to B.2 is selected as the target node. While both B.3 and B.4 qualify, node B.3 is selected arbitrarily. Thus, calls originating at node B.3 and destined for C.1 or C.2 are more than likely to be routed through B.2 and may be subject to attack. These are labeled target calls. In this work, calls originating at the nodes of group C and destined for B.3 are also viewed as target calls. Also, the rate at which the outgoing VPI/VCI pair is modified for the target calls at B.2 is specified by the redirection period, in terms of timesteps. The complete list of channels at B.2's disposal includes B.2→C.2, B.2→B.3, and B.2→B.4, which it will employ to deliberately misdirect traffic. Thus, the input file 'attack.in' will contain the line: '2 111 112.'

5.4.1. Experiments

For this attack, four cases are considered to develop an understanding of the impact of the two variables—number of target calls and frequency of redirection. For cases 1 and 2, the number of target calls is set at 30 and 50, respectively, and the redirection time period is selected at 5000 timesteps. Cases 3 and 4 are designed to intensify the severity of the attack. The number of target calls is set at 80 and 120, and the redirection time period is decreased to 2000 timesteps, implying faster hopping between the available channels for misdirecting the traffic cells. Input file 'atm_input_5' is modified with the number of target calls, while input file 'ATM_PARAMS' is modified to accept the values of the redirection period.

5.4.2. Analysis of the simulation results

To gain an understanding of the impact of this attack, key data from the simulation are logged, as explained subsequently.

First, when the perpetrator at the attacker node successfully intercepts a target call, the following data are written into the log file:

```
BEGIN
ATTACK 2 IN PROGRESS
target:100 attacker:101
[ATT2] init, count is 37
END
[106011] BW_AVAIL: link [2|3]:150631
[106011] ATT2 adding 32002:5 32004:4
new attack two added on vpci:32002
—ATT2—tagging [32004:4][32002:5]
```

The content of the 'count' field represents the number of calls that have been processed by the switch up to the present time. The last line is important in that it implies that the call has been intercepted by the attacker. The original input/output vpi/vci pair for the cells of this call relative to the switch fabric consists of identifier 32,004 at port four for the input side and 32,002 at port five for the output side.

Second, upon selection of a randomly chosen arbitrary output vpi/vci pair, the following information is logged. It indicates that for the vpi/vci identifier 32,008 at port four on the input side, the new output vpi/vci pair consists of identifier 1015 at port four:

```
[214252] ATT2 NEW OUT: for input:32008|4
orig:32006|5 old:32006|114230 new:10515|4.
```

Third, when a cell is dropped, the following data are logged, implying that at the time instant given by 480,939 timesteps, the ATM cell along link 4→6 is dropped. The physical propagation delay along the link is 652, and the total bandwidth capacity is 156,000, of which 3072 is available at the current timestep:

[480939] PACKET DROP output buffer link: LINK [4/6*fd*:5st:1]t/1 156000:652: bw:3072.

The information contained in the logs is utilized for a comparative analysis of cell drop behavior in the four cases, under normal and attack scenarios.

Figs. 6 and 7 present the cell drop behavior in each of the four cases, and focuses on the links that exhibit a difference between the normal and attack scenarios. For such links, the arrow identifies the link by direction, and the two sets of numbers represent the cells dropped under the normal scenario, indicated by the symbol N, and attack scenario, indicated by symbol A. It is pointed out that at any node, the output buffer is shared among all of the outgoing links.

5.4.2.1. Case 1. For a total of 30 target calls and a redirection period of 5000 timesteps, differential cell drop behavior is observed at five links, B.2→B.4, B.4→B.1,

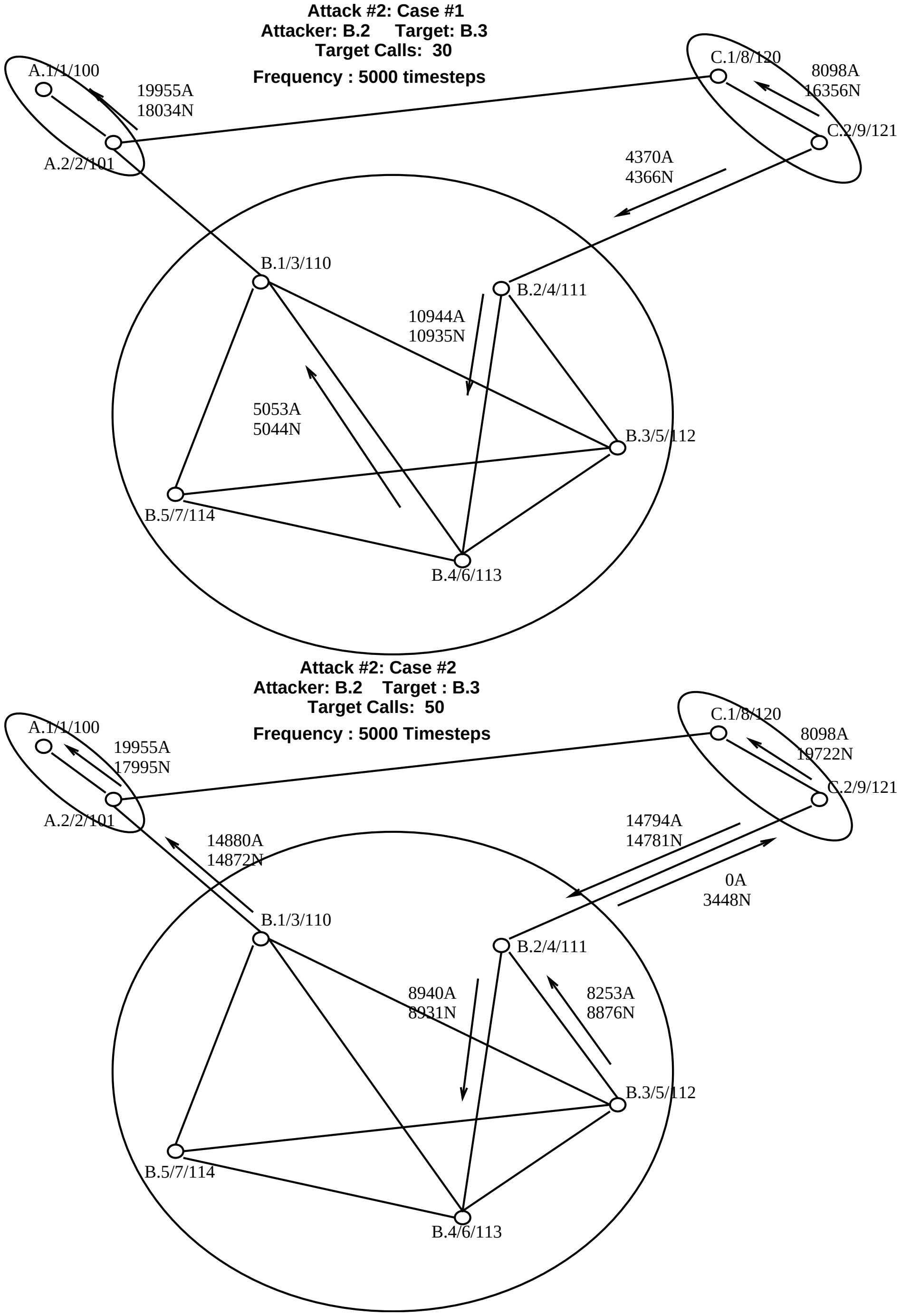

Fig. 6. Cell drop rates at the links under normal and attack 2 scenarios.

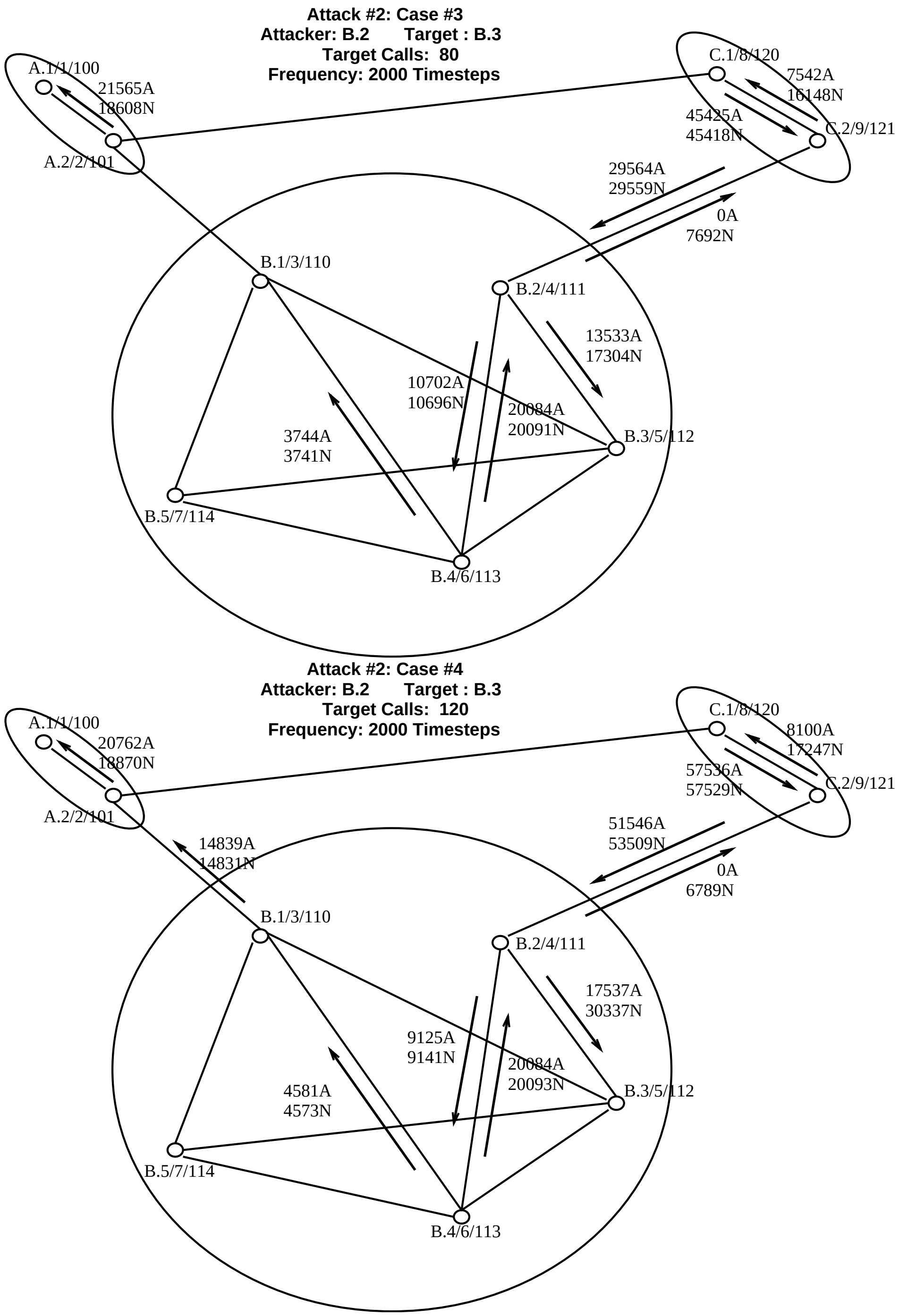

Fig. 7. Cell drop rates at the links under normal and attack 2 scenarios (Cont'd).

C.2 → B.2, C.2 → C.1, and A.2 → A.1. Possible explanations are presented subsequently.

- Along the link, C.2 → C.1, cell drop is high under the normal scenario, implying that a number of calls are attempting to transport an excessive number of cells along this link. The significant reduction in cell drop under the attack scenario may be explained as follows. Given that the attacker is located at node B.2, for many of the calls originating at node B.3 and routed through B.2 toward the destination C.1, the cells are deliberately misdirected along other links. As a result, fewer cells are transported along the link C.2 → C.1 in turn implying less cell drop.One would expect link B.2 → C.2 to behave similarly to the link C.2 → C.1. However, there is no differential cell drop between the normal and attack scenarios along the link B.2 → C.2, the reason being as follows. Just as a subset of the cells meant for transport from B.3 to C.2 along link B.2→C.2 are redirected elsewhere, similarly, a subset of the cells meant for transport from B.3 to B.4 along link B.2→B.4 are possibly misdirected along B.2→C.2, thereby canceling the two opposing effects. The calls originating at B.3, destined for B.4, and routed through B.2 may constitute a part of the traffic synthesized by the traffic generator within ATMSIM 1.0.

- Along the link A.2→A.1, cell drop is high under the normal scenario. The fact that cell drop is high also along the link C.2→C.1 possibly implies that a number of calls are established between nodes C.2 and A.1 and their constituent cells are being transported from node C.2 to node A.1. Under attack, the congestion along C.2→C.1 is reduced, enabling more cells to be routed from C.2 toward A.1 via C.1. This contributes to more cell drop along the link A.2→A.1 under the attack scenario. The slight increase in the number of cells dropped along the link B.4→B.1 implies an increase in the number of cells being transported from B.4 possibly toward the nodes of group A. This may bear a slight contribution to the increased cell loss under attack along link A.2→A.1.
- The difference in the cell drop along link C.2→B.2 between the normal and attack scenarios, is slight. The overloading of the single buffer at node C.2 from excess traffic along the link C.2→C.1 is more likely than the onset of the attack to influence the cell drop along the link C.2→B.2.
- The less than significant increase in cell drop under the attack scenario along the links B.2→B.4 and B.4→B.1 may be attributed to the increase in the number of cells that are misdirected by B.2 toward B.4, some of which find their way toward B.1. Thus, the traffic along the links B.2→B.4 and B.4→B.1 increases, causing a slightly higher cell drop.

5.4.2.2. Case 2. Relative to case 1, only the number of target calls is increased, to 50, in case 2. Except for the links B.2→C.2 and B.3→B.2, the general behavior of the links under case 2 is similar to that in case 1. The differential cell drop under normal and attack scenarios along links B.1→A.2, C.2→B.2, and B.2→B.4 is slight, and as in case 1, they may be attributed to either the overloading of the buffers at the nodes or the misdirection of cells by the attacker node B.2. The behaviors along links C.2→C.1 and A.2→A.1 are similar to those in case 1, and similar explanations will apply. Under more target calls, the differential behaviors along these links are magnified, as revealed by the increased difference in the cell drop rates between the normal and attack scenarios.

Given the increased number of target calls in case 2, more of the cells from B.2 transported to C.2 via B.2 under the normal scenario are misdirected away from link B.2→C.2 and possibly along link B.2→B.4 under the attack scenario. The result is a significant differential cell drop behavior between the normal and attack scenarios along link B.2→C.2, which, contrary to expectation, failed to manifest itself in case 1.

The appreciable decrease in the cell drop rate at link B.3→B.2 under the attack scenario, may be explained as follows. Under normal scenario, nodes B.1, B.5, and B.4 transport a number of cells through B.3 towards B.2 or the nodes of group C. Also, a part of the traffic cells from C.2 or C.1 intended for nodes of group B may pass through node B.3. The resulting overloading of the buffer of node B.3 causes an appreciable cell drop along the link B.3→B.2. Under attack, the increased number of target calls originating at B.3 implies that a significant number of cells originating at B.3 and intended for the nodes of group C via B.2 are misdirected at B.2 towards B.4. In turn, B.4 directs these misdirected cells towards B.5, B.1, and B.3. The resulting overloading of B.4's buffer implies a decrease in the number of cells sent by B.4 or via B.4 towards the nodes of group C or node B.2 via node B.3. Also, cells originating at the nodes of group C and intended for B.3 are intercepted and misdirected by B.2, thereby relieving pressure on the output buffer of B.3. Thus, the traffic encountered by B.3 decreases, in turn, implying less cell drop along the link B.3→B.2.

5.4.2.3. Cases 3 and 4. Under cases 3 and 4, while the number of target calls is increased to 80 and 120, the redirection time period is decreased to 2000 timesteps. The network continues to exhibit the same general behavior as in cases 1 and 2, the only difference being that the effects are amplified. In addition, the link B.2→B.3 reveals an appreciable difference in the cell drop rate between the normal and attack scenarios, which may be explained as follows. Under the normal scenario, the increased number of cells stemming from an increased number of calls originating at the nodes of group C and destined either for B.3 or for other nodes of group B but routed through B.3 congest the link B.2→B.3, causing an appreciable cell drop rate. Under attack, node B.2 redirects these cells away, thereby lowering the cell drop rate along the link B.2→B.3.

In summary, the inference from cases 1 through 4 is that while the impact of attack 2 manifests itself in the network, the manifestation may occur close to the location of the perpetrator or at an unexpected region of the network, away from the location of the target node and the node controlled by the perpetrator. Thus, localizing the source of the attack may be difficult. In essence, attack 2 is highly dynamic, and its observable impact is a strong function of the current state of the network. Conceivably, attack 2 may be detected in an otherwise stable network by detecting a sharp change-increase or decrease-in the cell drop rate when the external traffic is intense. However, under light traffic load attack 2 may elude easy detection.

Under attack 2, cells intended for a node may appear at unexpected nodes, causing confusion and other unintended effects at higher levels. This study is limited in that the analysis is confined to the network layer and makes no attempt to systematically examine the receipt of stray cells and detect the attack through a comprehensive high-level analysis.

5.5. Attack 3

Under this attack, effort is made to establish dummy sessions with other nodes in the current peer group and reserve network resources so as to deliberately deny service to genuine users. In developing this attack, the perpetrator may synthesize either a few bogus calls, each requiring significant bandwidth resource, labeled type A, or a number of bogus calls, each requesting modest bandwidth, labeled type B. Unlike attacks 1 and 2, this is a diffused attack in that it lacks a specific target node or link. Instead, it aims to inflict as much damage as possible to the entire network.

Assume that the attacker is located at node B.4. The choice is dictated by the fact that B.4 occupies a central place in the peer group with direct connection to all of its peer nodes in the current group. Although B.3 is also connected directly to all other nodes in the network, B.4 is selected arbitrarily over B.3. The reference input file ‘atm_input_6’ is modified to include the dummy call SETUP requests along with the bandwidth resource request and their constituent traffic cells. In addition to its effort to establish bogus calls with its peer nodes B.1, B.2, B.3, and B.5, node B.4 will also attempt to establish bogus calls with nodes C.2 and A.2. Although not a gateway node and even if it is not a peer group leader, the PNNI 1.0 specifications permit node B.4 to possess knowledge of the gateway nodes of other peer groups.

5.5.1. Experiments

Logically, the routes of the bogus calls are chosen as follows: B.4→B.1→A.2→A.1, B.4→B.1, B.4→B.2→C.2→C.1, B.4→B.2, B.4→B.3, and B.4→B.5. A number of preliminary simulations were designed and executed to determine (i) the range of the bandwidth requests under types A and B and (ii) the number of bogus calls under each of types A and B to yield maximal differential network behavior under attack 3. From the results of the preliminary simulations, while bogus calls of type B request bandwidths in the range 4–6 Mb/s, calls of type A request bandwidths in the range 20–30 Mb/s. A total of three sets of input traffic are synthesized, sets one through three, and the number of calls in each set for each type of traffic is so chosen that the cumulative bandwidth requests for all bogus calls under each of types A and B are similar. Set zero corresponds to the normal scenario and serves as a reference. Table 5 presents the details of the input traffic for each of the three sets. An increase in the number of bogus calls beyond set three reveals no significant change in the network behavior under attack.

Table 5
Details of the input traffic for attack 3

Set #	Number of bogus calls	
	Type A	Type B
0	0	0
1	12	60
2	24	120
3	60	300

5.5.2. Analysis of the simulation results

By nature, attack 3 aims at denying user calls. Thus, a logical measure of the success of this attack is the user call success rate. It may be pointed out that the graphs shown here present only the legitimate user calls, not bogus calls.

Fig. 8 plots the fraction of successful user calls in the entire network, expressed as a percentage of total user calls inserted into the network, as a function of the input traffic set, for each of type A and B attacks. For an increasing number of bogus calls from 0 (set 0) to 60 (set 3) for type A and from 0 (set 0) to 300 (set 3) for type B, the severity of the attack increases, causing a decrease in the call success rate. At the peak of the attack, virtually all of the available bandwidth is usurped by the bogus calls, and the network reaches a saturation point. Further increase in the number of bogus calls is accompanied by negligible impact on network performance. Comparative analysis of the call success rates

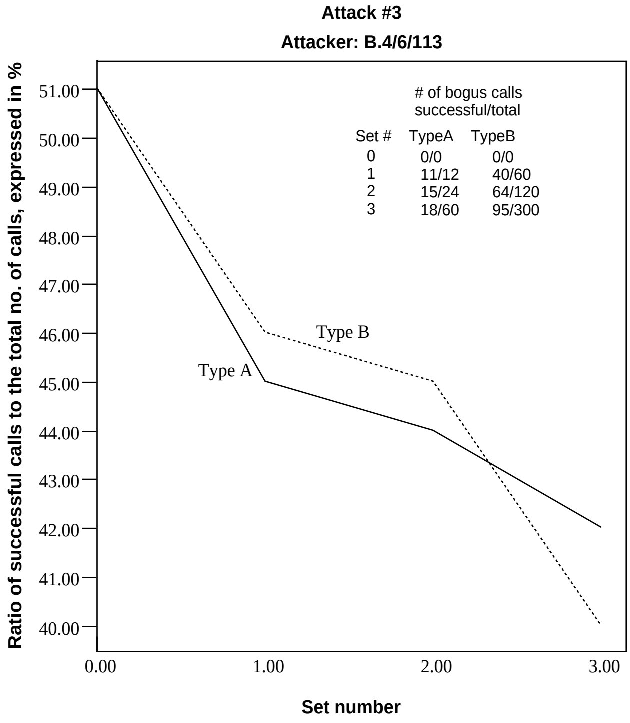

Fig. 8. Fraction of successful user calls in the entire network, expressed as a percentage, as a function of the input traffic set, for type 3A and 3B attacks.

for type A and B reveals that while the attack with type A bogus calls causes network performance to drop faster than with type B bogus calls, the call success rate in the entire network drops to its lowest level under type B bogus calls. The key reason is that bogus calls with lower bandwidth demands are more likely to be established than calls with high bandwidth requirements, eventually usurping more of the network resources and inflicting greater damage on the network performance. In addition, the larger number of successful bogus calls under type B traffic implies that a greater fraction of the network's computational resources are consumed, thereby slowing the call setup process. It is also observed that despite its severity, attack 3 is unable to zero the call success rate in the entire network, reflecting the richness in route availability in representative networks and their resistance to complete defeat by a perpetrator.

To gain a better understanding of the nature of attack 3, Figs. 9–11 present the fractional call success rates at select individual nodes of the network, A.1, A.2, and B.5, respectively. The rationale underlying the choice of the nodes is as follows. Node A.1 is located farthest from the source of the attack. It is located in a different peer group and does not constitute a gateway node. While node A.2 is located in peer group A, different from group B where, the perpetrator is located, it is connected to peer group B by virtue of being a gateway node. Node B.5 is situated in the same peer group as the attacker and is expected to bear the brunt of the attack. In Fig. 9, the call success rate at node A.1 reveals no influence from the attack. This is expected, since the perpetrator at B.4 cannot reach node A.1. The gateway node, A.2, is visible to the attacker, and its susceptibility is reflected by the drop in the call success rate, shown in Fig. 10, from 53 to 46%, which equals 7%. In contrast,

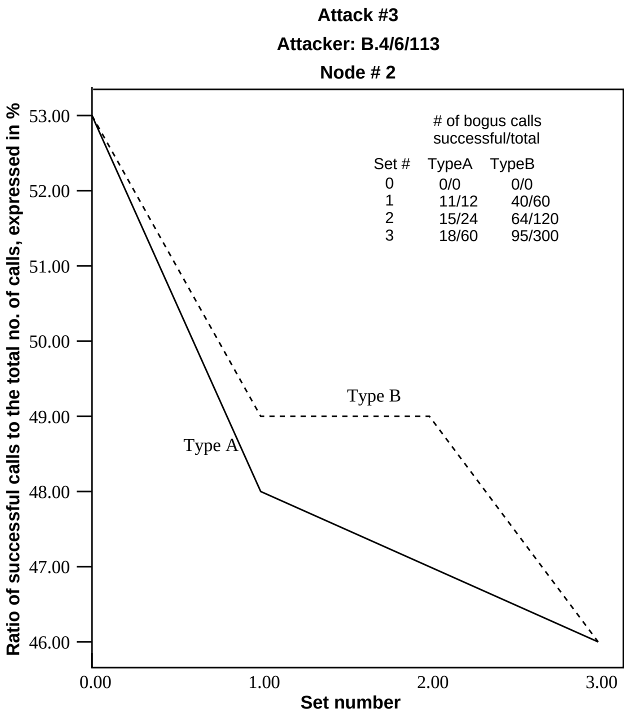

Fig. 10. Fractional call success rate at node A.2 under attack 3, as a function of the input traffic sets.

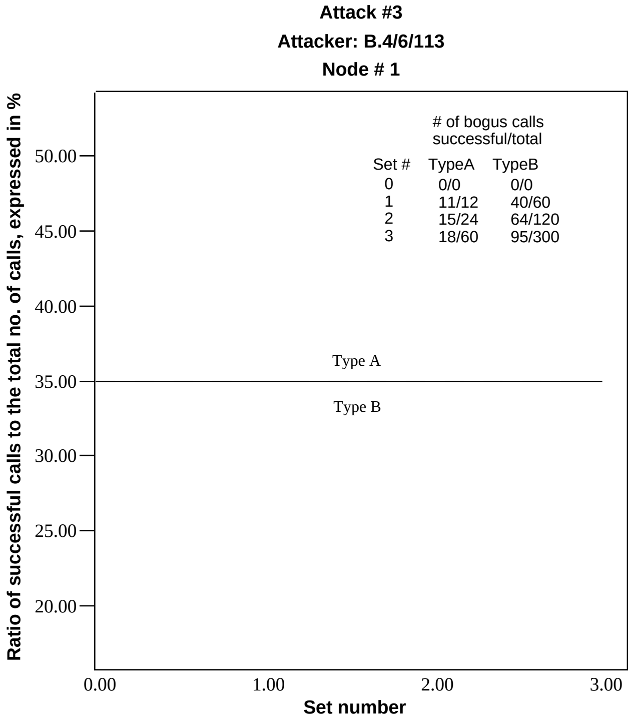

Fig. 9. Fractional call success rate at node A.1 under attack 3, as a function of the input traffic sets.

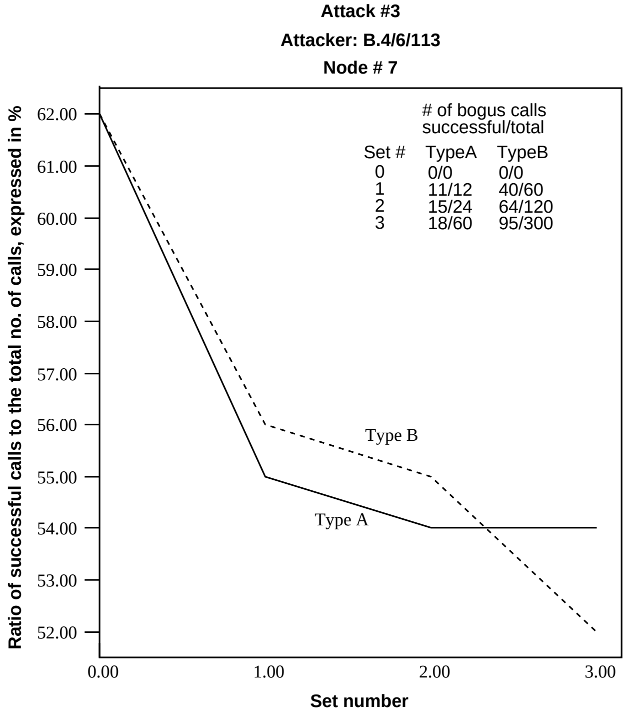

Fig. 11. Fractional call success rate at node B.5 under attack 3, as a function of the input traffic sets.

the drop in the call success rate at node B.5, shown in Fig. 11, is 62−54%=8% for attack with type A traffic and 62−52%=10% for attack with type B traffic. Clearly, by virtue of being much closer to the attacker, node B.5 is more susceptible to attack 3 than A.2. To gain statistical confidence and for reliable simulation results, every experiment is repeatedly executed a number of times, and the final simulation result is obtained through averaging the data across all of the runs.

When a given network operating at the stable region experiences a sharp drop in the average call success rate throughout the network as well as at a number of the peer nodes of a group, and no obvious reason is present, it is likely to be a victim of attack 3. Where, the bandwidth demands of a number of successfully established calls are appreciably high, the attack may have been launched with type A traffic. In the event that the call setup time is appreciably higher and the number of calls with high bandwidth demand is less than significant, the attack is likely to have been launched with type B traffic. Localizing attack 3 is relatively straightforward, since the nodes close to the source of the attack, especially in the same peer group, are affected more severely than those at a distance, particularly in other peer groups.

5.6. Attack 4

Under this attack, a perpetrator controlling a node in the network will attempt to usurp all network resources at the disposal of a target node, thereby isolating it from the remainder of the network. The underlying mechanism employed by this attack is similar to that utilized in attack 3 in that the perpetrator attempts to establish bogus calls to as many of the neighboring nodes of the target node as possible, routing them through the target node and usurping as much as possible the bandwidth resources of the links connected to the target node.

5.6.1. Experiments

To understand how the relative locations of the attacker and target nodes in the network topology influence the impact of this attack, especially in relationship to the connectivity with other peer groups, a number of attacker node and target node combinations are examined in this study. A total of three sets are included in the study here. In this subsection, a target call is defined as one that includes the target node in its route, either as the source, destination, or any intermediate node. From the study described earlier in Section 5.5, the use of type B traffic is observed to cause much greater damage to the network than type A and is therefore employed in this study for worst-case analysis. The appropriate traffic input files are modified to include bogus calls that utilize the routes specified for each of the three sets of attacker node and target node combinations.

Under set 1, B.3 and B.4 constitute the location of the perpetrator and the target node, respectively. The input file ‘attack.in’ contains the line 1 112 113. For each of the four routes: B.3→B.4→B.1, B.3→B.4→B.5, B.3→B.5→B.4, and B.3→B.4→B.2 a total of 80 bogus calls are synthesized with bandwidth demands ranging from 4 to 6 Mb/s. The rationale underlying the choice of the (B.3, B.4) node pair is as follows. Given that both B.3 and B.4 constitute the only nodes that connect to the gateway nodes in peer group B, many of the intergroup calls are likely to include them in their routes. The choice of any one of them as a target node offers a good chance to observe the attack in action. Here, B.4 is arbitrarily chosen as the target node, while B.3 is selected as the attacker node. It is pointed out that under the choices, the attacker node is directly connected to the target node.

Under set 2, while the attacker continues to be situated at B.3, the target is located at an interior node B.5 that is connected only to a single gateway node, B.1, and presumably encounters the least intergroup traffic of all other nodes in peer group B. As in set 1, the attacker node is directly connected to the target node. A secondary aim underlying this choice is to examine how well this attack refrains from disturbing the remainder of the network while focusing the damage on the relatively remote target node. The input file ‘attack.in’ contains the line: 1 112 114. For each of the four routes, B.3→B.5→B.1, B.3→B.5→B.4, B.3→B.4→B.5, and B.3→B.1→B.5, a total of 80 bogus calls are synthesized with bandwidth demands ranging from 4 to 6 Mb/s.

Under set 3, the goal is to study the impact of the attack on a gateway node including the extent of the damage inflicted to other peer groups. The target is located at B.2, and the attacker is placed at node B.4. While the perpetrator is connected to both gateway nodes, it is also directly connected to the target node. The input file ‘attack.in’ contains the line: 1 113 111. For each of the three routes, B.4→B.2→C.2, B.4→B.2→B.3, B.4→B.3→B.2, and B.4→B.3→B.2→C.2, a total of 80 bogus calls are synthesized with bandwidth demands ranging from 4 to 6 Mb/s.

5.6.2. Analysis of the simulation results

Fig. 12 presents the average call success rates at each of the nine nodes of the network, under normal and attack scenarios, corresponding to set 1. The rate is computed based on all user call requests that are inserted into the network. As expected, the call success rate at the target node six (B.4) is reduced significantly from over 62–22%. However, because the perpetrator must use the links at node five (B.3) to launch the attack, the call success rate for legitimate user calls at node five is also sharply reduced, from 62 to 30%. An important observation is that for nodes seven (B.5) and four (B.2) the call success rates are lowered, implying that the links connected to B.5 and B.2 are exploited by the perpetrator to launch the attack. Nodes eight (C.1), nine (C.2), and one (A.1) are located far away from the source of the attack and reveal zero impact on their

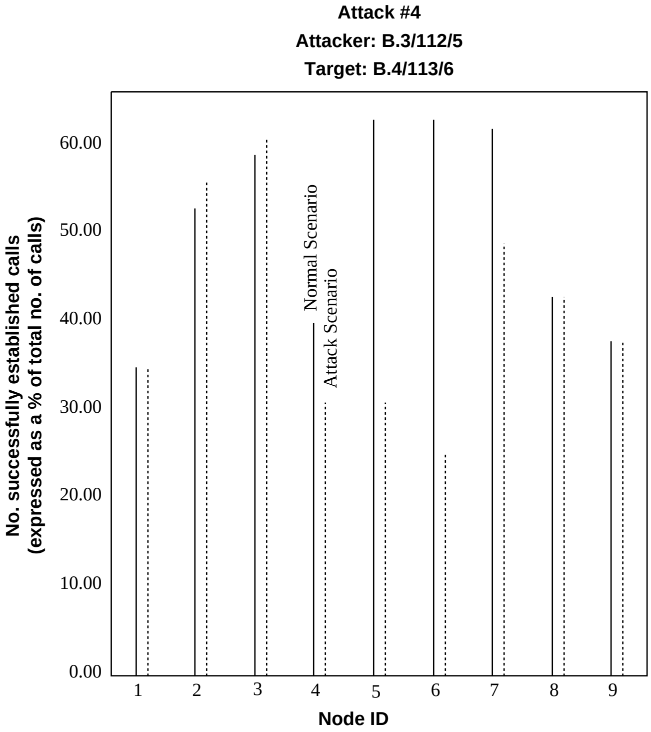

Fig. 12. Call success rates at the nodes of the network for normal and attack four scenarios, for set 1.

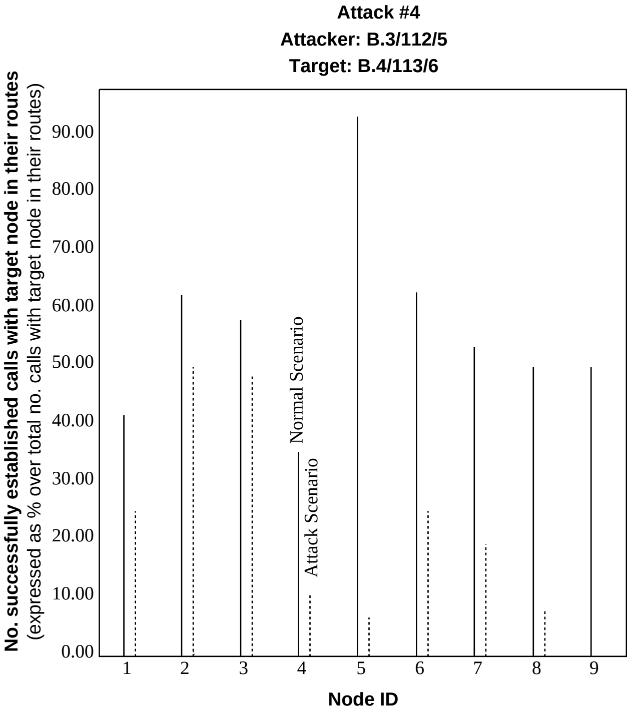

Fig. 13. Success rates for target calls at the nodes of the network for normal and attack four scenarios, for set 1.

call success rates. The increase in the call success rates at nodes two (A.2) and three (B.1) is explained as follows. Given that many of the legitimate user calls fail due to lack of resources, the bandwidths along other links that would have been otherwise utilized under the normal scenario become available under the attack scenario. In turn, this permits a few of the calls that were previously denied under the normal scenario to be successfully established, causing a slight increase in the call success rates.

Fig. 13 presents a detailed picture of the influence of attack 4 by focusing solely on the target calls, i.e. those that include the target node in their route. Calls with the target node as the source, calls sinking into the target node, and calls that simply pass through the target node all qualify. The graphs reveal that attack 4 is highly successful in that it affects every node in the entire network that attempts to reach the target node B.4. In contrast to Fig. 12, target calls are solely considered here, and since they can fail only under attack, the graphs for all nodes under attack are uniformly lower than under the normal scenario.

The general behavior of the graphs in Fig. 14 for set 2 is similar to that for set 1.

Fig. 15 presents the success rates as a function of the nodes in the network for normal and attack scenarios, for set 3, for all calls in the network as well as the target calls. Except for the target node four (B.2) in Fig. 15(a), the damage from the attack on other nodes in the network appears to be less severe than for sets 1 and 2. Given its location in the peer group B and that it is a gateway node, B.2 appears to play a minor role relative to the intra-group calls within group B. As a result, an attack on it has not caused widespread reduction in the call success rates at all of the nodes of B. However, as shown in Fig. 15(b), the target calls are adversely affected as a result of the attack. Clearly, inter-group calls from the nodes of group B to C are likely to be routed through B.2 and are susceptible to attack. Intergroup calls originating at the nodes of group C and destined for members of group B are not affected by the attack, since the link C.2→B.2 is beyond B.4's capacity to attack. By definition of an ATM network and according to the PNNI 1.0 specification, a node within a peer group may not possess knowledge of the internal topology of a different peer group. This is shown in both Fig. 15(a) and (b).

In summary, attack 4 can serve as an effective tool against a peer node, except when it serves as a gateway node. The target and attacking nodes are likely to experience the most significant drop in their call success rates, which in turn, may serve to point to the source of the attack.

5.7. Attack 5

The objective in this attack is to attempt to prevent two specific nodes from communicating with one another. As in the case of the previous attack 4, here, type B traffic is

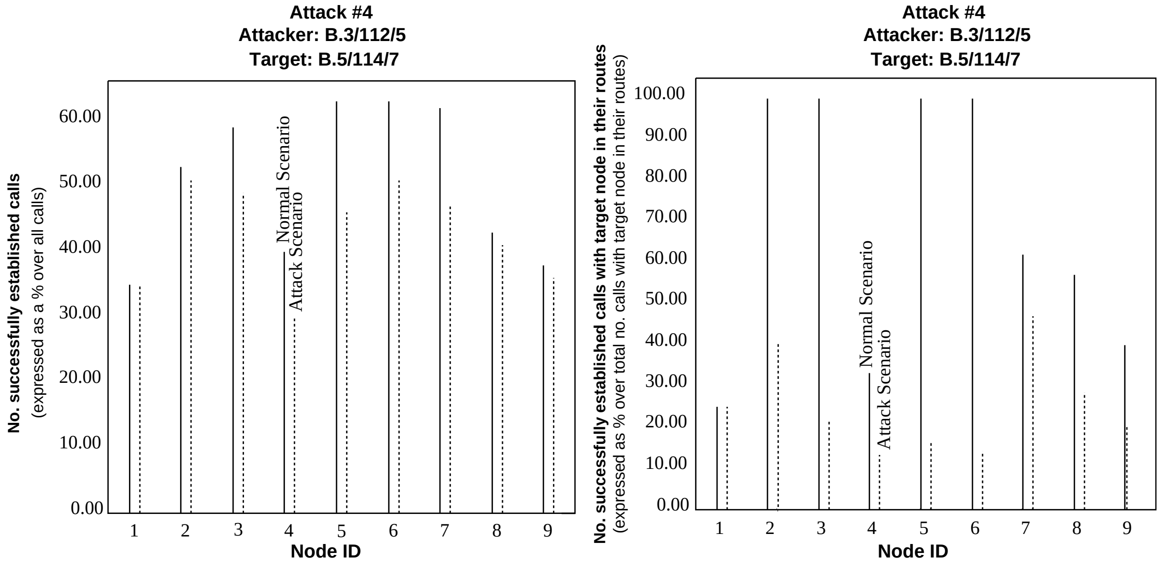

Fig. 14. Success rates for (a) all calls and (b) target calls, at the node of the network for normal and attack scenarios, for set 2.

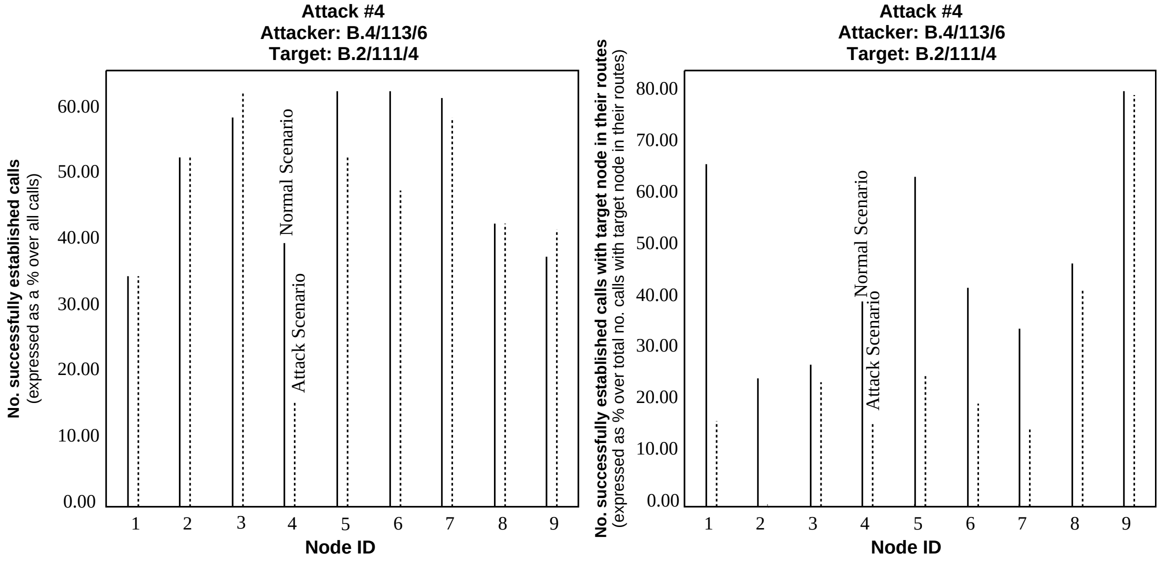

Fig. 15. Success rates for (a) all calls and (b) target calls, at the node of the network for normal and attack scenarios, for set 3.

employed. While the link interconnecting the two specific nodes is labeled target link, the calls routed through the target link are termed target calls. The details of the attack and analysis of results are not presented here for space limitations. However, in summary, attack 5 can serve as an effective tool in inhibiting communication between two peer nodes, connected through a link. Where, one of the nodes belongs to a different peer group, the effectiveness of the attack is greatly diminished. The target link and a few of the neighboring links that are employed in synthesizing and launching the attack are likely to experience the most significant drop in their link utilization rates, which may serve to point to the source of the attack.

6. Conclusions

This paper has presented a new, modeling and asynchronous distributed simulation-based approach to systematically uncover vulnerabilities in ATM network designs. In this approach, attacks are synthesized to expose weaknesses in networks, modeled utilizing a representative ATM network, and analyzed through a simulation utilizing an asynchronous, distributed, and accurate ATM simulator, that executes on a network of Pentium workstations under Linux, configured as a loosely-coupled parallel processor. Thus, the environment underlying the evaluation of the vulnerabilities reflect reality, implying, in turn, realistic results. The approach has been demonstrated for ATM networks and may be easily generalized to MPLS and future network designs.

References

[1] A. Miczo, Digital logic testing and simulation, Harper and Row, New York, 1986.

[2] S. Ghosh, P. Robinson, A framework for investigating security attacks in ATM networks, in: Proceedings of the IEEE MILCOM'99 Conference, Atlantic City Convention Center, NJ, 1999, pp. 724–728.

[3] D. Bertsekas, R. Gallagher, Data networks, Prentice Hall, Englewood Cliffs, NJ, 1992.

[4] K. Thompson, On trusting trust, Unix Rev. 7 (11) (1984) 71–74.

[5] T.J. Chaney, E. Molnar, Anomalous behavior of synchronizer and arbiter circuits, IEEE Trans. Comput. C-22 (4) (1972) 421–422.

[6] ATM Forum Technical Committee, Private Network–Network Interface Specification Version 1.0 (PNNI 1.0), www.atmforum.com/atmforum/specs/approved.html, ATM Forum, 1996.

[7] D.T. Tarman, E.L. Witzke, Implementing security for ATM networks, Artech House, Boston, MA, 2002.

[8] S. Ghosh, Principles of secure network systems design, Springer, New York, 2002.

[9] Multiprotocol Label Switching (MPLS) Technical Documentation. Cisco Systems Inc., 2004.

[10] Private communications with Dr Seong-Soon Joo, BcN Department Head, ETRI, Korea, 2004.

[11] Dr K.P. Jun, Vice-President, ETRI, Korea, Toward BcN (Broadband convergence Network, Keynote address: ATM Forum Conference, 2004.

[12] G.H. Johannessen, Signaling systems. An international concern, Bell Lab. Rec. 48 (1) (1970) 13–18.

[13] C. Breen, C.A. Dahlbom, Signaling systems for control of telephone switching, Bell Syst. Tech. J. 39 (6) (1960) 1381–1444.

[14] The Technical Journal. http://mbay.net/~mpoirier/bstj.html.

[15] S. Ghosh, T. Lee, Principles of modeling and asynchronous distributed simulation of complex systems, IEEE Press, Piscataway, NJ, 2000.

[16] Q. Razouqi, S.S. Joo, S. Ghosh, Performance analysis of fuzzy thresholding based buffer management for a large-scale cell-switching network, IEEE Trans. Fuzzy Syst. 8 (4) (2000) 425–441.

[17] Q. Razouqi, S. Ghosh, The Influence of buffer management on end-to-end cell delay in a cell switching network, IEICE Trans. Commun. E86 (3) (2003) 1073–1081.